

# Operational Threat and Risk Information Sharing and Federation Model

---

*OMG Document Numbers*

INVENTORY SYSA/2016-05-01

SUBMISSION DOCUMENT SYSA/2016-05-02 (THIS DOCUMENT)

THREAT/RISK CONCEPTUAL MODEL XMI SYSA/2016-05-03

SIMF PROFILE XMI SYSA/2016-05-04

NIEM MAPPING MODEL XMI SYSA/2016-05-05

STIX UML MODEL XMI SYSA/2016-05-06

STIX MAPPING MODEL SYSA/2016-05-07

NON-NORMATIVE ARTIFACTS (ZIP) SYSA/2016-05-08

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](http://www.omg.org/report_issue).)



# Table of Contents

0	Submission-related material.....	25
0.1	Submission Introduction.....	25
0.2	Submission Team .....	25
0.2.1	Submitters 25	
0.2.2	Contributors & Supporters.....	25
0.3	Proof of concept .....	26
0.4	Resolution of Requirements .....	27
0.4.1	Mandatory requirements .....	27
0.4.2	Non-mandatory features.....	30
0.5	Resolution of Discussion Issues .....	30
1.1	Scope .....	32
2	Conformance.....	32
2.1	Canonical model conformance .....	33
2.2	Mapping conformance.....	33
2.3	STIX mapping conformance .....	33
2.4	NIEM mapping conformance .....	33
3	References .....	34
4	Terms and Definitions .....	35
5	Symbols .....	35
6	Additional Information .....	35
6.1	Acknowledgments .....	35
7	Operational Threat and Risk Guide (Non Normative) .....	38
7.1	Mission and purpose.....	38
7.2	Technology capabilities.....	39
7.2.1	Federated analytics and simulation capabilities .....	39
7.2.2	Information Translating, Analytics, and Sharing capabilities .....	40
7.2.3	Risk Analytics Capabilities.....	40
7.3	Approaches to Federation and Integration.....	41
7.3.1	Syntactic Federation and Translation.....	41
7.3.2	Canonical data formats .....	41
7.3.3	Semantic federation and translation.....	42
7.4	Defining and Leveraging Conceptual Models .....	45
7.4.1	Expressing conceptual models.....	45

7.4.2	Layering	46
7.4.3	Source of concepts.....	46
7.5	Top Level Concepts .....	48
7.6	Mixing Concepts with “multiple classification” .....	51
8	Conceptual Model Specification (Normative) .....	53
8.1	Threat-risk-conceptual-model::Foundational Concepts.....	53
8.1.1	Diagram: Core Concept Library .....	53
8.2	Threat-risk-conceptual-model::Foundational Concepts::Foundation .....	54
8.2.1	Diagram: Upper Foundation Concepts .....	54
8.2.2	Class Actor	54
8.2.3	Class Actual Entity .....	56
8.2.4	Class Anything.....	56
8.2.5	Association Categorization .....	58
8.2.6	Class Category .....	58
8.2.7	Class Context.....	58
8.2.8	Class Context Type.....	59
8.2.9	Association Contextualization .....	59
8.2.10	Class Entity	60
8.2.11	Association Generalization .....	62
8.2.12	Association Involvement .....	62
8.2.13	Class Responsible Performer .....	62
8.2.14	Class Role	63
8.3	Threat-risk-conceptual-model::Foundational Concepts::Identifiers .....	64
8.3.1	Diagram: Identifiers.....	65
8.3.2	Class Abbreviated Name .....	65
8.3.3	Association Identification .....	66
8.3.4	Class Identifier.....	66
8.3.5	Class Name	66
8.3.6	Class Name Identifier .....	67
8.3.7	Class Namespace .....	67
8.3.8	Class Network Identifier .....	67
8.3.9	Class Simple Identifier.....	67
8.3.10	Class Technical Identifier .....	68
8.3.11	Class Text Identifier .....	68
8.3.12	Class Unique Identifier .....	68
8.3.13	Class URIIdentifier.....	69
8.4	Threat-risk-conceptual-model::Foundational Concepts::Information.....	70

8.4.1	Diagram: Information .....	70
8.4.2	Class Confidence .....	71
8.4.3	Class Information Action.....	71
8.4.4	Class Information Object.....	72
8.4.5	Class Information Source.....	72
8.4.6	Class Information Store .....	72
8.4.7	Class Information Transfer .....	73
8.4.8	Class Metadata.....	73
8.4.9	Class Natural Language Text.....	73
8.4.10	Class Package .....	74
8.4.11	Class Reference .....	74
8.4.12	Class Report 74	
8.4.13	Class Software .....	74
8.4.14	Class Statement.....	75
8.4.15	Class Structured Information Object.....	75
8.4.16	Class Summary Description.....	75
8.5	Threat-risk-conceptual-model::Foundational Concepts::Patterns.....	76
8.5.1	Diagram: Patterns .....	76
8.5.2	Class Pattern 77	
8.5.3	Class Pattern Property.....	77
8.5.4	Class Value Binding .....	78
8.6	Threat-risk-conceptual-model::Foundational Concepts::Processes .....	80
8.6.1	Diagram: Process and Plans.....	81
8.6.2	Class Action On Entity .....	81
8.6.3	Class Activity.....	82
8.6.4	Class Invoke Process .....	82
8.6.5	Class Modus Operandi.....	82
8.6.6	Class Plan 83	
8.6.7	Class Process .....	83
8.6.8	Class Process Action.....	83
8.6.9	Class Scenario.....	84
8.7	Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units .....	85
8.7.1	Diagram: Quantities and units.....	85
8.7.2	Class Benefit Metric .....	86
8.7.3	Class Confidence Metric.....	86
8.7.4	Class Count 86	
8.7.5	Class Currency Benefit Metric.....	86

8.7.6	Class Metric	86
8.7.7	Class Probability Metric .....	87
8.7.8	Class Quantity Kind.....	87
8.7.9	Class Time Point.....	87
8.7.10	Class Value	87
8.8	Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds.....	89
8.8.1	Diagram: Quantity Kinds .....	89
8.8.2	Class Absorbed Dose (Radiation).....	89
8.8.3	Class Acceleration .....	90
8.8.4	Class Amount of Substance .....	90
8.8.5	Class Angle	90
8.8.6	Class Area	90
8.8.7	Class Color	91
8.8.8	Class Concentration.....	91
8.8.9	Class Concentration (amount of substance).....	91
8.8.10	Class Concentration (Mass) .....	91
8.8.11	Class Concentration (Volume).....	91
8.8.12	Class Count	92
8.8.13	Class Currency.....	92
8.8.14	Class Dose Equivalent (Radiation) .....	92
8.8.15	Class Electric Current .....	92
8.8.16	Class Electric Potential .....	93
8.8.17	Class Energy	93
8.8.18	Class Force	93
8.8.19	Class Frequency.....	93
8.8.20	Class Length	93
8.8.21	Class Luminosity .....	94
8.8.22	Class Luminous Intensity.....	94
8.8.23	Class Mass	94
8.8.24	Class Mass Density.....	95
8.8.25	Class Physical Characteristic .....	95
8.8.26	Class Physical Quantity Kind .....	95
8.8.27	Class Power	95
8.8.28	Class Pressure .....	95
8.8.29	Class Radiation Exposure .....	96
8.8.30	Class Radioactivity .....	96
8.8.31	Class Speed	96

8.8.32	Class Temperature .....	96
8.8.33	Class Time	96
8.8.34	Class Volume .....	97
8.9	Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units .....	98
8.9.1	Diagram: Common Units 1 .....	98
8.9.2	Diagram: Common Units 2 .....	99
8.9.3	Class Acre	99
8.9.4	Class Ampere .....	99
8.9.5	Class Becquerel (Bq) .....	100
8.9.6	Class Candela .....	100
8.9.7	Class Celsius	100
8.9.8	Class Concentration Percent .....	100
8.9.9	Class Coulomb/kilogram (C/kg) .....	100
8.9.10	Class Cubic Feet .....	101
8.9.11	Class Cubic Inch .....	101
8.9.12	Class Cubic Meter .....	101
8.9.13	Class Cup (US) .....	101
8.9.14	Class Curie (Ci) .....	101
8.9.15	Class Day	101
8.9.16	Class Degrees .....	102
8.9.17	Class Fahrenheit .....	102
8.9.18	Class Fluid Ounce (US) .....	102
8.9.19	Class Foot	102
8.9.20	Class Gallon (Imperial) .....	102
8.9.21	Class Gallon (US) .....	103
8.9.22	Class Gram	103
8.9.23	Class Gray (Gy) .....	103
8.9.24	Class Hertz	103
8.9.25	Class Horsepower .....	104
8.9.26	Class Hour	104
8.9.27	Class Inch	104
8.9.28	Class Joule	104
8.9.29	Class Kelvin	104
8.9.30	Class Kg per cubic meter .....	105
8.9.31	Class Kilogram .....	105
8.9.32	Class Kilogram per cubic meter .....	105
8.9.33	Class Kilometer .....	105

8.9.34	Class Kilometer per Hour .....	105
8.9.35	Class Kilowatt hour .....	106
8.9.36	Class Liquid Volume .....	106
8.9.37	Class Meter 106	
8.9.38	Class Meter per second squared.....	106
8.9.39	Class Mile 106	
8.9.40	Class Miles per Hour .....	107
8.9.41	Class Millimeter.....	107
8.9.42	Class Millisecond.....	107
8.9.43	Class Minute 107	
8.9.44	Class Mole 107	
8.9.45	Class Mole Per Cubic Meter.....	108
8.9.46	Class Newton .....	108
8.9.47	Class Ounce-Mass (US).....	108
8.9.48	Class Pascal 108	
8.9.49	Class Pint (US) .....	108
8.9.50	Class Pound-Force .....	109
8.9.51	Class Pound-Mass (Imperial).....	109
8.9.52	Class Pound-Mass (US lb).....	109
8.9.53	Class PSI 109	
8.9.54	Class Quart (US).....	109
8.9.55	Class Radians.....	110
8.9.56	Class Radiation Absorbed Dose (rad).....	110
8.9.57	Class Roentgen (R).....	110
8.9.58	Class Roentgen Equivalent Man (REM).....	110
8.9.59	Class Second111	
8.9.60	Class Sievert (Sv), .....	111
8.9.61	Class Square Feet.....	111
8.9.62	Class Square Meter.....	111
8.9.63	Class Volt 111	
8.9.64	Class Watt 112	
8.9.65	Class Yard 112	
8.9.66	Class Year 112	
8.10	Threat-risk-conceptual-model::Foundational Concepts::Rules .....	113
8.10.1	Diagram: Rules .....	113
8.10.2	Association Class Causality Rule.....	113
8.10.3	Class Constraint .....	114

8.10.4	Class Expression.....	114
8.10.5	Class Expression Language .....	114
8.10.6	Class Rule 115	
8.10.7	Class Text Expression.....	115
8.11	Threat-risk-conceptual-model::Foundational Concepts::Situations.....	116
8.11.1	Diagram: Situation.....	116
8.11.2	Association Cause and Effect .....	116
8.11.3	Class Occurrence .....	117
8.11.4	Class Situation .....	117
8.11.5	Class State 119	
8.11.6	Association Time Order.....	119
8.12	Threat-risk-conceptual-model::Foundational Concepts::Timeframes .....	120
8.12.1	Diagram: Actual Thing .....	120
8.12.2	Class Actual Occurrence.....	120
8.12.3	Class Actual Situation.....	121
8.12.4	Class Actual State .....	121
8.12.5	Class Current Situation .....	121
8.12.6	Class Non Happening .....	121
8.12.7	Class Past Situation.....	122
8.12.8	Class Potential Situation .....	122
8.13	Threat-risk-conceptual-model::Generic Concepts.....	123
8.13.1	Diagram: Generic Concept Library.....	123
8.14	Threat-risk-conceptual-model::Generic Concepts::Abilities .....	124
8.14.1	Diagram: Ability .....	124
8.14.2	Association Class Ability.....	125
8.14.3	Class Alter Ability .....	125
8.14.4	Class Diminish Ability.....	126
8.14.5	Class Enhance Ability.....	126
8.14.6	Class Facilitator .....	126
8.15	Threat-risk-conceptual-model::Generic Concepts::Actor Relationships .....	127
8.15.1	Diagram: Actor Identifiers.....	127
8.15.2	Diagram: Actor/Organization Relations .....	128
8.15.3	Association Class Actor Association .....	129
8.15.4	Class Country.....	129
8.15.5	Class Country ID .....	129
8.15.6	Class Geopolitical Entity .....	129
8.15.7	Class Geopolitical ID.....	130

8.15.8	Class Incorporated Organization .....	130
8.15.9	Association Class Incorporation .....	130
8.15.10	Class License Identifier .....	131
8.15.11	Class Local Identifier.....	131
8.15.12	Class Managed Actor Identifier.....	131
8.15.13	Association Class Regional Authority .....	131
8.15.14	Class State Identifier.....	132
8.15.15	Class Tax Identification .....	132
8.16	Threat-risk-conceptual-model::Generic Concepts::Assessments.....	133
8.16.1	Diagram: Assessment.....	133
8.16.2	Class Assessed Entity .....	133
8.16.3	Class Assessment Activity .....	134
8.16.4	Class Assessment Report .....	134
8.17	Threat-risk-conceptual-model::Generic Concepts::Capabilities .....	135
8.17.1	Diagram: Capability.....	135
8.17.2	Association Class Capability .....	135
8.18	Threat-risk-conceptual-model::Generic Concepts::Composite Conditions .....	137
8.18.1	Diagram: Composite Condition .....	137
8.18.2	Class AND Condition .....	137
8.18.3	Class Composite Condition.....	137
8.18.4	Class OR Condition .....	138
8.18.5	Class XOR Condition .....	138
8.19	Threat-risk-conceptual-model::Generic Concepts::Contact Information.....	139
8.19.1	Diagram: Contact Information.....	139
8.19.2	Class Communications Security Level.....	140
8.19.3	Association Class Contact Information.....	140
8.19.4	Class Contact Means.....	140
8.19.5	Class Contactable.....	141
8.19.6	Class Electronic Contact.....	141
8.19.7	Class Email Address .....	142
8.19.8	Class Internet Contact.....	142
8.19.9	Class Postal Address .....	142
8.19.10	Class Postal Address Structured .....	142
8.19.11	Class Postal Address Text .....	143
8.19.12	Class Postal Code .....	144
8.19.13	Class Private Network Contact .....	144
8.19.14	Class Radio Contact.....	144

8.19.15	Class Social Network Contact .....	144
8.19.16	Class Telephone Area Code.....	145
8.19.17	Class Telephone Country Code .....	145
8.19.18	Class Telephone Number.....	145
8.19.19	Class Telephone Number Structured .....	145
8.19.20	Class Telephone Number Text .....	146
8.19.21	Class Website Contact .....	146
8.20	Threat-risk-conceptual-model::Generic Concepts::Control.....	148
8.20.1	Diagram: Control .....	148
8.20.2	Diagram: Control Authority.....	149
8.20.3	Diagram: Custody .....	150
8.20.4	Diagram: Transfer of control .....	151
8.20.5	Association Asserting Policy .....	151
8.20.6	Class Authority .....	152
8.20.7	Association Class Automated Control .....	152
8.20.8	Class Automated Entity .....	152
8.20.9	Class Computer Control System .....	153
8.20.10	Association Class Control.....	153
8.20.11	Class Control Action.....	154
8.20.12	Class Controlled Entity.....	154
8.20.13	Class Controlling Actor .....	154
8.20.14	Class Create Entity.....	155
8.20.15	Class Custodian .....	155
8.20.16	Association Class Custody.....	155
8.20.17	Class Destroy Entity .....	156
8.20.18	Class Leader 156	
8.20.19	Association Class Leadership .....	156
8.20.20	Class Lose Control.....	157
8.20.21	Class Managed Entity .....	157
8.20.22	Class Obtain Control.....	157
8.20.23	Class Owner 158	
8.20.24	Association Class Ownership.....	158
8.20.25	Association Class Possession.....	158
8.20.26	Class Property.....	159
8.20.27	Association Class Subject to Authority.....	159
8.20.28	Class Transfer Control.....	159
8.21	Threat-risk-conceptual-model::Generic Concepts::Courses of action .....	160

8.21.1	Diagram: Course of Action .....	160
8.21.2	Class Course of Action .....	160
8.21.3	Association Class Course Of Action Rule .....	161
8.22	Threat-risk-conceptual-model::Generic Concepts::Credentials.....	162
8.22.1	Diagram: Credentials and Managed Identifiers .....	162
8.22.2	Class Credential .....	163
8.22.3	Class Identity Provider .....	163
8.22.4	Class Managed Identifier .....	163
8.23	Threat-risk-conceptual-model::Generic Concepts::Cyber .....	165
8.23.1	Diagram: Cyber .....	165
8.23.2	Class Cyber Weapon.....	165
8.24	Threat-risk-conceptual-model::Generic Concepts::Enterprises.....	166
8.24.1	Diagram: Enterprise .....	166
8.24.2	Class Enterprise .....	166
8.25	Threat-risk-conceptual-model::Generic Concepts::Entity Kinds.....	168
8.25.1	Diagram: Entity Kinds .....	168
8.25.2	Class Animal168	
8.25.3	Class Physical Entity.....	169
8.26	Threat-risk-conceptual-model::Generic Concepts::Items .....	172
8.26.1	Diagram: Items .....	172
8.26.2	Class Automaton.....	172
8.26.3	Class Communicating Device .....	173
8.26.4	Class Communications Network.....	173
8.26.5	Class Computer System .....	174
8.26.6	Class Conveyance .....	174
8.26.7	Class Device 174	
8.26.8	Class Item 175	
8.26.9	Class Managed Item Identifier.....	175
8.26.10	Class Physical Tool.....	176
8.26.11	Class Physical Weapon.....	176
8.26.12	Class Telecommunication Device.....	176
8.27	Threat-risk-conceptual-model::Generic Concepts::Locations .....	177
8.27.1	Diagram: Location .....	177
8.27.2	Diagram: Location Identification.....	178
8.27.3	Class Bounded Topology.....	178
8.27.4	Class Coordinate.....	179
8.27.5	Class Coordinate System .....	179

8.27.6	Class Geopolitical Region .....	179
8.27.7	Class Location ID .....	180
8.27.8	Class Location Identifier.....	180
8.27.9	Class Map 180	
8.27.10	Class Map Coordinate.....	180
8.27.11	Class Physical Location .....	181
8.27.12	Class Point On Earth.....	181
8.27.13	Class Relative Coordinate.....	182
8.27.14	Class Relocation .....	182
8.27.15	Class Topological Point.....	182
8.27.16	Class Topology .....	183
8.27.17	Class World Geodetic System .....	183
8.28	Threat-risk-conceptual-model::Generic Concepts::Manufacturers.....	184
8.28.1	Diagram: Manufacturer.....	184
8.28.2	Class Manufactured Thing.....	184
8.28.3	Class Manufacturer.....	185
8.29	Threat-risk-conceptual-model::Generic Concepts::Objectives.....	186
8.29.1	Diagram: Impact .....	186
8.29.2	Diagram: Objectives .....	187
8.29.3	Class Benefit187	
8.29.4	Class Desirability Metric .....	188
8.29.5	Class Harm 188	
8.29.6	Class Impact 189	
8.29.7	Class Means 190	
8.29.8	Association Means to End .....	190
8.29.9	Class Objective .....	191
8.29.10	Class Opportunity .....	192
8.29.11	Class Stakeholder.....	193
8.29.12	Association Class Stakeholder Desirability .....	193
8.30	Threat-risk-conceptual-model::Generic Concepts::Observations .....	194
8.30.1	Diagram: Observability.....	194
8.30.2	Diagram: Observation.....	195
8.30.3	Class Measurement.....	195
8.30.4	Association Class Observability .....	195
8.30.5	Class Observation .....	196
8.30.6	Class Observation Tool.....	196
8.30.7	Class Observer .....	196

8.31	Threat-risk-conceptual-model::Generic Concepts::Organizations.....	198
8.31.1	Diagram: Organization .....	198
8.31.2	Association Class Membership.....	198
8.31.3	Class Mission Objective .....	199
8.31.4	Class Organization.....	199
8.31.5	Class Program.....	199
8.32	Threat-risk-conceptual-model::Generic Concepts::Permissions.....	201
8.32.1	Diagram: Permission.....	201
8.32.2	Association Class Permission .....	202
8.33	Threat-risk-conceptual-model::Generic Concepts::Persons .....	203
8.33.1	Diagram: Person .....	203
8.33.2	Diagram: Person Identifiers .....	204
8.33.3	Class Access Identifier.....	204
8.33.4	Class Financial Identifier .....	205
8.33.5	Class Managed Person Identifier .....	205
8.33.6	Class Passport Identifier .....	205
8.33.7	Class Person 205	
8.33.8	Association Class Person at location .....	206
8.33.9	Class Person Name .....	206
8.33.10	Class Person Structured Name.....	206
8.33.11	Class Person Textual Name .....	207
8.33.12	Class Social Security Number.....	207
8.34	Threat-risk-conceptual-model::Generic Concepts::Places.....	208
8.34.1	Diagram: Place .....	208
8.34.2	Class Facility .....	208
8.34.3	Class Place 208	
8.34.4	Class Residence .....	209
8.35	Threat-risk-conceptual-model::Generic Concepts::Policies .....	210
8.35.1	Diagram: Policy .....	210
8.35.2	Class Policy 210	
8.35.3	Association Subject of Rule.....	211
8.36	Threat-risk-conceptual-model::Generic Concepts::Predictions.....	212
8.36.1	Diagram: Prediction.....	212
8.36.2	Class Prediction .....	212
8.36.3	Class Predictor.....	213
8.37	Threat-risk-conceptual-model::Generic Concepts::Resources.....	214
8.37.1	Diagram: Resource .....	214

8.37.2	Class Performer .....	214
8.37.3	Class Resource.....	215
8.37.4	Class Tool 215	
8.37.5	Class Weapon .....	216
8.38	Threat-risk-conceptual-model::Generic Concepts::Systems.....	217
8.38.1	Diagram: System.....	217
8.38.2	Class Access Point.....	217
8.38.3	Class Boundary.....	218
8.38.4	Association Subsystem .....	218
8.38.5	Class Subsystem .....	219
8.38.6	Class System219	
8.39	Threat-risk-conceptual-model::Generic Concepts::Transfer .....	220
8.39.1	Diagram: Transfer.....	220
8.39.2	Class Transfer .....	220
8.40	Threat-risk-conceptual-model::Threat and Risk Specific Concepts .....	221
8.40.1	Diagram: Threat and Risk Specific Concepts .....	221
8.41	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS .....	223
8.41.1	Diagram: Vulnerability Vectors.....	224
8.41.2	Class CVSS Score.....	225
8.42	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Campaigns .....	234
8.42.1	Diagram: Campaign.....	234
8.42.2	Class Campaign .....	234
8.43	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger Categories.....	235
8.43.1	Diagram: Danger Categories.....	235
8.43.2	Diagram: Danger Source Categories.....	236
8.43.3	Diagram: Failure Categories .....	237
8.43.4	Diagram: Impact Categories .....	238
8.43.5	Class Access Control Failure .....	238
8.43.6	Class Biological Danger .....	239
8.43.7	Class CBRN Danger .....	239
8.43.8	Class Chemical Danger.....	239
8.43.9	Class Civil Unrest Danger .....	239
8.43.10	Class Compliance Impact .....	239
8.43.11	Class Control Failure .....	240
8.43.12	Class Criminal Danger.....	240
8.43.13	Class Cyber Danger .....	240
8.43.14	Class Cyber System Failure .....	240

8.43.15	Class Danger Category .....	240
8.43.16	Class Decision-making Impact .....	240
8.43.17	Class Disinformation Impact .....	241
8.43.18	Class Electromagnetic Spectrum Impact.....	241
8.43.19	Class Environmental Impact .....	241
8.43.20	Class Failure Category.....	241
8.43.21	Class Financial Impact.....	241
8.43.22	Class Fire Danger .....	242
8.43.23	Class Geophysical Danger .....	242
8.43.24	Class Health Impact.....	242
8.43.25	Class Identity Theft.....	242
8.43.26	Class Image Impact.....	242
8.43.27	Class Impact Category .....	243
8.43.28	Class Inability to Communicate Impact.....	243
8.43.29	Class Industrial Control Failure .....	243
8.43.30	Class Information Impact.....	243
8.43.31	Class Information Loss Impact .....	243
8.43.32	Class Infrastructure Impact.....	244
8.43.33	Class Intellectual Property Impact.....	244
8.43.34	Class Legal Impact.....	244
8.43.35	Class Loss of Control Danger .....	244
8.43.36	Class Meteorological Danger.....	244
8.43.37	Class Mission Impact.....	245
8.43.38	Class Non-Technical Impact.....	245
8.43.39	Class Nuclear Danger .....	245
8.43.40	Class Physical System Failure .....	245
8.43.41	Class Process Failure .....	245
8.43.42	Class Radiological Danger.....	245
8.43.43	Class Safety Danger.....	246
8.43.44	Class Safety Impact .....	246
8.43.45	Class Security Danger.....	246
8.43.46	Class Source of Danger Category .....	246
8.43.47	Class System Failure.....	246
8.43.48	Class Terrorism Danger .....	247
8.43.49	Class Transport Impact .....	247
8.43.50	Class War Danger .....	247
8.44	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger Sources .....	248

8.44.1	Diagram: Danger Sources .....	248
8.44.2	Diagram: Threat Actors .....	249
8.44.3	Class Danger Source.....	249
8.44.4	Class Disrupt Objective .....	250
8.44.5	Class Disruptive Action .....	250
8.44.6	Class Threat Actor .....	250
8.44.7	Class Threat Objective.....	251
8.45	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects .....	252
8.45.1	Diagram: Threat Effects.....	253
8.45.2	Class Abuse Resource.....	254
8.45.3	Class All Actions .....	254
8.45.4	Class Capture Resource .....	254
8.45.5	Class Close Information.....	254
8.45.6	Class Create Information .....	254
8.45.7	Class Damage .....	254
8.45.8	Class Damage Resource.....	255
8.45.9	Class Delete Information .....	255
8.45.10	Class Disrupt Process .....	255
8.45.11	Class Entry Action .....	255
8.45.12	Class Exceed Capacity.....	256
8.45.13	Class Exit Action .....	256
8.45.14	Class Interrupt Process .....	256
8.45.15	Class Modify Information.....	256
8.45.16	Class Modify Resource .....	256
8.45.17	Class Open Information .....	257
8.45.18	Class Read Information .....	257
8.45.19	Class Resource Actions .....	257
8.45.20	Class Stop Process .....	257
8.46	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents and failures .....	258
8.46.1	Diagram: Incident .....	258
8.46.2	Association Class Cause of Incident .....	258
8.46.3	Class Failure .....	259
8.46.4	Class Incident .....	259
8.46.5	Class Witness.....	260
8.47	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators .....	261
8.47.1	Diagram: Indicator.....	262
8.47.2	Diagram: Sighting.....	263

8.47.3	Class Blacklist Indicator .....	263
8.47.4	Association Class Indication.....	263
8.47.5	Class Indicator .....	264
8.47.6	Class Indicator Pattern.....	264
8.47.7	Class Indicator Watchlist.....	265
8.47.8	Class Sighting .....	265
8.47.9	Class Whitelist Indicator.....	267
8.48	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Kill Chains .....	268
8.48.1	Diagram: Kill Chain.....	268
8.48.2	Class Kill Chain.....	268
8.48.3	Class Kill Chain Step.....	268
8.49	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments .....	270
8.49.1	Diagram: Risk Treatment.....	270
8.49.2	Diagram: Safeguard Monitoring .....	271
8.49.3	Class Avoid Danger.....	271
8.49.4	Class Countermeasure.....	271
8.49.5	Class Mitigation Actor.....	272
8.49.6	Class Monitoring Safeguard .....	272
8.49.7	Class Risk Treatment Strategy.....	272
8.49.8	Class Safeguard Activity.....	273
8.49.9	Class Transfer Risk.....	273
8.50	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks .....	274
8.50.1	Diagram: Risk.....	274
8.50.2	Diagram: Risk Metrics.....	275
8.50.3	Class Accept Risk .....	275
8.50.4	Class Protect Assets Objective .....	275
8.50.5	Class Risk 276	
8.50.6	Class Risk Group .....	276
8.50.7	Class Risk Mitigation Strategy .....	276
8.50.8	Class Risk Owner.....	277
8.50.9	Class Risk Topic .....	277
8.50.10	Class Security and Safety Objective .....	277
8.50.11	Association Class Stakeholder Risk.....	278
8.50.12	Class Threat Likelihood.....	278
8.50.13	Class Valued Asset .....	278
8.50.14	Association Class Valued Assets .....	279
8.51	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Threats .....	281

8.51.1	Diagram: Threat.....	281
8.51.2	Class Threat	281
8.52	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Undesirable Situations .....	283
8.52.1	Diagram: Undesirable Situation.....	284
8.52.2	Class Attack	284
8.52.3	Association Danger Impact.....	285
8.52.4	Class Indirect Threat.....	285
8.52.5	Class Natural Threat .....	285
8.52.6	Class Undesirable Event .....	285
8.52.7	Class Undesirable Situation .....	286
8.52.8	Class Undesirable State .....	287
8.52.9	Class Unintentional Threat .....	287
8.52.10	Class Unwitting Participant .....	287
8.52.11	Class Victim	288
8.53	Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities.....	289
8.53.1	Diagram: Cyber Vulnerability .....	289
8.53.2	Diagram: Vulnerability .....	290
8.53.3	Diagram: Vulnerability Identifiers.....	291
8.53.4	Class Communications Vulnerability.....	291
8.53.5	Class CVE Identifier.....	291
8.53.6	Class Cyber Vulnerability.....	292
8.53.7	Class Information System Vulnerability .....	292
8.53.8	Class Information Vulnerability.....	292
8.53.9	Class OSVDB Identifier .....	292
8.53.10	Class Physical Vulnerability .....	293
8.53.11	Class Software Vulnerability .....	293
8.53.12	Class Vulnerability .....	293
8.53.13	Class Vulnerability Identifier.....	294
8.53.14	Class Vulnerability Metric.....	294
9	STIX Mapping Specification (Normative) .....	295
9.1	How STIX is represented .....	295
9.2	Generic NIEM Mapping Rules and Conventions .....	295
9.3	STIX Mapping to the threat/risk conceptual model .....	296
9.3.1	Diagram: High Level STIX Mapping .....	296
9.4	STIX Mapping to the threat/risk conceptual model::Facades.....	297
9.4.1	Diagram: Facade Summary.....	297
9.4.2	Class ActualObservableFacade.....	297

9.4.3	Class AffectedAssetFacade.....	298
9.4.4	Class ExploitTargetFacade .....	298
9.4.5	Class ObservablePatternFacade.....	298
9.4.6	Class Threat Report .....	298
9.5	STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules .....	299
9.6	Class STIX Campaign Rule.....	299
9.7	Class STIX Categories Rule.....	300
9.8	Class STIX Course Of Action Rule.....	301
9.9	Class STIX Incident Rule.....	302
9.10	Class STIX Indicator Rule .....	303
9.11	Class STIX Objective Rule .....	304
9.12	Class STIX Observable Rule.....	305
9.13	Class STIX Sighting Rule .....	306
9.14	Class STIX Statement Rule .....	307
9.15	Class STIX Threat Actor Rule .....	308
9.16	Class STIX TTP Rule.....	309
9.17	Class STIX Vocabulary Rule .....	310
9.18	Class STIX Vulnerability Rule.....	311
10	NIEM Mapping Specification (Normative) .....	312
10.1	How NIEM is represented.....	312
10.2	Generic NIEM mapping rules and conventions.....	312
10.3	NIEM Mapping to the threat / risk model::Facades::Contact Information .....	314
10.3.1	Diagram: Contact Information Facades .....	314
10.3.2	Class Postal Address Facade.....	314
10.3.3	Class Telephone Number Facade.....	315
10.4	NIEM Mapping to the threat / risk model::Facades::Injury.....	316
10.4.1	Diagram: Person Injury Facade .....	316
10.4.2	Class PersonInjuryFacade.....	316
10.5	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships.....	317
10.5.1	Diagram: NIEM Mapping Rules.....	317
10.5.2	Diagram: NIEM Mapping Summary 1.....	318
10.5.3	Diagram: NIEM Mapping Summary 2.....	319
10.6	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Activity	320
10.6.1	Diagram: Activity Mapping Summary.....	320
10.6.2	Class Activity Map Rule .....	320
10.7	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Assessment	322
10.7.1	Diagram: Assessment Mapping Summary .....	322

10.7.2	Class Assessment Map Rule .....	323
10.8	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation.....	324
10.8.1	Diagram: Contact Information Mapping Summary.....	324
10.8.2	Class Address Map Rule.....	325
10.8.3	Class Contact Information Mapping Rule.....	326
10.8.4	Class Internet Contact Map Rule .....	327
10.8.5	Class Radio Map Rule .....	328
10.8.6	Class Telephone Map Rule .....	329
10.9	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Entity	330
10.9.1	Diagram: Entity Mapping Summary .....	330
10.9.2	Class Entiy Map Rule .....	330
10.10	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Identification .....	332
10.10.1	Diagram: Identification Mapping Summary .....	332
10.10.2	Class Identification Map Rule .....	333
10.11	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Incident	334
10.11.1	Diagram: Incident mapping summary .....	334
10.11.2	Class Incident Map Rule.....	334
10.12	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Injury	336
10.12.1	Diagram: Injury Mapping Summary .....	336
10.12.2	Class Injury Map Rule .....	337
10.13	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Item	338
10.13.1	Diagram: Item Mapping Summary .....	338
10.13.2	Class Item Map Rule.....	339
10.14	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location	340
10.14.1	Diagram: Location mapping summary .....	341
10.14.2	Class Area Map Rule .....	342
10.14.3	Class Coordinate Map Rule .....	342
10.14.4	Class Facility Map Rule.....	343
10.14.5	Class Location Map Rule.....	344
10.15	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Organization .....	345
10.15.1	Diagram: NIEM Organization Mapping Summary .....	345
10.15.2	Class Organization Map Rule .....	346
10.16	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Person	347
10.16.1	Diagram: Person Mapping Summary .....	347
10.16.2	Class Person Map Rule .....	348

10.16.3	Class Person Name Map Rule.....	349
10.17	NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM PrimitiveTypes .....	350
11	Threat and Risk Alignment to NIST 800-53.....	351
12	Annex A: UML Conceptual Modeling Profile Semantics (non-normative).....	384
12.1	Introduction .....	384
12.1.1	Classes      385	
12.1.2	Instances      385	
12.1.3	Class Generalization .....	386
12.1.4	Properties      391	
12.1.5	Associations 392	
12.1.6	Property and association end hierarchies .....	393
12.1.7	Association Classes.....	393
12.1.8	Annotation  395	
12.1.9	Specific kinds of classes .....	396
12.1.10	Assertions about concepts.....	399
12.1.11	Constraining properties and associations .....	399
12.1.12	Tightening a property's type .....	401
12.1.13	Inferring a type from its properties .....	402
12.1.14	Property Chain.....	403
12.1.15	Equivalent Property .....	405
12.1.16	Equivalent Class .....	405
12.2	SIMF Profile::SIMF Concept Modeling Profile Reference.....	407
12.2.1	Diagram SIMF Conceptual Modeling Profile.....	407
12.2.2	Stereotype Annotation .....	407
12.2.3	Stereotype Annotation Property.....	408
12.2.4	Stereotype Anything .....	408
12.2.5	Stereotype Base Unit Type .....	408
12.2.6	Stereotype Classifies.....	408
12.2.7	Stereotype Concept Model .....	409
12.2.8	Stereotype Disjoint With .....	409
12.2.9	Stereotype Enumerates .....	409
12.2.10	Stereotype Equivalent Class .....	409
12.2.11	Stereotype Equivalent Property .....	409
12.2.12	Stereotype Equivalent To .....	410
12.2.13	Stereotype External Reference.....	410

12.2.14	Stereotype Has Value .....	411
12.2.15	Stereotype Information Model.....	411
12.2.16	Stereotype Intersection .....	411
12.2.17	Stereotype Is In Context .....	412
12.2.18	Stereotype Model.....	412
12.2.19	Stereotype Phase.....	412
12.2.20	Stereotype Quantity Kind .....	412
12.2.21	Stereotype Resource .....	413
12.2.22	Stereotype Role.....	413
12.2.23	Stereotype Sufficient.....	413
12.2.24	Stereotype Synonym.....	413
12.2.25	Stereotype Union .....	413
12.2.26	Stereotype Unit Type .....	414
12.2.27	Stereotype Value Type .....	415
12.3	UML Profile – SIMF Rules & Model Mapping Semantics .....	416
12.3.1	Structure of Rule Specifications .....	416
12.3.2	Rule Model 416	
12.3.3	Representations.....	417
12.3.4	Mapping Rules.....	418
12.3.5	<<Match>> Elements .....	419
12.3.6	Pattern element traversals and patterns.....	420
12.3.7	Multiplicity constraints in patterns .....	421
12.3.8	Subsets of Pattern Elements.....	422
12.3.9	<<Pattern Element>> computations and constraints.....	425
12.3.10	<<Pattern Element>> strength.....	425
12.3.11	<<Pattern Element>> strength=Assert.....	426
12.3.12	<<Pattern Element>> strength=Exists .....	426
12.3.13	<<Pattern Element>> strength=Default.....	426
12.3.14	<<Pattern Element>> quantifier .....	427
12.3.15	<<Pattern Element>> explicit.....	428
12.3.16	Property Chains .....	429
12.3.17	Pattern Precedence.....	430
12.3.18	Generic Rules .....	431
12.3.19	Facades and Representation Computations.....	431
12.4	SIMF Profile::SIMF Rules Profile Reference .....	434
12.4.1	Diagram SIMF Rules Profile .....	434
12.4.2	Stereotype Facade.....	434

12.4.3	Stereotype Map.....	435
12.4.4	Stereotype Mapping Rule .....	436
12.4.5	Stereotype Match .....	436
12.4.6	Stereotype Pattern Element.....	436
12.4.7	Enumeration Pattern Element Strength.....	437
12.4.8	Enumeration Quantifier .....	438
12.4.9	Stereotype Represents.....	438
12.4.10	Stereotype Rule.....	439
12.4.11	Stereotype Rule Model .....	439
12.4.12	Stereotype Subset of .....	440
12.4.13	Stereotype Subsumes .....	440
12.5	SIMF Profile::SIMF Computation Rules.....	440
12.5.1	Diagram SIMF Computation Rules .....	441
12.5.2	Class ExistsRule .....	441
12.5.3	Class List First .....	441
12.5.4	Class MapID442	
12.5.5	Class Rule Computation .....	442
12.5.6	Class Summarize.....	442
13	Concept Index.....	443

# 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](mailto: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](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**

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 models	
6.5.1.1 Submissions shall define modular UML conceptual models to specify the concepts required to represent information about operational threats and risks.	The conceptual models are specified in section 8, <a href="#">Conceptual Model Specification (Normative)</a>
6.5.1.2 The conceptual 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 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 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 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 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 <a href="#">glossary</a> .
6.5.2.2 Proposal's conceptual 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 <a href="#">the terms may be slightly different</a> .
6.5.2.3 The concepts of threats shall include the following classifications: <ul style="list-style-type: none"><li>• Cyber/information and communication systems and assets</li><li>• Physical systems and assets, including embedded and manufacturing</li><li>• Electromagnetic spectrum assets (E.g., interference with wireless systems or radio)</li><li>• Industrial control systems</li></ul>	Categories are provided for all identified classifications in section 8.32. Others have <a href="#">been be added as extensions</a> .

<p>6.5.2.4 Models for operational threats and risks shall be consistent with the following constraints:</p> <ul style="list-style-type: none"> <li>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.</li> <li>Models must be able to support non-actor threats (such as natural disasters) that will not be associated with any coherent intentions or plans.</li> <li>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.</li> <li>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 &amp; vulnerabilities.</li> </ul>	<p>The model:</p> <ul style="list-style-type: none"> <li>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.</li> <li>Intentional (actor related), natural and systematic threats and risks are supported.</li> <li>Actors in an incident may be non-intentional. I.e. Bystanders and inadvertent actors.</li> <li>Risks are focused on those caused by any danger, including human and non-human.</li> </ul>
<p>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).</p>	<p>Likelihood and confidence metrics are included.</p>
<h3>6.5.3 Risk Management concepts</h3>	
<p>6.5.3.1 The conceptual model shall include concepts related to systematic identification of operational risks and assessing their likelihood and severity.</p>	<p>Operational risks and their likelihood and severity may be represented. This specification does not specify process or methodology.</p>
<p>6.5.3.2 The proposals shall include concepts related to prioritization of risks.</p>	<p>Risks may be rated as to their priority.</p>
<p>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.</p>	<p>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.</p>
<p>6.5.3.4 The proposals shall describe concepts related to exchange of risk indicators, including patterns for systematic identification of risks.</p>	<p><b>Indicators and patterns are included;</b> see “pattern” (8.4) and “indicator” (8.37).</p>
<h3>6.5.4 Mitigation and courses of action</h3>	
<p>6.5.4.1 The conceptual models shall include concepts of “course of action” and mitigation of threats and risks.</p> <p>Explanation: Coincident with understanding any threat or risk is taking steps to mitigate the specific threat and</p>	<p>Course of action rules are included (8.39).</p>

mitigate similar risks in the future. The conceptual 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 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 models as defined above.	A NIEM mapping is provided in section 10.
6.5.6.2 This NIEM-UML representation shall be mapped to the conceptual models such that the meaning of each threat/risk relevant NIEM element is described in the conceptual model.	A NIEM mapping is provided in section 10.
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 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 have been defined in section 10.
6.5.6.4 Any instance of the NIEM specification shall be able to be logically mapped to the conceptual 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. This mapping shall demonstrate that the conceptual model is sufficient to represent high-level STIX concepts.	A STIX mapping of common concepts and their representation in STIX is included in clause 9.
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 and mappings. Profiles are specified for conceptual modeling and mapping in section 11. The profile is consistent with the proposed SIMF specification.
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 models are sub-divided 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"><li>o OASIS Common Alerting Program &amp; EDXL</li><li>o Others as deemed important by submitters</li></ul>	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 modeling and mapping  Submissions may reference and/or define non-normative UML profiles and associated QVT (or other ways to express mapping logic) for conceptual modeling and the mapping.  Submitters are encouraged to follow the progress of and use as appropriate SIMF, ODM, MDMI, semantic web and other efforts to help define conceptual model and mappings.	A UML profile corresponding to the UML profile in SIMF is included in section 11.
6.6.3 Optional MOF representation  Submissions may define A MOF metamodel that utilizes the conceptual 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 <b>DoDAF concepts</b> but a complete DoDAF mapping and integration of concepts is not provided.

## 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 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 to their internal simulation data structure.**

### 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 provide the foundation for threats and risks but are not threat and risk specific. These 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 make a viable foundation for a general purpose information sharing and federation model.

### 6.7.3 Design choices

Submissions shall discuss their design choices for level of detail.

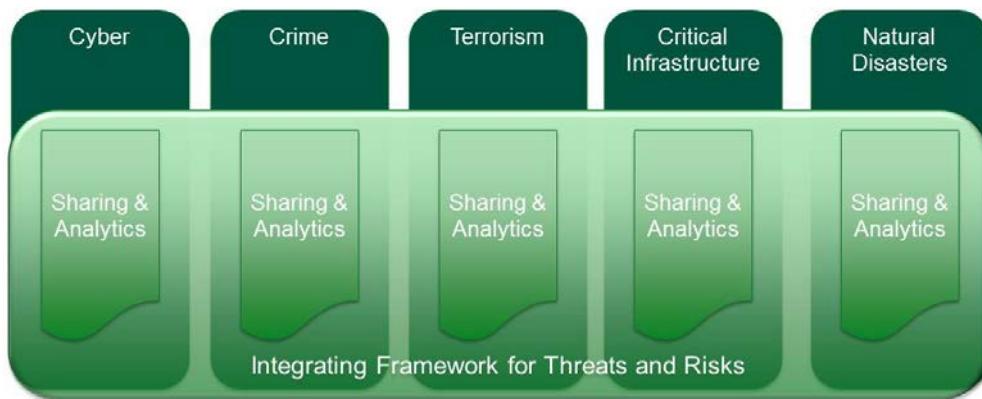
We looked for the level of detail that corresponds to information to be shared both across domains and disciplines.

## 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 organization, 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 Information Modeling for Federation [SIMF] 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 all of the concepts defined in the conceptual 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.

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 Mapping conformance**

A data format 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
- Fulfils either canonical model conformance or mapping conformance to one of the normative mappings: STIX or NIEM
- Demonstrates the input and/or output of threat/risk concepts

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 and comprehend that data in terms of the conceptual model, or,
- Produce STIX data from information comprehended based on the conceptual Model
- Fulfill 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 and comprehend that data in terms of the conceptual model, or,
- Produce NIEM data from information comprehended based on the conceptual Model
- Fulfill either canonical model conformance or conformance to another conformant mapping.

# 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) <b>Superstructure</b> v2.5 <a href="http://www.omg.org/spec/UML/2.5/">http://www.omg.org/spec/UML/2.5/</a>
[OMG MDA Guide]	<a href="http://www.omg.org/cgi-bin/doc?ormsc/14-06-01">http://www.omg.org/cgi-bin/doc?ormsc/14-06-01</a>
[BMM]	<a href="http://www.omg.org/spec/BMM/1.3/">http://www.omg.org/spec/BMM/1.3/</a>
[STIX]	<a href="https://stix.mitre.org/language/version1.2/index.html">https://stix.mitre.org/language/version1.2/index.html</a>
[NIEM]	NIEM-UML 3 Specification <a href="http://www.omg.org/spec/NIEM-UML/3.0/Beta1">http://www.omg.org/spec/NIEM-UML/3.0/Beta1</a>
[EDXL]	<a href="http://docs.oasis-open.org/emergency/">http://docs.oasis-open.org/emergency/</a>
[SI]	<a href="http://www.bipm.org/en/measurement-units/">http://www.bipm.org/en/measurement-units/</a>
[CVSS]	<a href="https://nvd.nist.gov/cvss.cfm">https://nvd.nist.gov/cvss.cfm</a>
[CAP]	<a href="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html">http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html</a>
[CNSSI 4009]	<a href="https://www.cnss.gov/CNSS/issuances/instructions.cfm">https://www.cnss.gov/CNSS/issuances/instructions.cfm</a>
[WGS-84]	<a href="http://earth-info.nga.mil/GandG/wgs84/">http://earth-info.nga.mil/GandG/wgs84/</a>
[OGC]	<a href="http://www.opengeospatial.org/">http://www.opengeospatial.org/</a>
[NRC]	<a href="http://www.nrc.gov/">http://www.nrc.gov/</a>
[DoDAF 2.0]	<a href="http://dodcio.defense.gov/Library/DoDArchitectureFramework.aspx">http://dodcio.defense.gov/Library/DoDArchitectureFramework.aspx</a>
[ISO 73:2009]	ISO Guide 73:2009 provides the definitions of generic terms related to risk management. <a href="http://www.iso.org/iso/catalogue_detail?csnumber=44651">http://www.iso.org/iso/catalogue_detail?csnumber=44651</a>
[NIST-SI]	<a href="http://physics.nist.gov/cuu/pdf/sp811.pdf">http://physics.nist.gov/cuu/pdf/sp811.pdf</a>
[NIST-UNITS]	<a href="http://www.nist.gov/pml/wmd/pubs/upload/AppC-12-hb44-final.pdf">http://www.nist.gov/pml/wmd/pubs/upload/AppC-12-hb44-final.pdf</a>
[NIST-800]	<a href="http://csrc.nist.gov/publications/PubsSPs.html">http://csrc.nist.gov/publications/PubsSPs.html</a>
[QODT]	<a href="http://www.qudt.org/">http://www.qudt.org/</a>

## 3.2 Non-normative References

[DICTIONARY.COM]	<a href="http://dictionary.com">http://dictionary.com</a>
------------------	---

[Firesmith 2003]

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

[SIMF]

[OMG Document AD/2016-05-02](#)

## 4 Terms and Definitions

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

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

**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.

**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** 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** of concern, activity or knowledge.

**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 the relevance, trust or belief in facts is open to interpretation.

Additional terms are defined in the model, clause 8.

## 5 Symbols

There are no symbols defined in this specification.

## 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 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** to then build capabilities that are able to 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 order<sup>1</sup> 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.

<sup>1</sup> <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](#).

### 7.2.1 Federated analytics and simulation capabilities

Federated analytics and simulation [is](#) intended to pull information from multiple unrelated sources *and make sense of them together*. This includes “connecting the dots” use cases, [fusion centers](#), 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

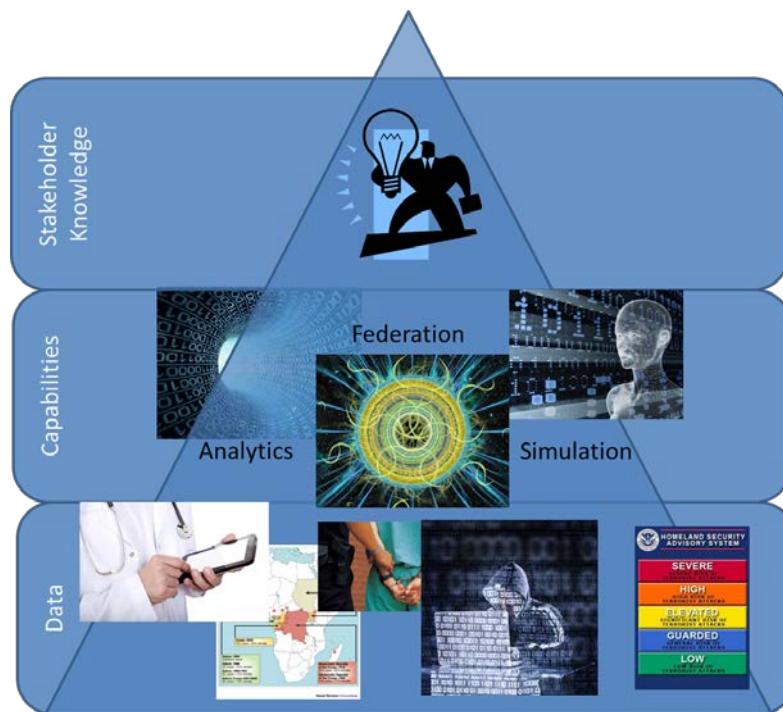


Figure 2 Federating Capabilities

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 will use the conceptual 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 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
- 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.

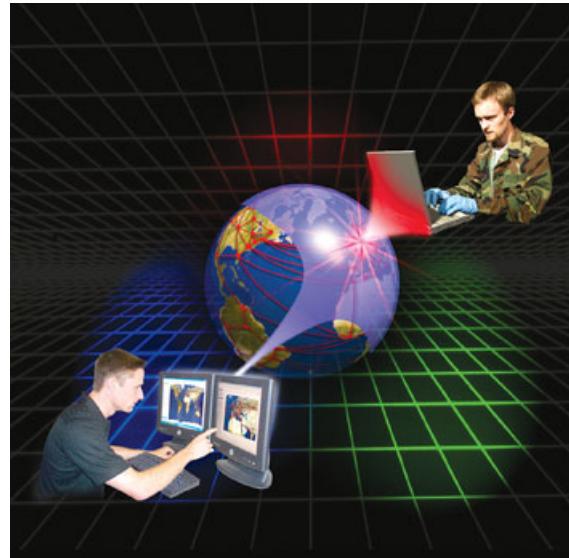


Figure 3 Information Sharing

Translators are nothing new –Saint Jerome (4<sup>th</sup> 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.

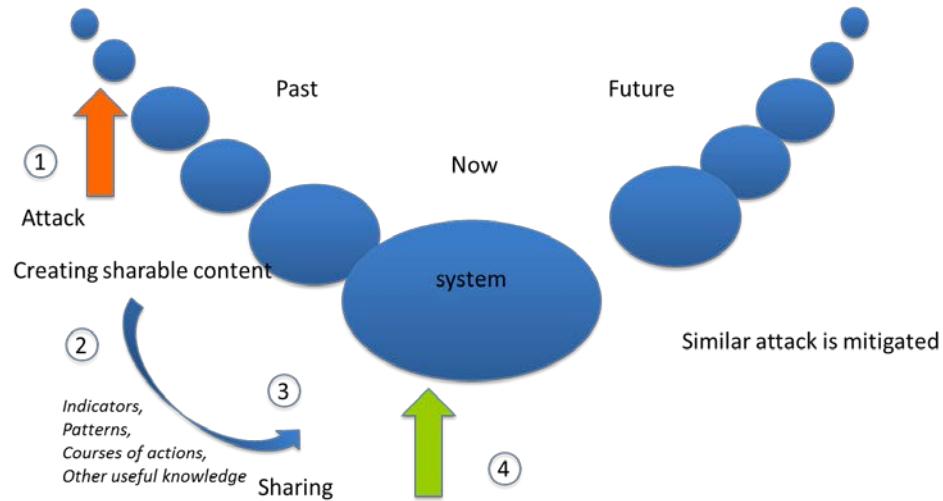
## 7.2.3 Risk Analytics Capabilities

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 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**

## 7.3 Approaches 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 approach.

### 7.3.1 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.

### 7.3.2 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.

### 7.3.3 Semantic federation and translation

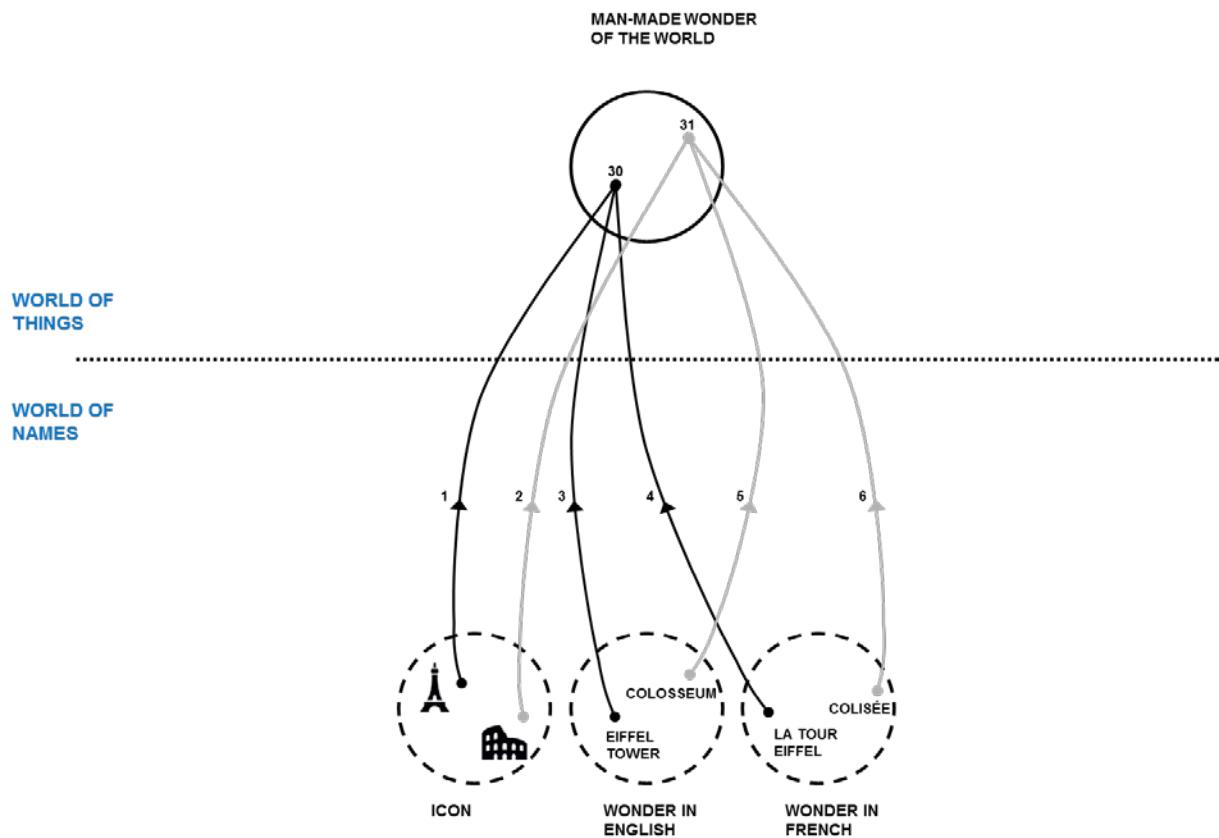
The semantic approach is the one leveraged in this specification. A semantic approach focuses on concepts and their meaning, not how they are represented in any particular syntax, vocabulary, or technology. Mappings then define how various data formats and vocabularies *represent* those concepts. Concepts are well defined in a conceptual model – a more precise way to define a vocabulary or taxonomy. Conceptual models may be called “ontologies”, but some ontologies are essentially programs and not conceptual. The essential difference between a conceptual model and any of the syntactic forms above is that it describes the real world things and their relationship as understood by stakeholders. It is a *model of the world*<sup>2</sup>, 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.

These real-world concepts are the pivot points between different ways to name, describe or talk about them. 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.

---

<sup>2</sup> Or more generally, real or possible worlds.



**Figure 5. the World vs. Names**

How do we know it's the same thing? While 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 thing. 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 model has some similarities to a canonical data format in that it attempts to capture cross-stakeholder information needs – but it abstracts above the 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.**

*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 [SIMF] submission** for this purpose.

## 7.4 Defining and Leveraging Conceptual Models

This section is intended to introduce the approach taken to express the risk and threat conceptual models and how the concepts are layered, modularized and organized.

### 7.4.1 Expressing conceptual models

As stated in 7.4.3, conceptual models are models of the world – or at least how communities conceive it. 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*<sup>3</sup> are conceptual models, however not all ontologies or ontology languages are conceptual. Of course, human natural languages are the most common way to express concepts.

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 modeling and mapping.

Our goal in this specification is to utilize a conceptual model as the pivot point between different data models and syntaxes for expressing information about real-world threats and risks. While using a conceptual 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 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 Information Modeling for Federation (SIMF). UML is a well-accepted modeling language with widely available resources – SIMF provides a standard way to use UML (and other languages) for the purpose of conceptual modeling and mapping. The combination of UML and the SIMF profile provides an expressive, well supported way to express the conceptual models and mappings. The SIMF profile is included in this specification as a non-normative appendix and therefore does not depend on SIMF being standardized. Any standard conformant UML tool can import and manage the profile and the conceptual model.

The intent of the conceptual 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 implemented*. In addition, this specification makes no assumption about a new “intermediate data format” based on the conceptual model- the conceptual 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 Web<sup>4</sup>” 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

---

<sup>3</sup> *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](http://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.

<sup>4</sup> 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/>]

well suited to data federation. The conceptual model can be mapped to semantic web technologies generated from the conceptual model based on the SIMF specification.

#### 7.4.2 Layering

The conceptual 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 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.** The same layering supports reuse of these more general concepts for other conceptual models.



**Figure 6 Conceptual Model Layering**

The above illustration shows the conceptual model layering.

- **Foundational Concepts:** The foundational concept library defines basic constructs for conceptual modeling such as ideas of entities, roles, types, and identifiers. Any model is expected to use these concepts.
- **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.
- **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.**

#### 7.4.3 Source of concepts

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

- NIEM
- STIX
- NIST 800 Series
- ISO 8000 and NIST Units
- EDXL

Due to the multiple inputs, none match exactly. Every effort has been made to retain the semantics of the concepts and synthesize them.

## 7.5 Top Level Concepts

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). All concepts can be organized into hierarchies. These hierarchies result in some “top level” 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.

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 is being defined we connect it to the most general entity concept (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 it is a general concept, classes it relates are general concepts as well.** Properly representing these general concepts **naturally** introduces a hierarchy of other general concepts as are found in the generic concept library.

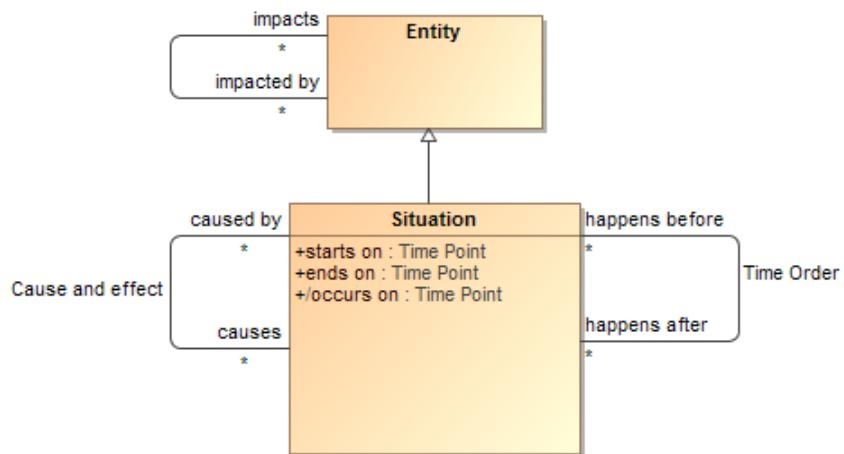


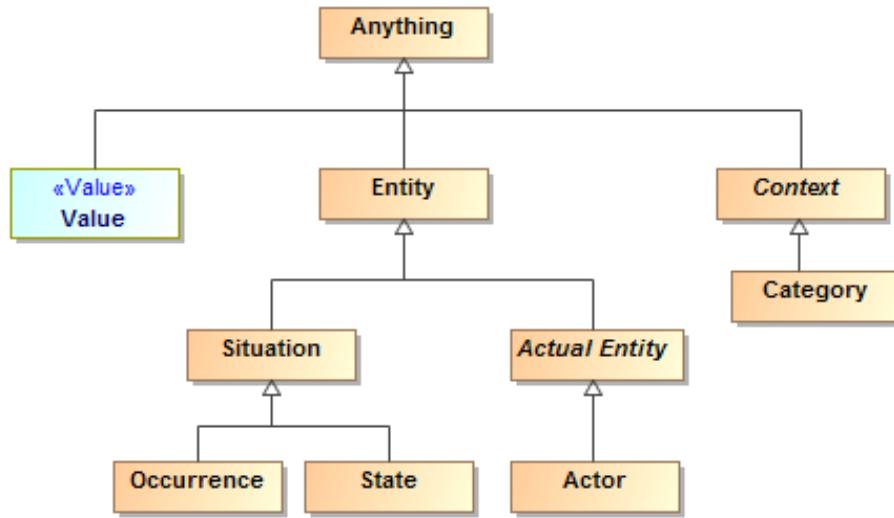
Figure 7. Example of Top Level Classes

The above example shows some of the top level **class 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.

### The top level hierarchy

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



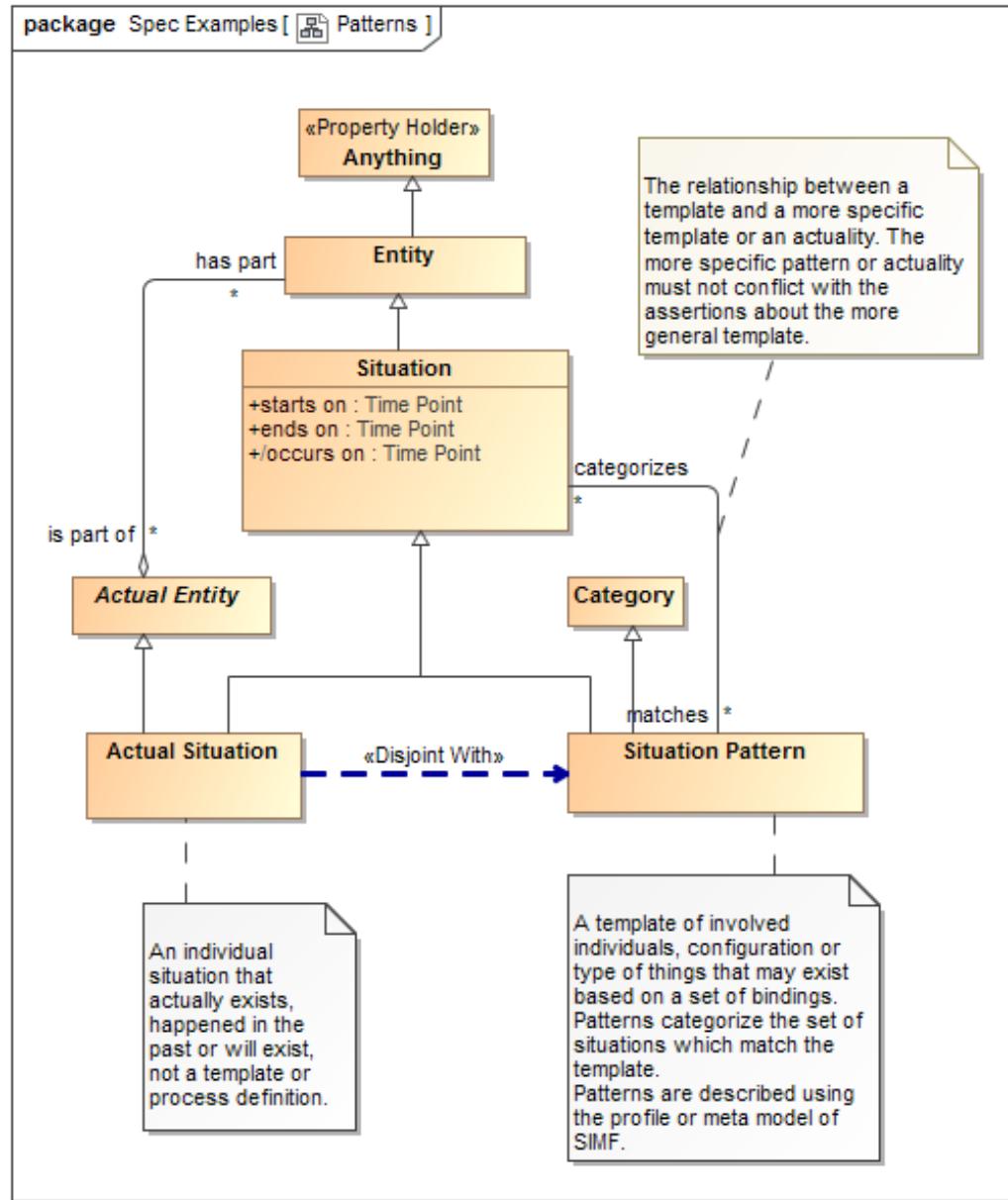
**Figure 8. Top Level Classes**

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 **a** 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 supertypes are part of that concepts definition.

## Templates and actual situations



**Figure 9. Situation Patterns**

Fundamental concepts in the conceptual 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.

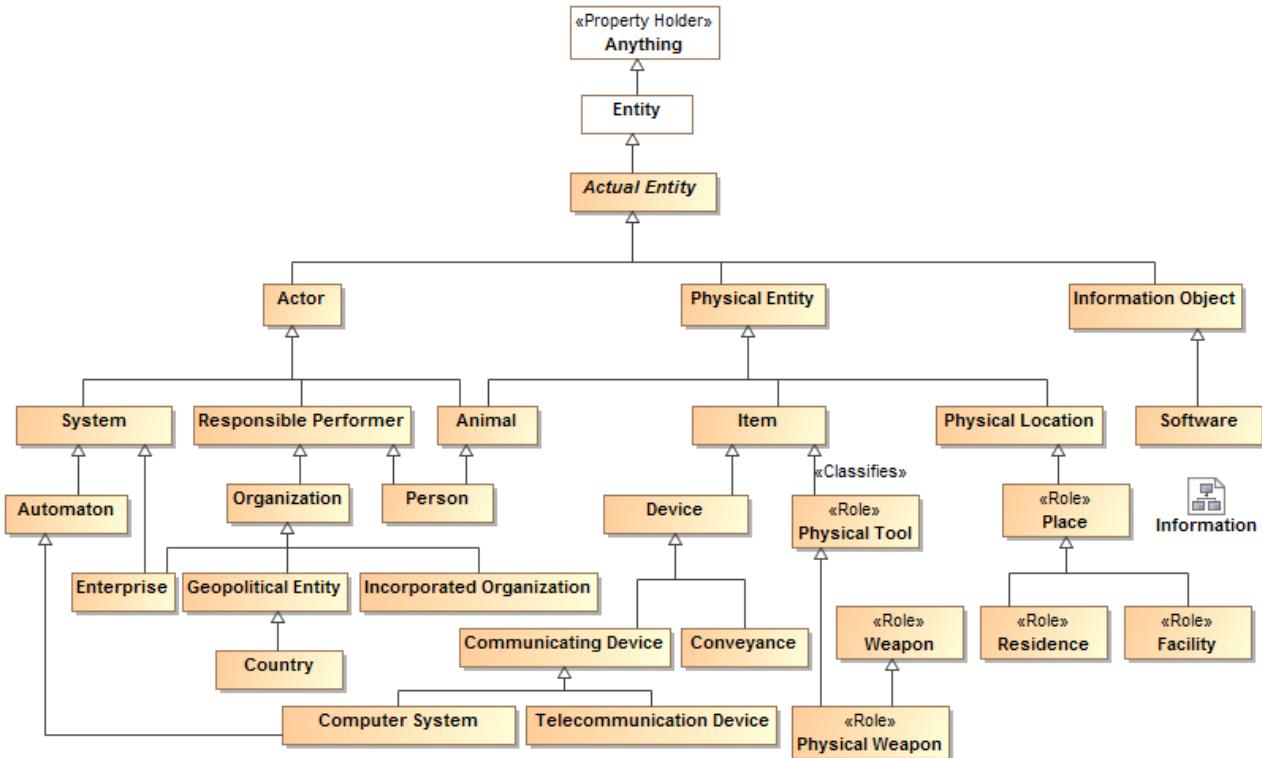
While patterns and actual situations are quite different, what can be said about them is very similar. While a pattern has variables it also has some constants – the things that are the same across all the actual situations that describe it.

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 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.

## 7.6 Mixing Concepts with “multiple classification”

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 class. In most software languages such an object can only be a member of one class and that class if 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 **police officer** could also be in the role of a victim in some incident.

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** 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 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 Conceptual Model Specification (Normative)

This section specifies the threat/risk conceptual model.

## 8.1 Threat-risk-conceptual-model::Foundational Concepts

The foundational concept library provides concepts that are the foundation for more specialized concepts and are likely to be utilized to express any domain model.

### 8.1.1 Diagram: Core Concept Library

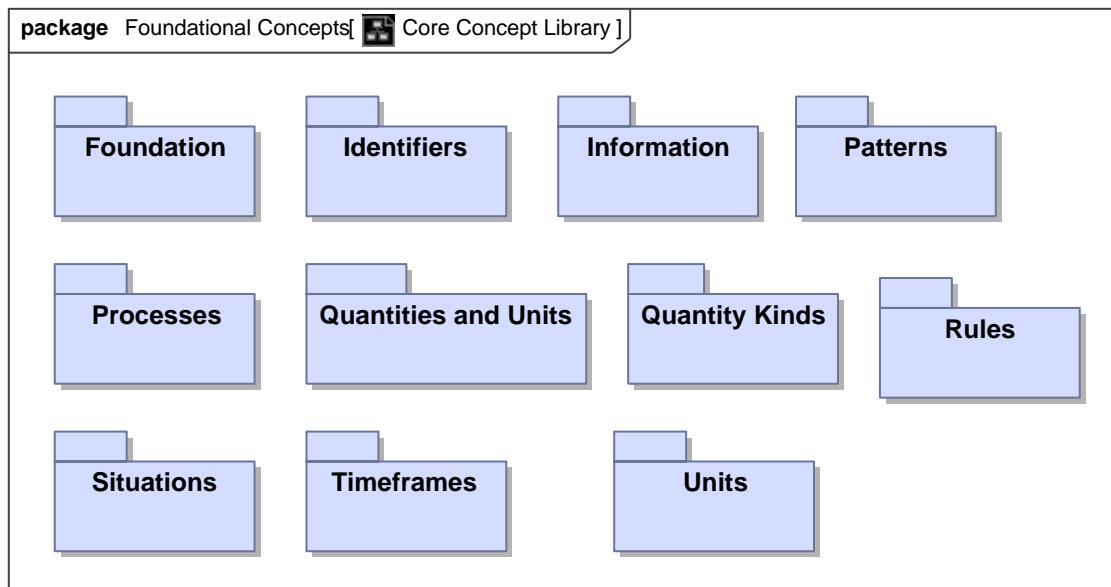


Figure 1. Core Concept Library

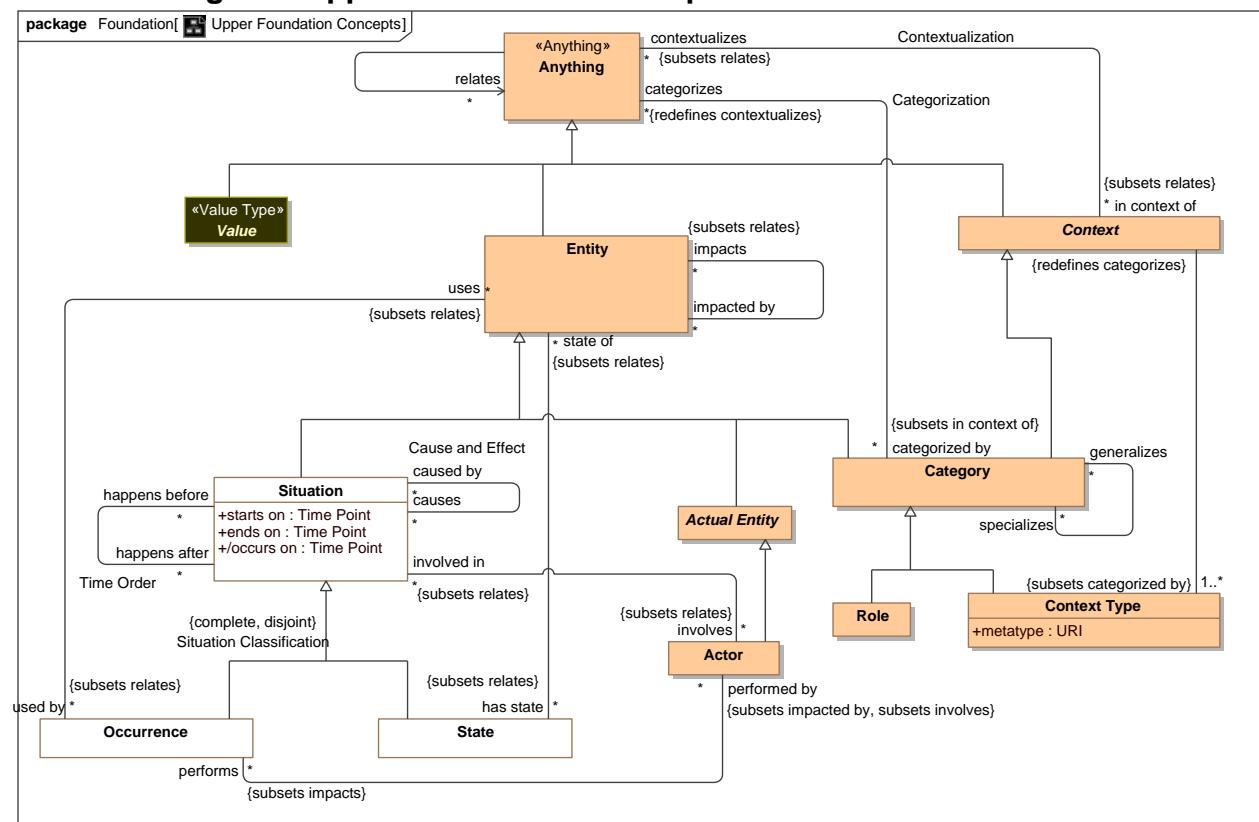
## **8.2 Threat-risk-conceptual-model::Foundational Concepts::Foundation**

The foundation library provides fundamental concepts that apply to any domain or area of concern. These fundamental concepts are specialized and related for more specific concerns, such as risk management.

Such 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" - 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).

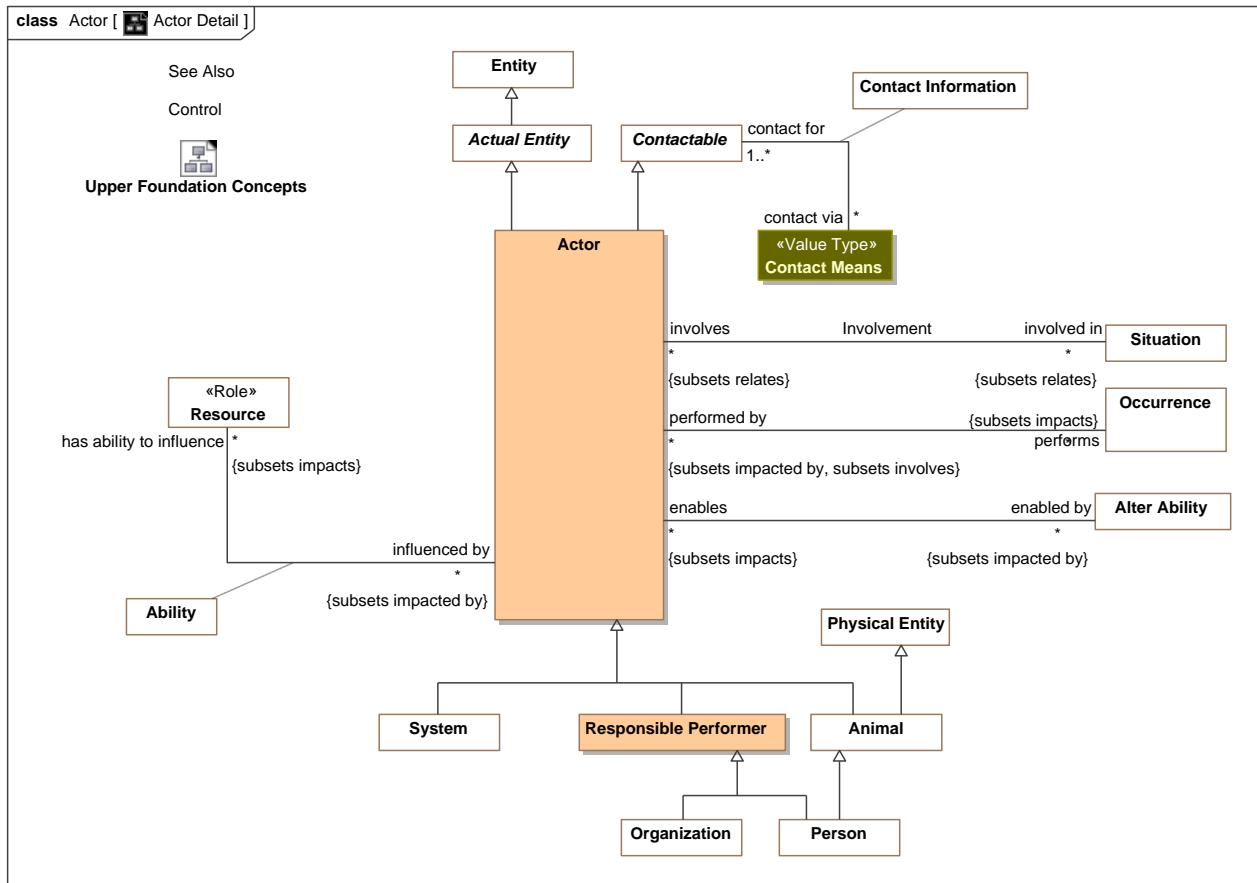
### **8.2.1 Diagram: Upper Foundation Concepts**



**Figure 2.** Upper Foundation Concepts

### 8.2.2 Class Actor

An entity capable of behavior - acting in a process.



**Figure 1.** Actor Detail

## 8.2.21 Direct Supertypes

#### Actual Entity, Contactable

## **package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

## 8.2.22 Associations

/ operates at : **Place** [\*] Subsets: has ability to influence: **Resource**

#### Locations where actors perform acts

/ enabled by : **Alter Ability** [\*] Subsets: impacted by:**Entity**

An occurrence that enables an actor's capability.

## ✓ · Activity

✓ · Managed Identifier [\*]

/ performs : Occurrence [\*] Subsets; impacts; Entity

An activity an actor performs

/ involved in : [Situation](#) [\*] Subsets: relates; [Anything](#)

Situations in which an actor has any kind of involvement

 has ability to : [Process](#) [\*] Subsets: has ability to influence: [Resource](#) performs: [Occurrence](#)

The ability of an actor to perform a process.

 has permission to perform : [Process](#) [\*] Subsets: has ability to: [Process](#) performs: [Occurrence](#)

Process actor has the permission to perform.

 recved via : [Transfer](#) [\*]

action that receives something

 sent via : [Transfer](#) [\*]

Action that sends something

### 8.2.3 Class Actual Entity

An actual entity is an identifiable and individual person, specific object, process, agreement, etc. Actual Individuals do not have to be physical but do not include types, categories or values.

A more specific class of thing (e.g., Person) is intended [to also classify](#) the individual thing.

Individuality (or selfhood) is the state or quality of being an individual; particularly of being [a](#) separate from other individuals and [possessing](#) identity. Individuals typically have a lifetime and [may change](#) over that lifetime. Individuals may have parts [and processes](#) that together help define the individual but may change over time. Also known as "Endurant" in [BFO].

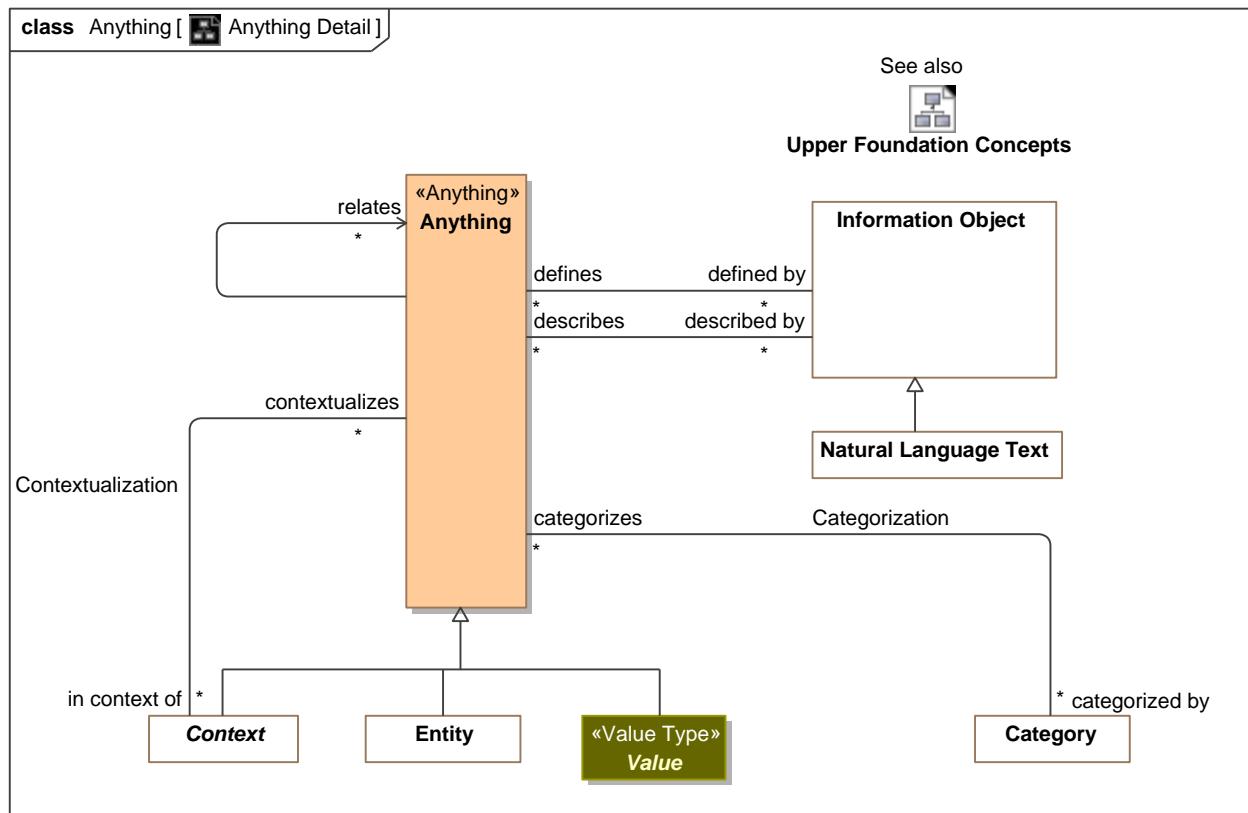
#### 8.2.31 Direct Supertypes

[Entity](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

### 8.2.4 Class Anything

Any thing or value that does or may exist in any possible world. *Anything* is the supertype of all types and may therefore participate in [unbounded relations](#).



**Figure 2. Anything Detail**

**package Threat-risk-conceptual-model::Foundational Concepts::Foundation**

### 8.2.41 Attributes

 modelElementID : [URI](#)

Identity of the information in a model at the granularity of a single element.

### 8.2.42 Associations

 in context of : [Context](#) [\*] Subsets: relates:[Anything](#)

Context that contextualizes something.

 defined by : [Information Object](#) [\*]

Natural language definitions of something.

 described by : [Information Object](#) [\*]

A description for some concept.

 relates : [Information Object](#) [\*]

A generic relation to capture arbitrary relations that do not have more specific meaning. <relates> is the implicit supertype of all relations between entities - **this subset constraint** is not shown on all diagrams.

 categorized by : [Category](#) [\*] Subsets: in context of:[Context](#)

The category(s) that categorize something. Categories include types.

## 8.2.5 Association Categorization

Categorization states that something is categorized by the category. Categorization also represents the "instance" of a type.

Each category has a <categorizes> set of anything so categorized. The constraints for set membership may or may not be formally stated.

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

### 8.2.5.1 Association Ends

/ categorizes : [Anything](#) [\*] Subsets: in context of:[Context](#)

The set of "instances" categorized by a category or type. The extent of the category.

/ categorized by : [Category](#) [\*] Subsets: in context of:[Context](#)

The category(s) that categorize something. Categories include types.

## 8.2.6 Class Category

An arbitrary grouping of anything. A category is an asserted context - one defined by some authority or actor.

### 8.2.6.1 Direct Supertypes

[Context](#), [Entity](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

### 8.2.6.2 Associations

/ categorizes : [Anything](#) [\*] Redefines: contextualizes:[Anything](#)

The set of "instances" categorized by a category or type. The extent of the category.

/ generalizes : [Anything](#) [\*] Redefines: contextualizes:[Anything](#)

The more general role of a generalization.

/ specializes : [Anything](#) [\*] Redefines: contextualizes:[Anything](#)

The more specific role of a generalization.

/ types : [Pattern Property](#) [\*]

The properties typed by a category.

## 8.2.7 Class Context

A grouping of concepts with some commonality and with some common attributes facts and/or relations. Rules defined for a context are true for anything contextualized by that context.

### 8.2.71 Direct Supertypes

Anything

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

### 8.2.72 Associations

/ contextualizes : Anything [\*] Subsets: relates:Anything

Anything a context contextualizes.

/ : Context Type [1..\*] Subsets: categorized by:Category

/ has rule : Rule [\*] Subsets: contextualizes:Anything

A rule asserted within a context.

## 8.2.8 Class Context Type

Context type is a way to group related categories, context or types. A category of categories - related to the concept "power type" or "power set". e.g., "Locale" could be a context type for a set of locations that define certain rules or geopolitical rules.

### 8.2.81 Direct Supertypes

Category

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

### 8.2.82 Attributes

◊ metatype : URI

Reference to a type in a model where instances of the context type must categorize this metatype. e.g., the kind of thing that can be categorized.

### 8.2.83 Associations

/ : Context Redefines: categorizes:Anything

## 8.2.9 Association Contextualization

Contextualization says that the thing contextualized is subject to the facts about the context it is in context of.

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

### 8.2.91 Association Ends

/ contextualizes : Anything [\*] Redefines: categorizes: Anything

Anything a context contextualizes.

/ in context of : Context [\*] Redefines: categorizes: Anything

Context that contextualizes something.

## 8.2.10 Class Entity

Anything identifiable that may change over time (or the extent may change over time). This includes: person, place, thing, agreement, situation, events, context, category, and type.

Distinguished from Values.

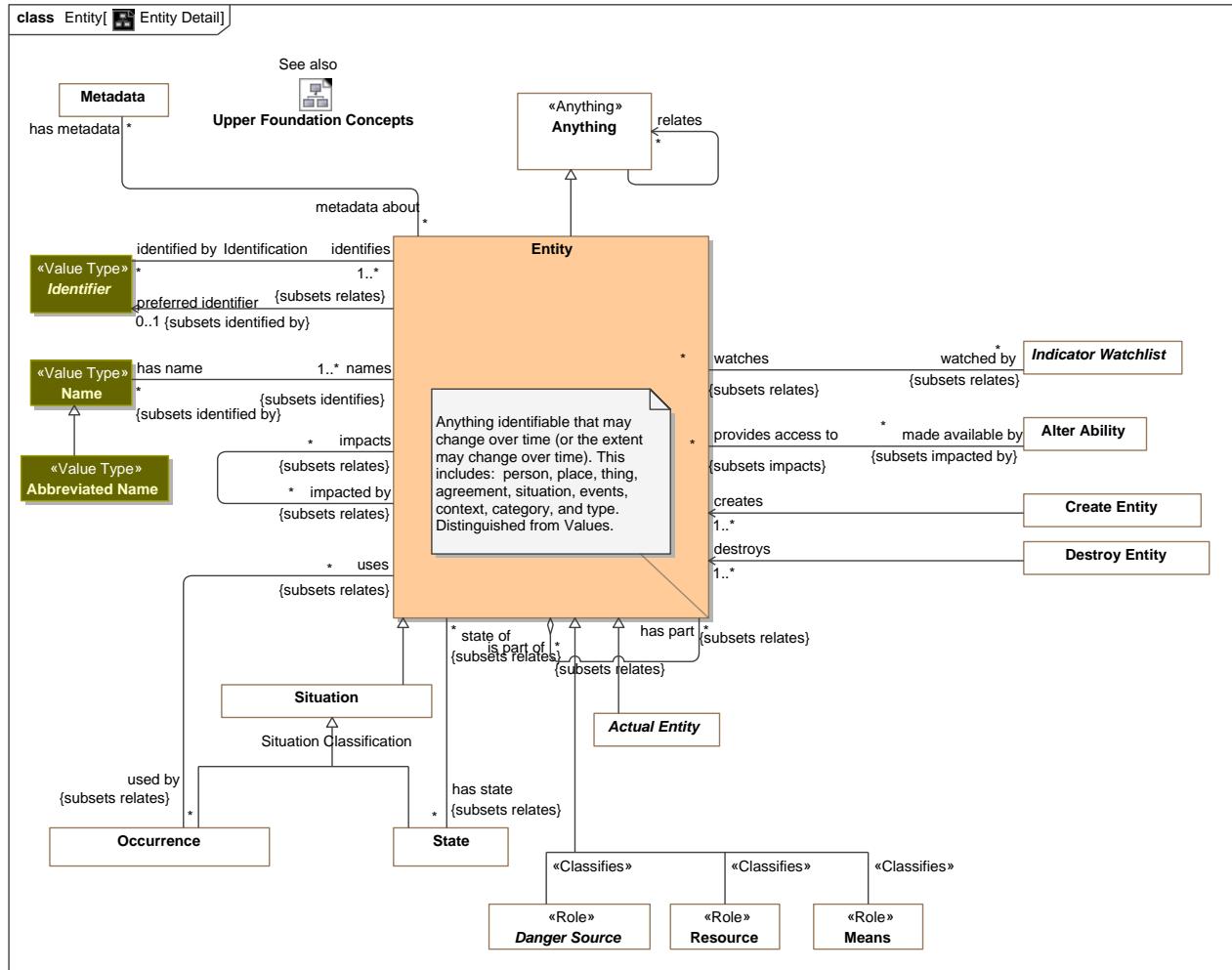


Figure 3. Entity Detail

### 8.2.101 Direct Supertypes

[Anything](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

### 8.2.102 Associations

used by : [Occurrence](#) [\*] Subsets: relates:[Anything](#)

Occurrences used by an occurrence.

is part of : [Occurrence](#) [\*] Subsets: relates:[Anything](#)

Composite entity of which this entity is a part.

- / has state : [State](#) [\*] Subsets: relates:[Anything](#)  
 States (or snapshots) of an entity over its lifetime.
  - / impacted by : [State](#) [\*] Subsets: relates:[Anything](#)  
 Entities that impact another entity.
  - / has name : [Name](#) [\*] Subsets: identified by:[Identifier](#)  
 A name for the entity
  - / watched by : [Indicator Watchlist](#) [\*] Subsets: relates:[Anything](#)  
 Watch lists an entity is in.
  - / made available by : [Alter Ability](#) [\*] Subsets: impacted by:[Entity](#)  
 An act that makes an entity available to an actor as a resource.
  - / has metadata : [Metadata](#) [\*]  
 Metadata associated with information about an entity
  - / subject to : [Metric](#)  
 A rule that must be satisfied by an entity.
    - ↗ preferred identifier : [Identifier](#) [0..1] Subsets: identified by:[Identifier](#)  
 Most common identifier for an entity.
    - / identified by : [Identifier](#) [\*]  
 Identifiers for a concept - note that a concept may have multiple identifiers and they may be context specific.
    - / impacts : [Identifier](#) [\*]  
 Things an entity may affect.
      - ↗ has confidence : [Confidence](#) [0..1] Subsets: has metadata:[Metadata](#)  
 Confidence is metadata reflecting the trust that the facts about the entity are valid.
      - / sourced from : [Statement](#) [\*] Subsets: has metadata:[Metadata](#)  
 Source of information about an entity or a particular situation or fact.
      - / has observation : [Observation](#) [\*] Subsets: used by:[Occurrence](#)  
 Observations made about an entity.
      - / has indicator : [Indicator](#) [\*] Subsets: contextualizes:[Anything](#)  
 Indicators that suggest patterns of information about an entity
      - / affected by : [Action On Entity](#) [\*] Subsets: impacted by:[Entity](#)  
 Actions that can cause some change in the entity.
      - / transferred by : [Transfer](#) [\*] Subsets: impacted by:[Entity](#)  
 Transfers of the entity between actors.
        - / has part : [Transfer](#) [\*] Subsets: impacted by:[Entity](#)  
 A part of something. This is a general concept of part and does not assume exclusivity of partness or total part inclusion.

### **8.2.11 Association Generalization**

The set of instances contextualized by the specialized context is a subset of the set of instances contextualized by the generalized context.

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

#### **8.2.11.1 Association Ends**

 generalizes : [Category](#) [\*] Subsets: impacted by:[Entity](#)

The more general role of a generalization.

 specializes : [Category](#) [\*] Subsets: impacted by:[Entity](#)

The more specific role of a generalization.

### **8.2.12 Association Involvement**

The relation between an actor and situations they are involved in.

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

#### **8.2.12.1 Association Ends**

 involved in : [Situation](#) [\*] Subsets: impacted by:[Entity](#)

Situations in which an actor has any kind of involvement.

 involves : [Actor](#) [\*] Subsets: impacted by:[Entity](#)

Actors involved in a situation in any way.

### **8.2.13 Class Responsible Performer**

An actor that may have responsibilities - people and organizations.

#### **8.2.13.1 Direct Supertypes**

[Actor](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

#### **8.2.13.2 Associations**

 associate : [Transfer](#) [\*] Subsets: impacted by:[Entity](#)

The actor associated with another.

 associated with : [Transfer](#) [\*] Subsets: impacted by:[Entity](#)

Another actor the actor is associated with.

## **8.2.14 Class Role**

A realized or potential classification of behavior or participation of an entity with respect to some situation, e.g., Joe is teaching class A123 or Joe is a teacher. Entities may have multiple roles that change over time and are typically contextual.

### **8.2.141 Direct Supertypes**

[Category](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Foundation

## **8.3 Threat-risk-conceptual-model::Foundational Concepts::Identifiers**

Identification connects identifiers with the entity they identify. Identifiers are all assumed to be values, that is they are immutable. An entity may be assigned different identifiers over time and may have many at any one time.

The base Identifier class 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 or the relation to an entity may be contextual.

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".

### 8.3.1 Diagram: Identifiers

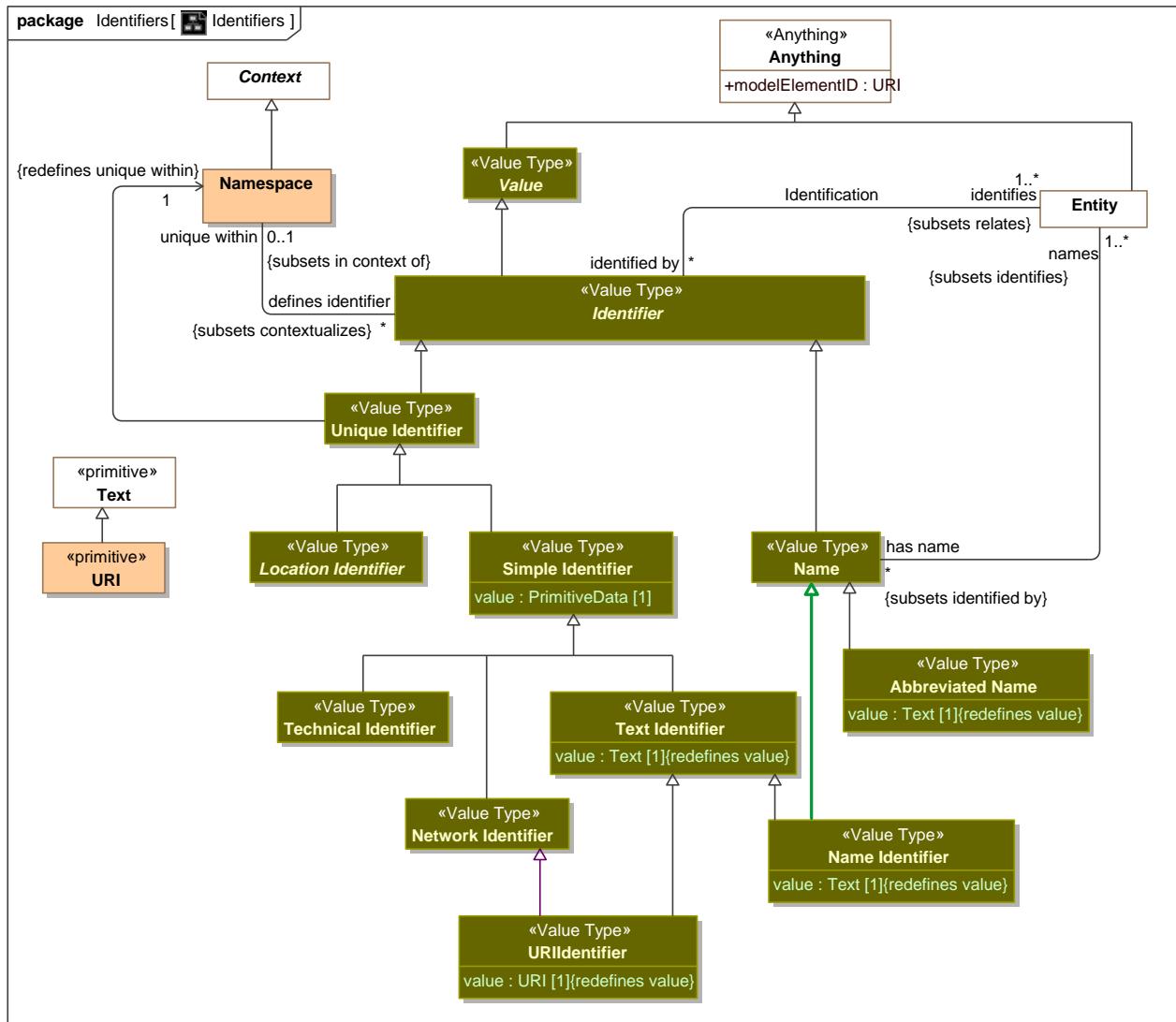


Figure 4. Identifiers

### 8.3.2 Class Abbreviated Name

A short name for something or someone which may not be unique.

#### 8.3.21 Direct Supertypes

[Name](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### 8.3.22 Attributes

◊ value : [Text](#) [1]

The text of a textual identifier.

### 8.3.3 Association Identification

Identification connects an identifier with an entity it identifies. At the top level identification is not necessarily unique, but certain identifiers are unique within a namespace.

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### 8.3.31 Association Ends

/ identifies : [Entity](#) [1..\*] Subsets: impacted by:[Entity](#)

Entity identified by an identifier.

/ identified by : [Identifier](#) [\*] Subsets: impacted by:[Entity](#)

Identifiers for a concept - note that a concept may have multiple identifiers and they may be context specific.

### 8.3.4 Class Identifier

Anything that is used to identify a concept. Note that any identifier may be contextualized by a set of context.

#### 8.3.41 Direct Supertypes

[Value](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### 8.3.42 Associations

/ identifies : [Entity](#) [1..\*] Subsets: relates:[Anything](#)

Entity identified by an identifier.

/ unique within : [Namespace](#) [0..1] Subsets: in context of:[Context](#)

Namespace in which an identifier is unique.

### 8.3.5 Class Name

A word or set of words by which a person, animal, place, or thing is known, addressed, or referred to. Names are not necessarily unique.

#### 8.3.51 Direct Supertypes

[Identifier](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### 8.3.52 Associations

/ names : [Entity](#) [1..\*] Subsets: identifies:[Entity](#)

The named entity.

### **8.3.6 Class Name Identifier**

A human **usable** name unique within **some namespace**.

#### 8.3.6.1 Direct Supertypes

[Name](#), [Text Identifier](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### 8.3.6.2 Attributes

 value : [Text](#) [1]

The text of a name.

### **8.3.7 Class Namespace**

A context that provides a way to make identifiers unique and identify exactly one entity. For example, the Virginia driver's license division provides unique driver's license numbers.

#### 8.3.7.1 Direct Supertypes

[Context](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### 8.3.7.2 Associations

 defines identifier : [Identifier](#) [\*] Subsets: contextualizes:[Anything](#)

Identifiers unique within a namespace.

### **8.3.8 Class Network Identifier**

A text identifier valid within an electronic network.

#### 8.3.8.1 Direct Supertypes

[Simple Identifier](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

### **8.3.9 Class Simple Identifier**

A code or other simple value identifying something as defined in some namespace. Codes may also be names or numbers.

#### 8.3.9.1 Direct Supertypes

[Unique Identifier](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### 8.3.9.2 Attributes

 value : [PrimitiveData](#) [1]

The representation of the identifier as primitive data

### **8.3.10 Class Technical Identifier**

A technical identifier is defined within a closed technical implementation for references and identity within that system or information element. Such identifiers may have no meaning outside of that system.

Typical technical identifiers include inter document "refs", record numbers, etc. The system should be referenced as the namespace.

Technical identifiers are usually but not always textual.

#### **8.3.101 Direct Supertypes**

[Simple Identifier](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

### **8.3.11 Class Text Identifier**

A textual representation of an identifier - e.g., words, phrases or digits.

#### **8.3.111 Direct Supertypes**

[Simple Identifier](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### **8.3.112 Attributes**

 value : [Text](#) [1]

The text of a textual identifier.

### **8.3.12 Class Unique Identifier**

An identifier unique within some context.

#### **8.3.121 Direct Supertypes**

[Identifier](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### **8.3.122 Associations**

 : [Namespace](#) [1] *Redefines:* unique within:[Namespace](#)

### **8.3.13 Class URIIdentifier**

A URI Identifier for a concept unique within the W3C URI system.

#### 8.3.131 Direct Supertypes

[Network Identifier](#), [Text Identifier](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Identifiers

#### 8.3.132 Attributes

 value : [URI](#) [1]

A Universal resource identifier text.

## 8.4 Threat-risk-conceptual-model::Foundational Concepts::Information

Concepts relating to information (including data) about entities.

### 8.4.1 Diagram: Information

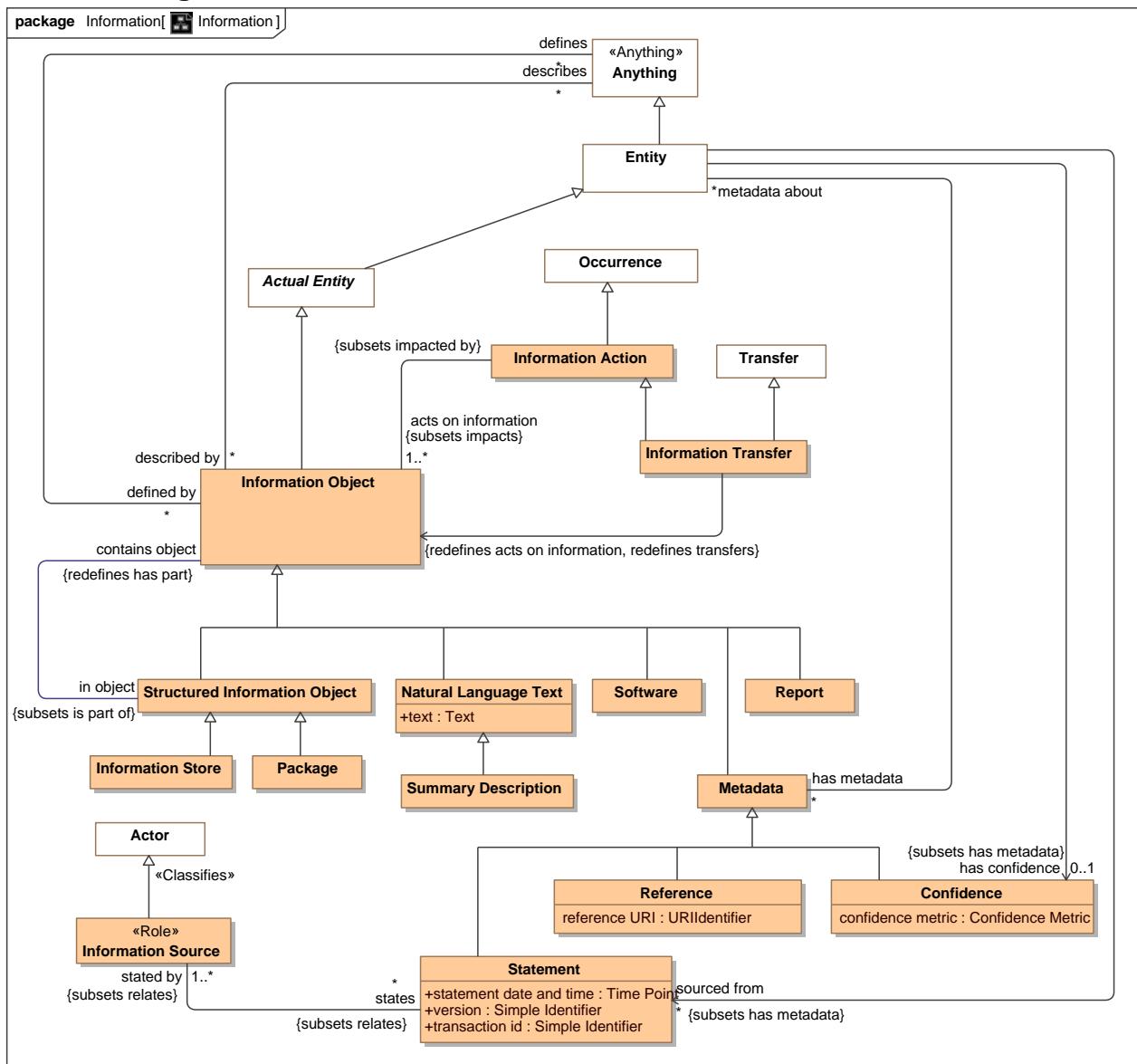


Figure 5. Information

## 8.4.2 Class Confidence

A statement and measure of the confidence in any fact or set of facts about an entity.

### 8.4.21 Direct Supertypes

[Metadata](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

### 8.4.22 Attributes

confidence metric : [Confidence Metric](#)

A metric reflecting confidence.

## 8.4.3 Class Information Action

An action that impacts information objects.

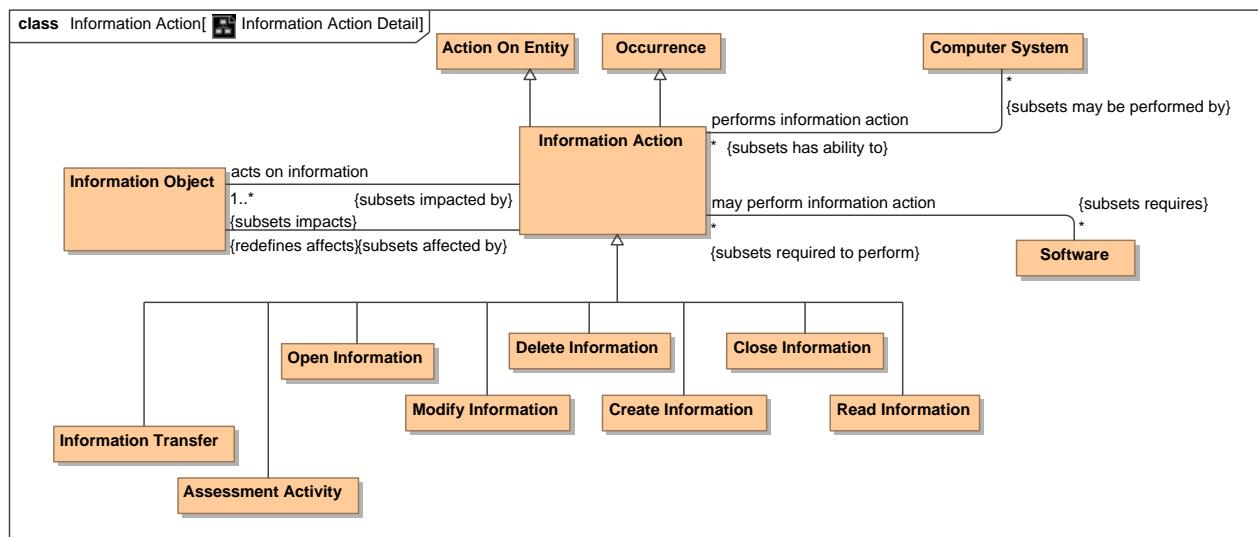


Figure 6. Information Action Detail

### 8.4.31 Direct Supertypes

[Action On Entity](#), [Occurrence](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

### 8.4.32 Associations

/ acts on information : [Information Object](#) [1..\*] Subsets: impacts:[Entity](#)

The information that is created, updated or deleted by an information action.

/ : [Computer System](#) [\*] Subsets: may be performed by:[Actor](#)

/ : [Software](#) [\*] Subsets: requires:[Resource](#)

/ : [Information Object](#) Redefines: affects:[Entity](#)

#### **8.4.4 Class Information Object**

A representation of information/ data/ facts/ assertions/ statements about anything.

##### **8.4.4.1 Direct Supertypes**

Actual Entity

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

##### **8.4.4.2 Associations**

/ in object : Structured Information Object Subsets: is part of:Entity

Where an information object is used within another information object.

/ : Information Action Subsets: impacted by:Entity

/ describes : Anything [\*]

The concept described by an information object.

/ defines : Anything [\*]

A definition of something.

/ : Information Action Subsets: affected by:Action On Entity

/ is in : Computer System [\*] Subsets: is part of:Entity

A storage location for information.

/ : Information Vulnerability Subsets: has vulnerability:Vulnerability

#### **8.4.5 Class Information Source**

Metadata defining the source of all statements about something.

##### **8.4.5.1 Direct Supertypes**

Actor

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

##### **8.4.5.2 Associations**

/ states : Statement [\*] Subsets: relates:Anything

Statements made by an information source. States is metadata, a statement about the assertion, not about the concept it represents.

Sources may be people, organizations, documents, information systems, etc.

#### **8.4.6 Class Information Store**

A resource in which information is stored.

#### 8.4.61 Direct Supertypes

[Structured Information Object](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

#### 8.4.7 Class Information Transfer

The transfer of information from one store to another.

#### 8.4.71 Direct Supertypes

[Information Action](#), [Transfer](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

#### 8.4.72 Associations

 : [Information Object](#) *Redefines:* transfers:[Entity](#) acts on information:[Information Object](#)

#### 8.4.8 Class Metadata

Information about the source, provenance or origin of information. Metadata may be a managed entity, providing for provenance.

#### 8.4.81 Direct Supertypes

[Information Object](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

#### 8.4.82 Associations

 metadata about : [Entity](#) [\*]

The subject of metadata

#### 8.4.9 Class Natural Language Text

A description of something in a natural language. The language should be represented by a context.

#### 8.4.91 Direct Supertypes

[Information Object](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

#### 8.4.92 Attributes

 text : [Text](#)

Natural language text of a description.

## **8.4.10 Class Package**

A group of information objects.

### **8.4.101 Direct Supertypes**

[Structured Information Object](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

## **8.4.11 Class Reference**

A reference to external information justifying some assertion.

### **8.4.111 Direct Supertypes**

[Metadata](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

### **8.4.112 Attributes**

 reference URI : [URIIdentifier](#)

A URI with which to access more information about the element.

## **8.4.12 Class Report**

A collection of information about a topic.

### **8.4.121 Direct Supertypes**

[Information Object](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

## **8.4.13 Class Software**

Programs and other operating information used by a computer to control its function.

### **8.4.131 Direct Supertypes**

[Information Object](#), [Tool](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

### **8.4.132 Associations**

 executed by : [Computer System](#) [\*]

Computer systems able to execute software.

 may perform information action : [Information Action](#) [\*] Subsets: required to perform:[Process](#)

Actions software may perform.

 : [Software Vulnerability](#) Redefines: has vulnerability:[Vulnerability](#)

### **8.4.14 Class Statement**

Statements provide metadata as to the source of information - who or what said it.

#### **8.4.141 Direct Supertypes**

Metadata

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

#### **8.4.142 Attributes**

statement date and time : [Time Point](#)

Date and time information was created or modified.

version : [Simple Identifier](#)

A version identifier for information.

transaction id : [Simple Identifier](#)

Identifier for an act or transaction creating information.

#### **8.4.143 Associations**

/ stated by : [Information Source](#) [1..\*] Subsets: relates:[Anything](#)

Sources of a statement

### **8.4.15 Class Structured Information Object**

An information object that has sub-elements. e.g., a "record".

#### **8.4.151 Direct Supertypes**

[Information Object](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

#### **8.4.152 Associations**

/ contains object : [Information Object](#) Redefines: has part:[Entity](#)

An information object contained in another.

### **8.4.16 Class Summary Description**

A short description

#### **8.4.161 Direct Supertypes**

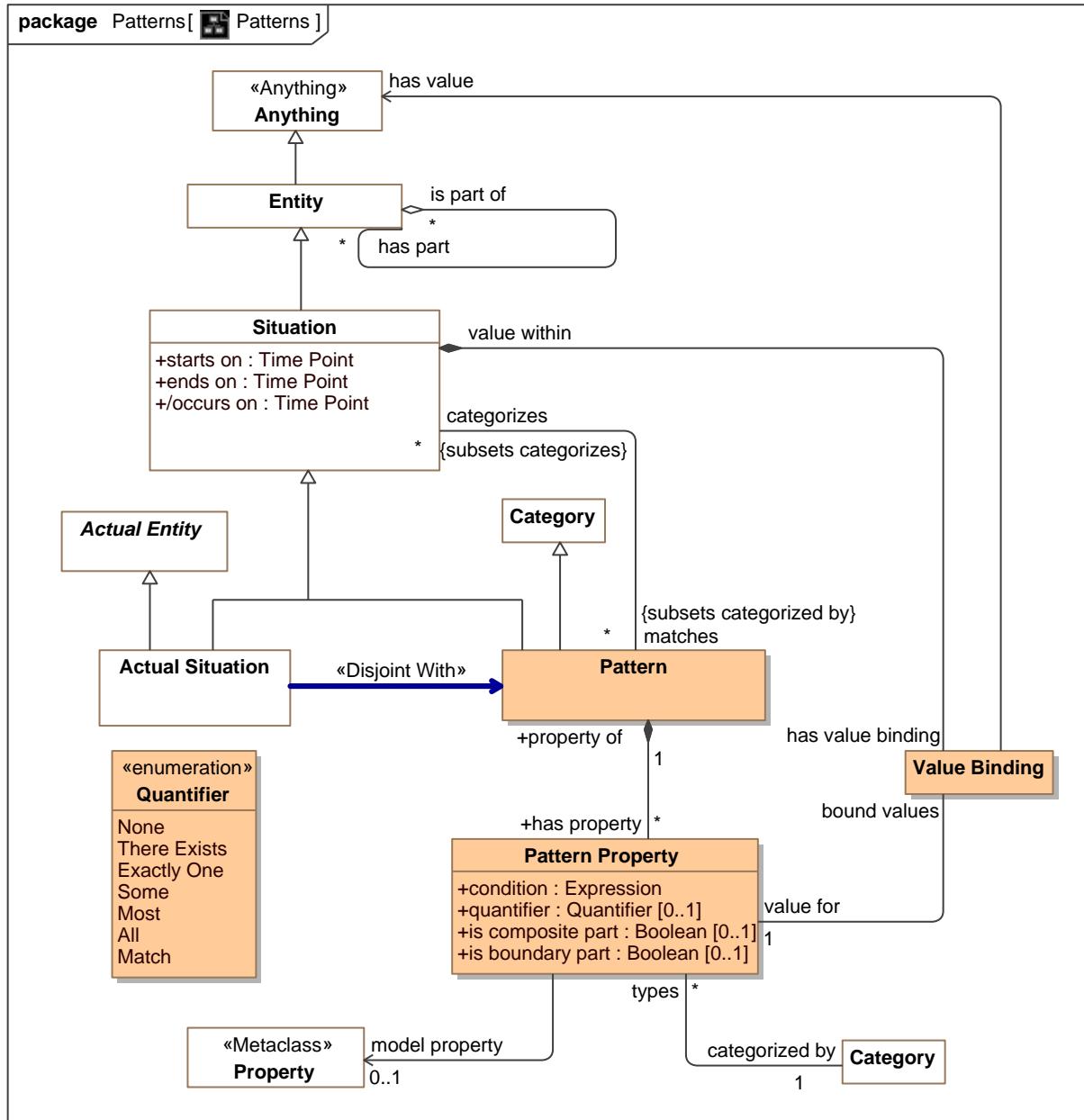
[Natural Language Text](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Information

## 8.5 Threat-risk-conceptual-model::Foundational Concepts::Patterns

Patterns define templates of individuals in a configuration and how such patterns match actual situations or other patterns. A pattern is a set of bindings that define values or sets of values that together define the template pattern. Actual situations represent individual actual situations that happened, are happening or will happen.

### 8.5.1 Diagram: Patterns



**Figure 7. Patterns**

### **8.5.2 Class Pattern**

A template of involved individuals, configuration, or type of things that may exist based on a set of bindings. Patterns categorize the set of situations which match the template.

A pattern may have parts, which constitute entities and relations defined within that pattern.

#### **8.5.21 Direct Supertypes**

[Category](#), [Situation](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Patterns

#### **8.5.22 Associations**

 categorizes : [Situation](#) [\*] Subsets: categorizes:[Anything](#)

The set of instances matching the pattern.

 has property : [Pattern Property](#) [\*]

### **8.5.3 Class Pattern Property**

A pattern property is a part of a pattern or rule and provides a contextual property within that pattern or rule for rules and relationships to be bound to.

A pattern property is a placeholder for all or a subset of the instances of the properties type as defined by the quantifier.

**package** Threat-risk-conceptual-model::Foundational Concepts::Patterns

#### **8.5.31 Attributes**

 condition : [Expression](#)

 quantifier : [Quantifier](#) [0..1]

An assertion that defines a quantification (based on the properties type) over a context.

e.g., for all people p: People is the context and P is the quantified property. In SIMF the quantified property would typically be named <quantifier> <type>. So the above quantified property would be named "all people". The quantified property will be asserted to have the quantified type.

 is composite part : [Boolean](#) [0..1]

True if the property represents an internal part of the pattern. False if the property is external to the pattern.

 is boundary part : [Boolean](#) [0..1]

True if the part is on the boundary of the pattern and connectible externally.

### 8.5.32 Associations

✓ property of : [Pattern](#) [1]

Pattern that defines a particular property.

✓ categorized by : [Category](#) [1]

The category or type that must classify a property.

↗ model property : [Property](#) [0..1]

Property defined in a model that is used in a pattern.

✓ bound values : [Value Binding](#)

Values for a property.

### 8.5.4 Class Value Binding

A value assigned to a user defined property within a situation.

Note also that any entity may be part of a situation and as such defines properties and relationships within that situation.

**package** Threat-risk-conceptual-model::Foundational Concepts::Patterns

### 8.5.41 Associations

✓ value for : [Pattern Property](#) [1]

Property for which the value is defined

✓ value within : [Situation](#)

Situation in which the value holds.

↗ has value : [Anything](#)

Value assigned to the property in the situation.

### 8.5.42 Enumeration Quantifier

The set of quantifiers for pattern variables

**package** Threat-risk-conceptual-model::Foundational Concepts::Patterns

**public enum** Quantifier

{None, There Exists, Exactly One, Some, Most, All, Match}

### 8.5.42Literals

○ None

A quantifier where no instance of the type fills the role.

○ There Exists

The existential quantifier - at least one. A logical "supertype" of "One of" and "Most"

○ Exactly One

The existential quantifier limited to exactly one of a potentially larger set

- Some

A stratified existential quantifier common values - example: Some people like spinach.

- Most

A stratified existential quantifier with a default for a "typical" value - example: People <typically> have 2 arms.

- All

The universal quantifier - the quantified property is a stand-in for all elements of the existent of the quantified type

- Match

Select is used in query and mapping patterns, all elements of the classified type that match the pattern are selected as instances of the pattern.

## **8.6 Threat-risk-conceptual-model::Foundational Concepts::Processes**

Processes are templates for (descriptions of) a related sets of occurrences (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 Occurrences.

Scenarios are typically less formal processes and describe how a series of occurrences may play out.

## 8.6.1 Diagram: Process and Plans

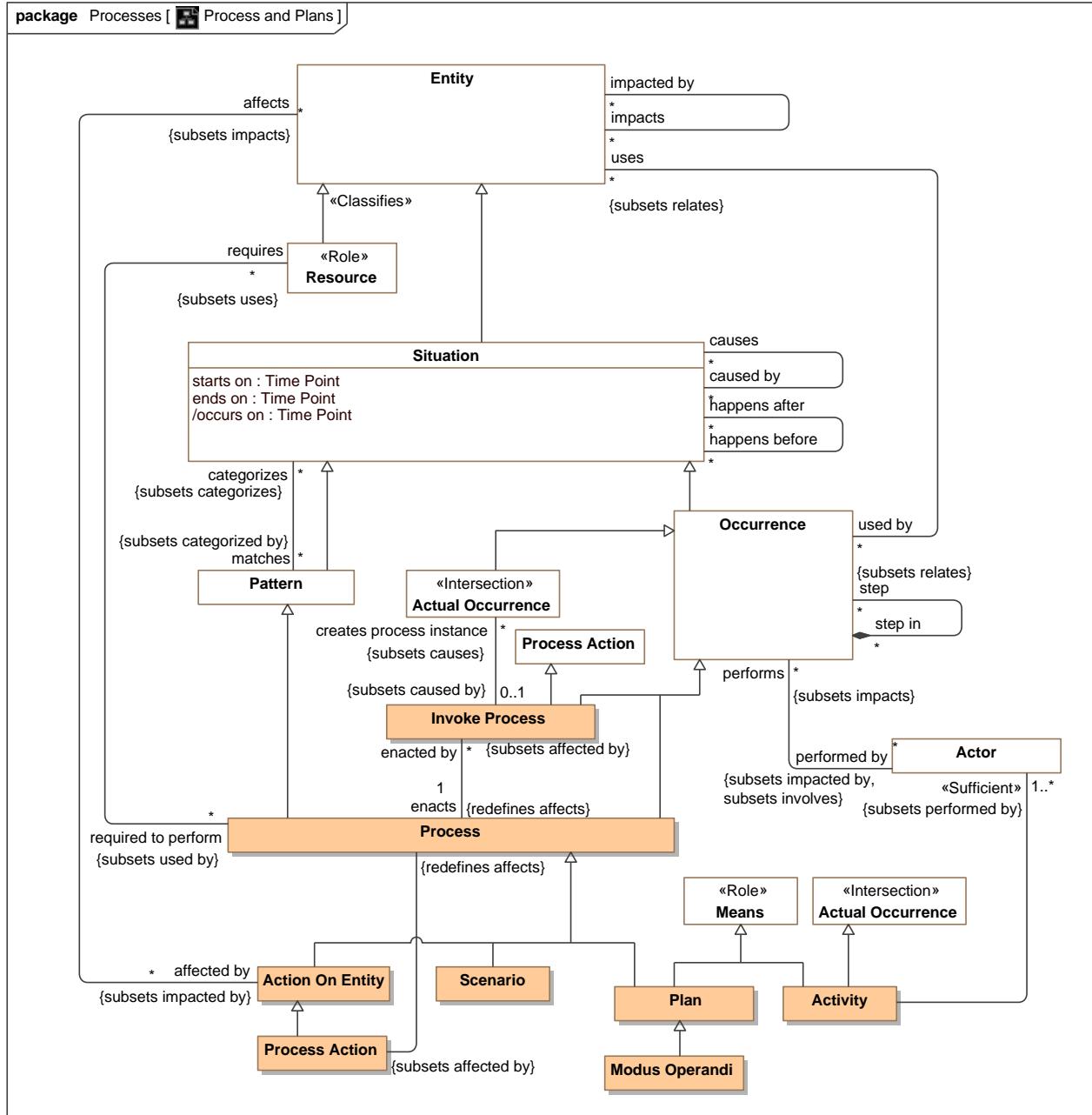


Figure 8. Process and Plans

## 8.6.2 Class Action On Entity

A process that affects specific things in specific ways.

### 8.6.21 Direct Supertypes

Process

**package** Threat-risk-conceptual-model::Foundational Concepts::Processes

### 8.6.22 Associations

/ affects : Entity [\*] Subsets: impacts:Entity

Entities affected by a action

### 8.6.3 Class Activity

An activity performed by one or more actors intended to meet a need.

### 8.6.31 Direct Supertypes

Actual Occurrence, Means

**package** Threat-risk-conceptual-model::Foundational Concepts::Processes

### 8.6.32 Associations

/ : Actor [1..\*] Subsets: performed by:Actor

### 8.6.4 Class Invoke Process

The activity of initiating the performance of a process.

The process instance will be classified by the process.

### 8.6.41 Direct Supertypes

Occurrence, Process Action

**package** Threat-risk-conceptual-model::Foundational Concepts::Processes

### 8.6.42 Associations

/ enacts : Process [1] Redefines: affects:Entity

The process an enactment uses to create a process instance

/ creates process instance : Actual Occurrence [\*] Subsets: causes:Situation

Process instance created by an enactment

### 8.6.5 Class Modus Operandi

A particular way or method for an actor to do something, especially one that is characteristic or well-established.

In threat terms, a particular tactic, technique or procedure for achieving a result.

Syn. TTP [STIX]

## 8.6.51 Direct Supertypes

[Plan](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Processes

## 8.6.6 Class Plan

A plan is a process definition that supports a stakeholder's objective. As a process definition a plan is a pattern for a series of activities.

### 8.6.6.1 Direct Supertypes

[Means](#), [Process](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Processes

## 8.6.7 Class Process

A template and definition for a family of occurrences (i.e. actions, events) that results in an outcome. A plan may be natural or caused by the activities of actors, in which case it is a plan.

A process may contain other entities and situations to define characteristics and sub-activities of the process.

### 8.6.7.1 Direct Supertypes

[Occurrence](#), [Pattern](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Processes

## 8.6.7.2 Associations

 requires : [Resource](#) [\*] Subsets: uses:[Entity](#)

A resource required for a process to take place.

 enacted by : [Invoke Process](#) [\*] Subsets: affected by:[Action On Entity](#)

Enactments of the process

 has capable performer : [Actor](#) [\*] Redefines: performed by:[Actor](#) influenced by:[Actor](#)

Actors capable of performing a process.

 may be performed by : [Actor](#) [\*] Redefines: influenced by:[Actor](#) performed by:[Actor](#)

Actors that have permission to perform a process.

 : [Process Action](#) Subsets: affected by:[Action On Entity](#)

## 8.6.8 Class Process Action

An action impacting a potential or realized process.

### 8.6.8.1 Direct Supertypes

[Action On Entity](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Processes

#### 8.6.82 Associations

 : [Process](#) *Redefines:* affects:[Entity](#)

#### 8.6.9 Class Scenario

A template for a set of occurrences (may be but are not always activities) and resource that formally or informally define how things may happen.

#### 8.6.91 Direct Supertypes

[Process](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Processes

#### 8.6.92 Attributes

 likelihood : [Probability Metric](#)

Possibility that the scenario did happen, is happening or will happen.

#### 8.6.93 Associations

 results in : [Undesirable Situation](#) [\*] *Redefines:* matches:[Pattern](#)

Danger that is a result of a scenario happening.

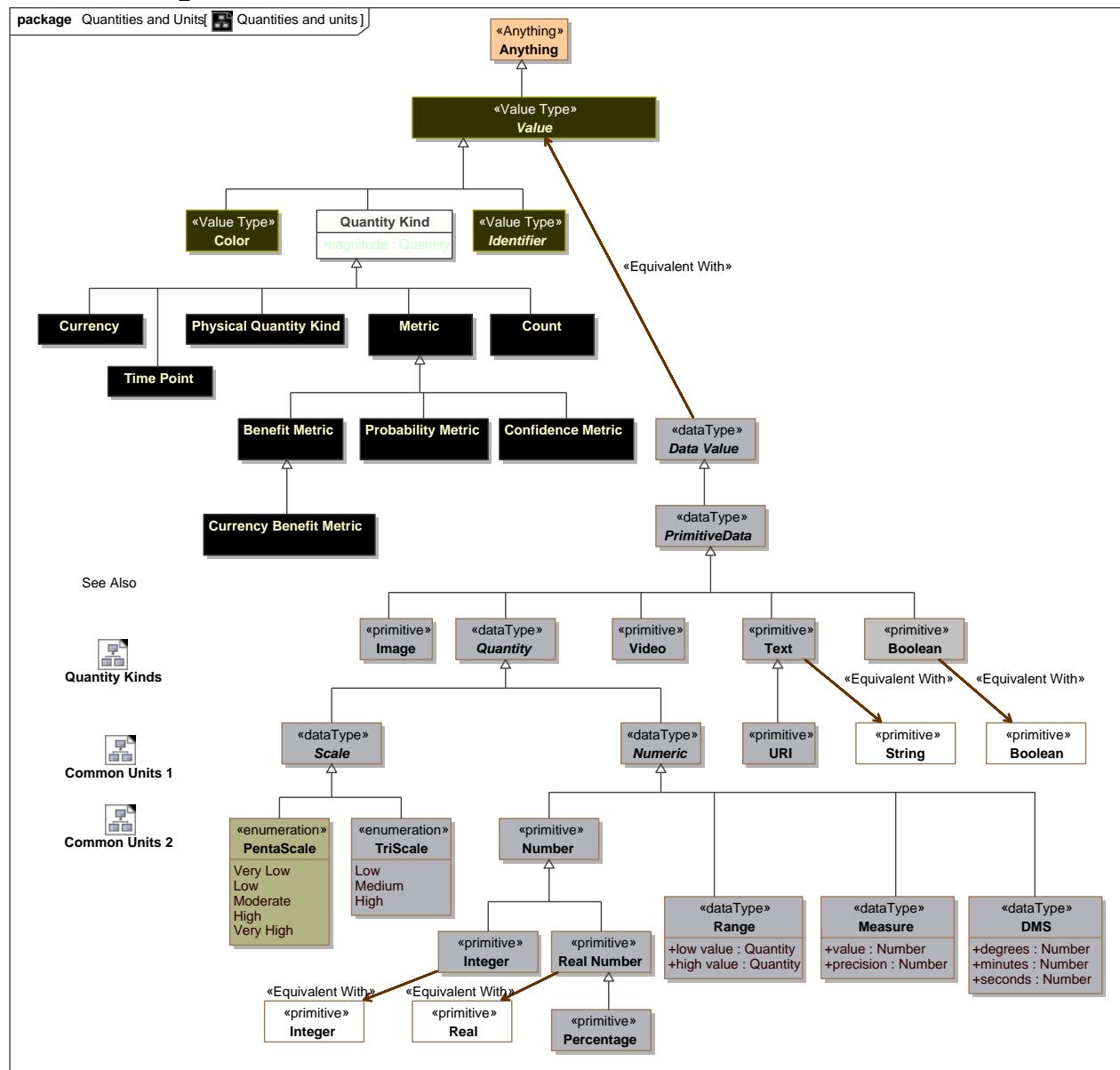
## **8.7 Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units**

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".

### 8.7.1 Diagram: Quantities and units



## Figure 9. Quantities and units

### 8.7.2 Class Benefit Metric

Any way to quantify benefit or harm.

#### 8.7.21 Direct Supertypes

[Metric](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units

### 8.7.3 Class Confidence Metric

Any metric of confidence.

#### 8.7.31 Direct Supertypes

[Metric](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units

### 8.7.4 Class Count

The number of something, e.g., 5 fish.

#### 8.7.41 Direct Supertypes

[Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units

### 8.7.5 Class Currency Benefit Metric

A metric for benefit or harm expressed in terms of a currency, such as dollars or yen.

#### 8.7.51 Direct Supertypes

[Benefit Metric](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units

### 8.7.6 Class Metric

A standard for measuring or evaluating something.

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".

### 8.7.61 Direct Supertypes

[Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units

### 8.7.7 Class Probability Metric

A metric that represents the possibility that something uncertain will happen.

### 8.7.71 Direct Supertypes

[Metric](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units

### 8.7.8 Class Quantity Kind

A real scalar quantity, defined and adopted by convention, with which any other quantity of the same quantity kind can be compared to express the ratio of the two quantities as a number. e.g., Degrees Centigrade, Miles. [JCGM 200:2008t]

### 8.7.81 Direct Supertypes

[Value](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units

### 8.7.82 Attributes

◆ magnitude : [Quantity](#)

The value of a quantity.

### 8.7.9 Class Time Point

A particular point in time, recognizing that any such point is a duration at a finer level of granularity.

### 8.7.91 Direct Supertypes

[Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units

### 8.7.10 Class Value

A value is an atomic piece of information without a specific lifetime or identity independent of the value. Values include numbers, strings, and other atomic "primitive" information.

### 8.7.101 Direct Supertypes

[Anything](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units

### 8.7.102 Enumeration PentaScale

An arbitrary scale of 5 values.

#### 8.7.102Direct Known Superclasses

##### Scale

```
package Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units
```

```
public enum PentaScale
```

```
{Very Low, Low, Moderate, High, Very High}
```

#### 8.7.102Literals

- Very Low
- Low
- Moderate
- High
- Very High

### 8.7.103 Enumeration TriScale

A scale of 3 arbitrary levels.

#### 8.7.103Direct Known Superclasses

##### Scale

```
package Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units
```

```
public enum TriScale
```

```
{Low, Medium, High}
```

#### 8.7.103Literals

- Low
- Medium
- High

## 8.8 Threat-risk-conceptual-model::Foundational Concepts::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.

### 8.8.1 Diagram: Quantity Kinds

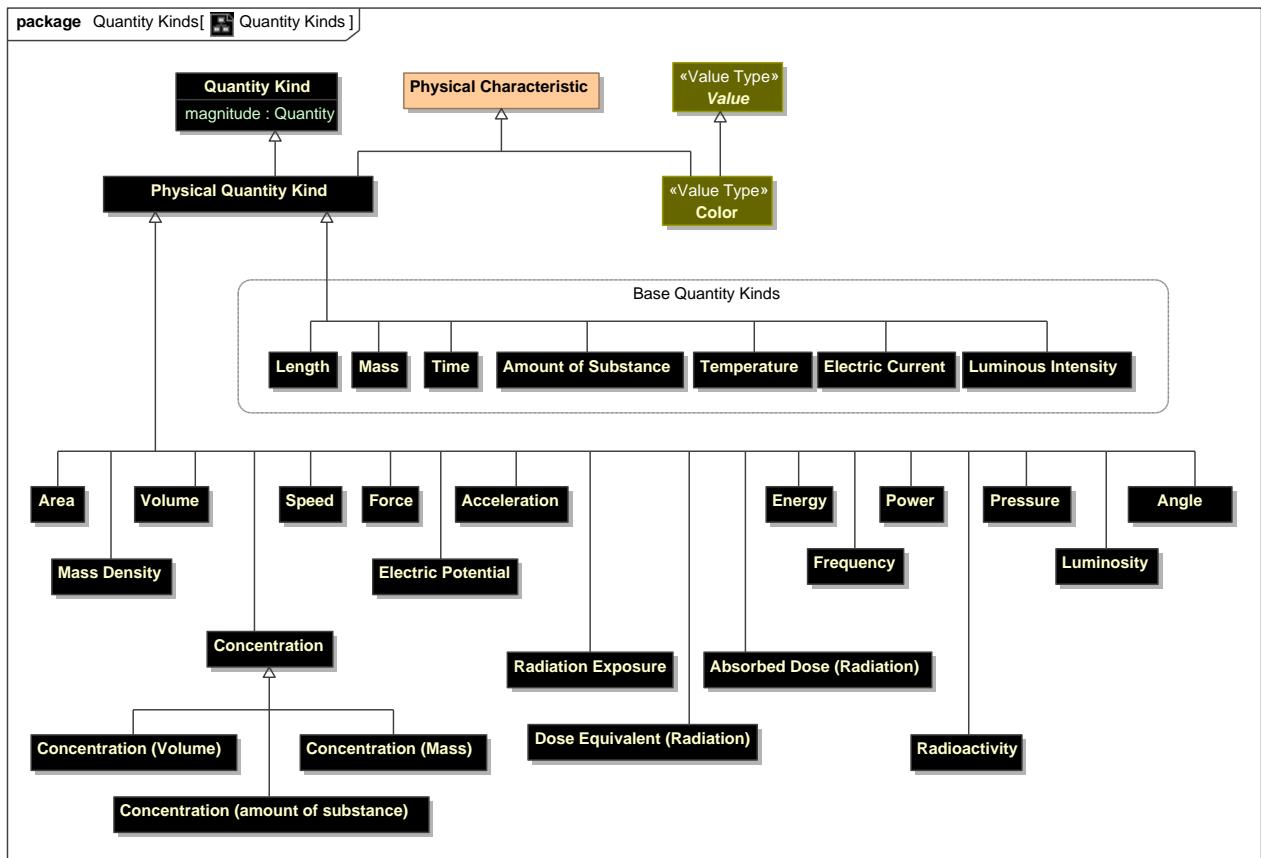


Figure 10. Quantity Kinds

### 8.8.2 Class Absorbed Dose (Radiation)

The energy of ionizing radiation absorbed per unit mass by a body, often measured in rads.

#### 8.8.21 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

### **8.8.3 Class Acceleration**

The rate of change of velocity per unit of time.

#### 8.8.31 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

### **8.8.4 Class Amount of Substance**

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.

#### 8.8.41 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

### **8.8.5 Class Angle**

The space (usually measured in radians or degrees) between two intersecting lines or surfaces at or close to the point where they meet.

#### 8.8.51 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

### **8.8.6 Class Area**

[QUOTD] Area is a quantity expressing the two-dimensional size of a defined part of a surface, typically a region bounded by a closed curve.

#### 8.8.61 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.7 Class Color**

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.

### **8.8.7.1 Direct Supertypes**

[Physical Characteristic](#), [Value](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.8 Class Concentration**

The abstract concept of concentration without being specific as to how it is measured.

### **8.8.8.1 Direct Supertypes**

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.9 Class Concentration (amount of substance)**

Amount-of-substance concentration.

### **8.8.9.1 Direct Supertypes**

[Concentration](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.10 Class Concentration (Mass)**

Mass per unit of volume.

### **8.8.10.1 Direct Supertypes**

[Concentration](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.11 Class Concentration (Volume)**

The volume concentration is defined as the volume of a constituent divided by the volume of the mixture.

### **8.8.11.1 Direct Supertypes**

[Concentration](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.12 Class Count**

The number of something. e.g., the number of people on earth.

### **8.8.121 Direct Supertypes**

[Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.13 Class Currency**

Any form of money.

### **8.8.131 Direct Supertypes**

[Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.14 Class Dose Equivalent (Radiation)**

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).

### **8.8.141 Direct Supertypes**

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.15 Class Electric Current**

The abstract unit of electric current which is the supertype of all current units and also acts as its "quantity kind".

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.[QUDT]

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.

### **8.8.151 Direct Supertypes**

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.16 Class Electric Potential**

[QUDT] Electric Potential is a scalar valued quantity associated with an electric field.

### 8.8.161 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.17 Class Energy**

The measure of energy and work.

### 8.8.171 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.18 Class Force**

(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).

### 8.8.181 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.19 Class Frequency**

Repetitions per unit of time. e.g., Hertz.

### 8.8.191 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.20 Class Length**

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.

### 8.8.201 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

### 8.8.21 Class Luminosity

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.

### 8.8.211 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

### 8.8.22 Class Luminous Intensity

The abstract unit of luminous intensity (brightness) which is the supertype of all luminous intensity units and also acts as its "quantity kind".

The candela is the luminous intensity SI Unit, in a given direction, of a source that emits monochromatic radiation of frequency  $540 \times 10^{12}$  hertz and that has a radiant intensity in that direction of  $1/683$  watt per steradian.

### 8.8.221 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

### 8.8.23 Class Mass

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  $9.8 \text{ m/s}^2$ . The SI unit of mass is the kilogram (kg).

### 8.8.231 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.24 Class Mass Density**

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  $\rho$  (the lower case Greek letter rho). Mathematically, density is defined as mass divided by volume.

### **8.8.241 Direct Supertypes**

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.25 Class Physical Characteristic**

A property of a physical object.

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.26 Class Physical Quantity Kind**

A measurable property of a physical object.

### **8.8.261 Direct Supertypes**

[Physical Characteristic, Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.27 Class Power**

(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.

### **8.8.271 Direct Supertypes**

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.28 Class Pressure**

The continuous physical force exerted on or against an object by something in contact with it.

### **8.8.281 Direct Supertypes**

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.29 Class Radiation Exposure**

A measure of exposure to radiation.

### 8.8.291 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.30 Class Radioactivity**

Radioactivity 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).

### 8.8.301 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.31 Class Speed**

Distance per unit of time.

### 8.8.311 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.32 Class Temperature**

The abstract unit 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.

### 8.8.321 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## **8.8.33 Class Time**

The abstract unit of time which is the supertype of all time units and also acts as its "quantity kind".

Time is a measure in which events can be ordered from the past through the present into the future, and also the measure of durations of events and the intervals between them.

#### 8.8.331 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

#### 8.8.34 Class Volume

The amount of space that a substance or object occupies.

#### 8.8.341 Direct Supertypes

[Physical Quantity Kind](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Quantity Kinds

## 8.9 Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

A package of common SI and U.S. Units. Note: All measures in concrete models should be bound to the expected units, even if units are implicit in the data structure.

### 8.9.1 Diagram: Common Units 1

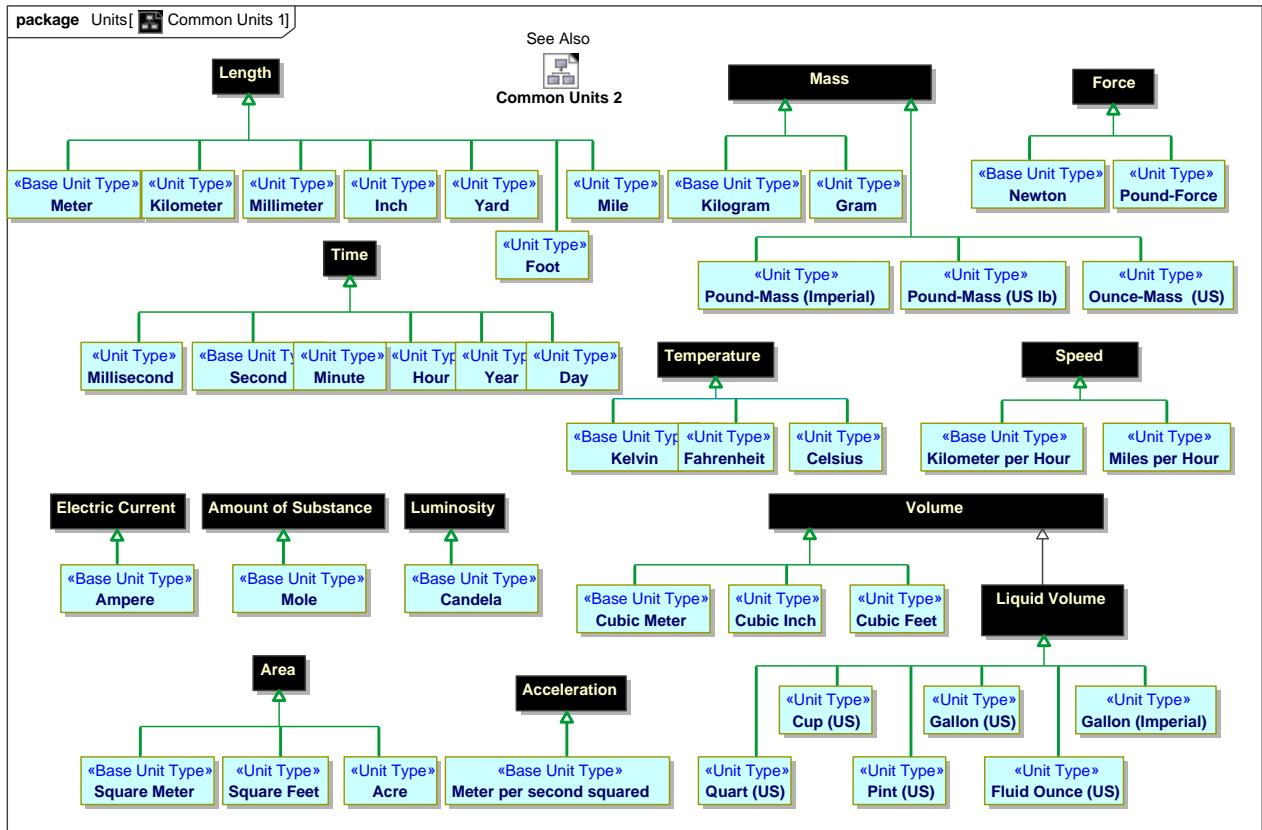


Figure 11. Common Units 1

## 8.9.2 Diagram: Common Units 2

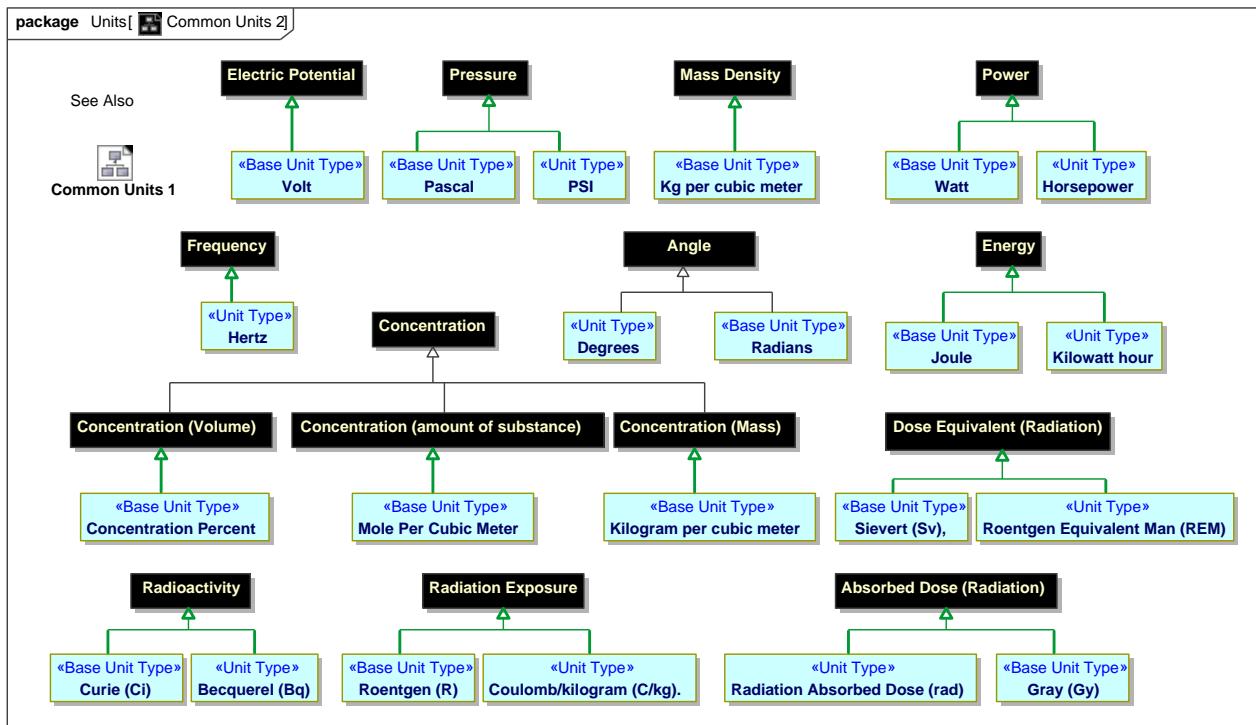


Figure 12. Common Units 2

## 8.9.3 Class Acre

1 acre = 43 560 square feet.

### 8.9.31 Direct Supertypes

[Area](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.4 Class Ampere

[NIST-SI] The ampere is that constant current which, if maintained in two straight parallel conductors of infinite length, of negligible circular cross-section, and placed 1 meter apart in a vacuum, would produce between these conductors a force equal to  $2 \times 10^{-7}$  newton per meter of length.

### 8.9.41 Direct Supertypes

[Electric Current](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.5 Class Becquerel (Bq)**

The SI unit of radioactivity, corresponding to one disintegration per second.

### 8.9.51 Direct Supertypes

[Radioactivity](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.6 Class Candela**

The candela is the luminous intensity, in a given direction, of a source that emits monochromatic radiation of frequency  $540 \times 10^{12}$  hertz and that has a radiant intensity in that direction of  $1/683$  watt per steradian.[NIST-SI]

### 8.9.61 Direct Supertypes

[Luminosity](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.7 Class Celsius**

Centigrade. The temperature scale (Celsius scale) in which  $0^\circ$  represents the ice point and  $100^\circ$  the steam point of water.

### 8.9.71 Direct Supertypes

[Temperature](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.8 Class Concentration Percent**

The volume of a constituent divided by the volume of the mixture.

### 8.9.81 Direct Supertypes

[Concentration \(Volume\)](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.9 Class Coulomb/kilogram (C/kg).**

Unit of radiation exposure.

### 8.9.91 Direct Supertypes

[Radiation Exposure](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.10 Class Cubic Feet**

A volume measured in feet.

### 8.9.101 Direct Supertypes

[Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.11 Class Cubic Inch**

A volume measured in inches.

### 8.9.111 Direct Supertypes

[Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.12 Class Cubic Meter**

A volume measured in meters.

### 8.9.121 Direct Supertypes

[Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.13 Class Cup (US)**

8 Fluid Ounces (US).

### 8.9.131 Direct Supertypes

[Liquid Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.14 Class Curie (Ci)**

The SI unit of measure for radioactivity is the curie (Ci) and Becquerel (Bq).

### 8.9.141 Direct Supertypes

[Radioactivity](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.15 Class Day**

A time unit of 24 hours.

## 8.9.151 Direct Supertypes

[Time](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.16 Class Degrees

A unit for an angle from 0-360.

## 8.9.161 Direct Supertypes

[Angle](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.17 Class Fahrenheit

The Fahrenheit scale in which  $32^{\circ}$  represents the ice point and  $212^{\circ}$  the steam point. of water Symbol: F.

## 8.9.171 Direct Supertypes

[Temperature](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.18 Class Fluid Ounce (US)

A unit of volume: 16 fluid ounces = 1 pint (pt)

= 28.875 cubic inches.

## 8.9.181 Direct Supertypes

[Liquid Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.19 Class Foot

A foot (pl. feet; abbreviation: ft; symbol: ', the prime symbol) is a unit of length in the imperial and US customary systems of measurement. Since 1959, both units have been defined by international agreement as equivalent to 0.3048 meters exactly. In both systems, the foot comprises 12 inches and three feet compose a yard.

## 8.9.191 Direct Supertypes

[Length](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.20 Class Gallon (Imperial)

A unit of volume.

## 8.9.201 Direct Supertypes

[Liquid Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.21 Class Gallon (US)

1 gallon (gal) = 231 cubic inches.

## 8.9.211 Direct Supertypes

[Liquid Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.22 Class Gram

The gram is a SI unit of mass.

## 8.9.221 Direct Supertypes

[Mass](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.23 Class Gray (Gy)

One of the two units used to measure the amount of radiation absorbed by an object or person, known as the "absorbed dose," which reflects the amount of energy that radioactive sources (with any type of ionizing radiation) deposit in materials (e.g., water, tissue, air) through which they pass. One gray (Gy) is the international system of units (SI) equivalent of 100 rads, which is equal to an absorbed dose of 1 Joule/kilogram. An absorbed dose of 0.01 Gy means that 1 gram of material absorbed 100 ergs of energy (a small but measurable amount) as a result of exposure to radiation.[NRC]

## 8.9.231 Direct Supertypes

[Absorbed Dose \(Radiation\)](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.24 Class Hertz

A unit of frequency. Cycles per second.

## 8.9.241 Direct Supertypes

[Frequency](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.25 Class Horsepower**

Horsepower (hp) is a unit of measurement of power (the rate at which work is done). There are many different standards and types of horsepower. This model uses the 746 watt interpretation of horsepower.

### **8.9.251 Direct Supertypes**

[Power](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.26 Class Hour**

A unit of time: 60 Minutes.

### **8.9.261 Direct Supertypes**

[Time](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.27 Class Inch**

A unit of length.

### **8.9.271 Direct Supertypes**

[Length](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.28 Class Joule**

The joule (symbol J, also called newton meter, watt second, or coulomb volt) is the SI unit of energy and work.

### **8.9.281 Direct Supertypes**

[Energy](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.29 Class Kelvin**

[NIST-SI] The kelvin, unit of thermodynamic temperature, is the fraction 1/273.16 of the thermodynamic temperature of the triple point of water.

### **8.9.291 Direct Supertypes**

[Temperature](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.30 Class Kg per cubic meter**

The SI unit for density.

#### 8.9.301 Direct Supertypes

[Mass Density](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.31 Class Kilogram**

The kilogram is the unit of mass; it is equal to the mass of the international prototype of the kilogram. [NIST-SI]

#### 8.9.311 Direct Supertypes

[Mass](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.32 Class Kilogram per cubic meter**

The SI Unit of density.

#### 8.9.321 Direct Supertypes

[Concentration \(Mass\)](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.33 Class Kilometer**

A unit of length, the SI measure of distances equal to 1000 meters, and equivalent to 3280.8 feet or 0.621 mile.

Symbol: km.

#### 8.9.331 Direct Supertypes

[Length](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.34 Class Kilometer per Hour**

The SI unit of speed

#### 8.9.341 Direct Supertypes

[Speed](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.35 Class Kilowatt hour**

The watt-hour (symbolized Wh) is a unit of energy equivalent to one watt (1 W) of power expended for one hour (1 h) of time.

#### 8.9.351 Direct Supertypes

[Energy](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.36 Class Liquid Volume**

Volume of a liquid.

#### 8.9.361 Direct Supertypes

[Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.37 Class Meter**

The meter is the length of the path traveled by light in vacuum during a time interval of 1/299 792 458 of a second.[NIST-SI]

The meter, (SI unit symbol: m), is the fundamental unit of length in the International System of Units (SI).

#### 8.9.371 Direct Supertypes

[Length](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.38 Class Meter per second squared**

The SI Unit of acceleration.

#### 8.9.381 Direct Supertypes

[Acceleration](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.39 Class Mile**

The mile is an English unit of length standardized as exactly 1.609344 kilometers.

#### 8.9.391 Direct Supertypes

[Length](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.40 Class Miles per Hour**

U.S. unit of speed.

### 8.9.401 Direct Supertypes

[Speed](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.41 Class Millimeter**

A unit of length equal to one thousandth of a meter and equivalent to 0.03937 inch.

Abbreviation: mm.

### 8.9.411 Direct Supertypes

[Length](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.42 Class Millisecond**

A unit of time: 1/1000th of a second.

### 8.9.421 Direct Supertypes

[Time](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.43 Class Minute**

A unit of time: 60 seconds.

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.44 Class Mole**

The mole is a unit of measurement used in chemistry to express amounts of a chemical substance, defined as the amount of any substance that contains as many elementary entities (e.g., atoms, molecules, ions, electrons) as there are atoms in 12 grams of pure carbon-12.

### 8.9.441 Direct Supertypes

[Amount of Substance](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.45 Class Mole Per Cubic Meter**

The SI unit for amount-of-substance concentration.

### 8.9.451 Direct Supertypes

[Concentration \(amount of substance\)](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.46 Class Newton**

The SI unit of force. Equivalent to 100,000 dynes. A Newton is equal to the force that would give a mass of one kilogram an acceleration of one meter per second per second.

### 8.9.461 Direct Supertypes

[Force](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.47 Class Ounce-Mass (US)**

U.S. Unit of Ounce representing Mass.

### 8.9.471 Direct Supertypes

[Mass](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.48 Class Pascal**

The SI unit of pressure, equal to one newton per square meter (approximately 0.000145 pounds per square inch, or  $9.9 \times 10^{-6}$  atmospheres).

### 8.9.481 Direct Supertypes

[Pressure](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.49 Class Pint (US)**

Unit of liquid volume: 2 pints = 1 quart (qt) = 57.75 cubic inches.

### 8.9.491 Direct Supertypes

[Liquid Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.50 Class Pound-Force**

The pound-force is equal to the gravitational force exerted on a mass of one avoirdupois pound on the surface of Earth.

Standard gravity is not constant but usually taken to be 9.80665 m/s<sup>2</sup> (about 32.174 049 ft/s<sup>2</sup>) in the context of the surface of the earth.

### 8.9.501 Direct Supertypes

[Force](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.51 Class Pound-Mass (Imperial)**

Exactly 453.59237 grams.

### 8.9.511 Direct Supertypes

[Mass](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.52 Class Pound-Mass (US lb)**

The pound avoirdupois, which forms the basis of the U.S. customary system of mass, is defined as exactly 453.59237 grams.

The avoirdupois pound is legally defined as a measure of mass, but the name pound is also applied to measures of force.

See also: <http://www.nist.gov/pml/wmd/metric/upload/frn-59-5442-1959.pdf>

### 8.9.521 Direct Supertypes

[Mass](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.53 Class PSI**

Pounds per square inch.

### 8.9.531 Direct Supertypes

[Pressure](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.54 Class Quart (US)**

4 quarts = 1 gallon (gal) = 231 cubic inches [NIST-UNITS].

### 8.9.541 Direct Supertypes

[Liquid Volume](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.55 Class Radians**

A unit of an angle where there are 2 PI radians in a circle.

### 8.9.551 Direct Supertypes

[Angle](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.56 Class Radiation Absorbed Dose (rad)**

One of the two units used to measure the amount of radiation absorbed by an object or person, known as the “absorbed dose,” which reflects the amount of energy that radioactive sources deposit in materials through which they pass. The radiation-absorbed dose (rad) is the amount of energy (from any type of ionizing radiation) deposited in any medium (e.g., water, tissue, air). An absorbed dose of 1 rad means that 1 gram of material absorbed 100 ergs of energy (a small but measurable amount) as a result of exposure to radiation. The related international system unit is the gray (Gy), where 1 Gy is equivalent to 100 rad. For additional information, see Doses in Our Daily Lives and Measuring Radiation. [NRC]

### 8.9.561 Direct Supertypes

[Absorbed Dose \(Radiation\)](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.57 Class Roentgen (R)**

A unit of exposure to ionizing radiation. It is the amount of gamma or x-rays required to produce ions resulting in a charge of 0.000258 coulombs/kilogram of air under standard conditions. [NRC]

### 8.9.571 Direct Supertypes

[Radiation Exposure](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## **8.9.58 Class Roentgen Equivalent Man (REM)**

One of the two standard units used to measure the dose equivalent (or effective dose), which combines the amount of energy (from any type of ionizing radiation that is deposited in human tissue), along with the medical effects of the given type of radiation. For beta and gamma radiation, the dose equivalent is the same as the absorbed dose. By contrast, the dose equivalent is larger than the absorbed dose for alpha and neutron radiation, because these types of radiation are more damaging to the human body. Thus, the dose equivalent (in rems) is equal to the absorbed dose (in rads) multiplied by the quality factor of the type of radiation [see Title 10, Section 20.1004, of the Code of Federal Regulations (10 CFR 20.1004), "Units of Radiation Dose"]. The related international system unit is the sievert (Sv), where 100 rem is equivalent to 1 Sv. [NRC]

### 8.9.581 Direct Supertypes

[Dose Equivalent \(Radiation\)](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.59 Class Second**

The second (symbol: s) is the base unit of time in the International System of Units (SI) and is also a unit of time in other systems of measurement (abbreviated s or sec); it is the second division of the hour by sixty, the first division by 60 being the minute.

The second is the duration of 9 192 631 770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the cesium 133 atom.[NIST-SI]

#### 8.9.591 Direct Supertypes

[Time](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.60 Class Sievert (Sv),**

The international system (SI) unit for dose equivalent equal to 1 Joule/kilogram. 1 sievert = 100 rem. Named for physicist Rolf Sievert.

#### 8.9.601 Direct Supertypes

[Dose Equivalent \(Radiation\)](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.61 Class Square Feet**

Area measured in feet.

#### 8.9.611 Direct Supertypes

[Area](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.62 Class Square Meter**

Area measured in SI meters.

#### 8.9.621 Direct Supertypes

[Area](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

### **8.9.63 Class Volt**

The SI unit of electromotive force, the difference of potential that would drive one ampere of current against one ohm resistance.

## 8.9.631 Direct Supertypes

[Electric Potential](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.64 Class Watt

The SI unit of power is the joule per second (J/s).

## 8.9.641 Direct Supertypes

[Power](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.65 Class Yard

A Unit of length equal to 3 feet.[NIST-UNITS]

## 8.9.651 Direct Supertypes

[Length](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.9.66 Class Year

The period of 365 days (or 366 days in leap years) starting from the first of January, used for reckoning time in ordinary affairs.

## 8.9.661 Direct Supertypes

[Time](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Quantities and Units::Units

## 8.10 Threat-risk-conceptual-model::Foundational Concepts::Rules

Rules define conditional behavior that has some condition and some result. The result may be an action (an action rule) or simply to say what must be true (a constraint).

### 8.10.1 Diagram: Rules

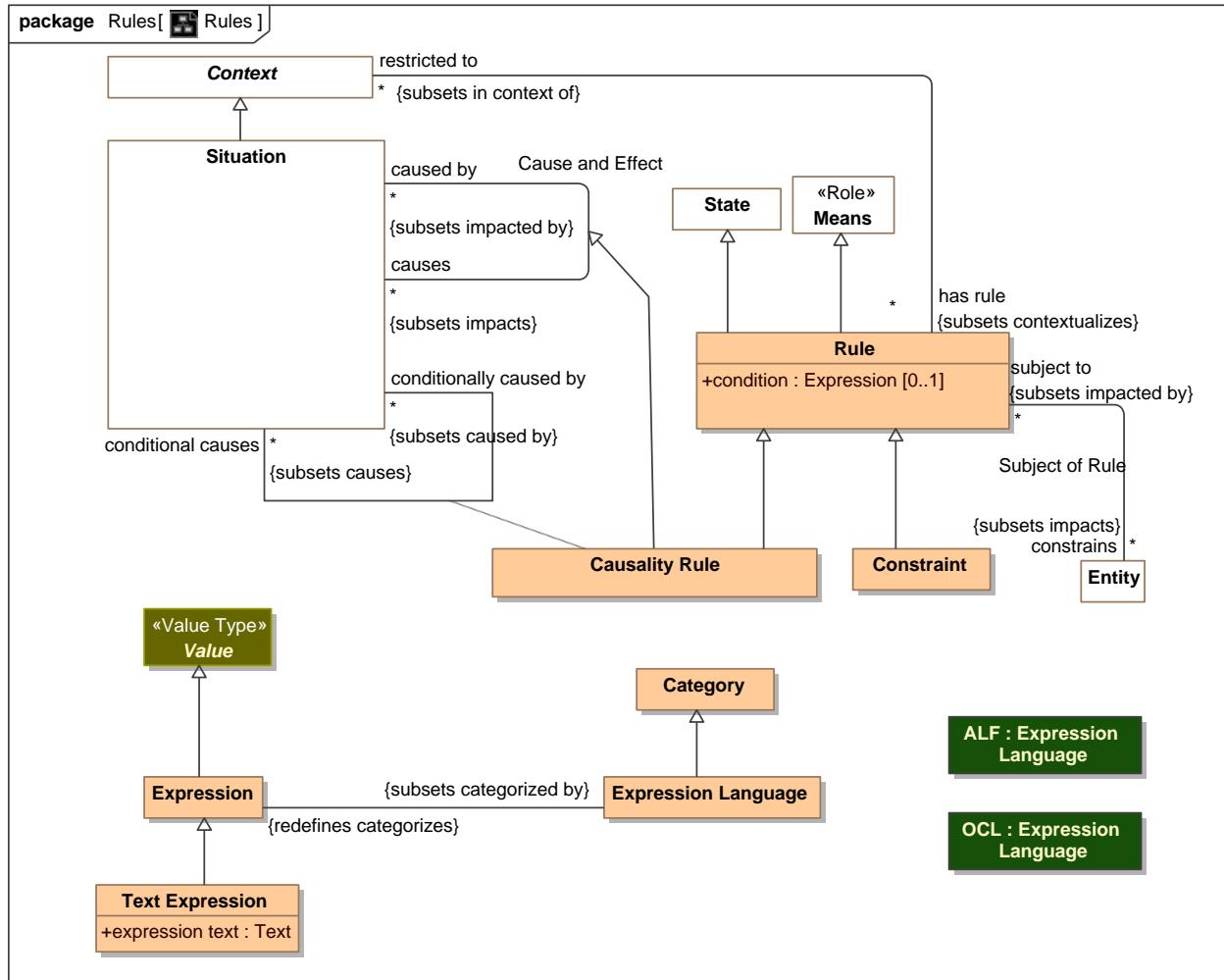


Figure 13. Rules

### 8.10.2 Association Class Causality Rule

A causality rule triggers a "do" effect when the "when" situation is matched under conditions(s) of the context - a proactive cause and effect.

## 8.10.21 Direct Supertypes

[Cause and Effect](#), [Rule](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Rules

### 8.10.21 Association Ends

 conditional causes : [Situation](#) [\*] *Redefines*: matches: [Pattern](#)

When a situation occurs.

 conditionally caused by : [Situation](#) [\*] *Redefines*: matches: [Pattern](#)

Things that may cause the situation.

## 8.10.3 Class Constraint

Anything which places limits on a situation.

## 8.10.31 Direct Supertypes

[Rule](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Rules

## 8.10.4 Class Expression

Expressions return a value based on a calculation.

## 8.10.41 Direct Supertypes

[Value](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Rules

## 8.10.42 Associations

 : [Expression Language](#) Subsets: categorized by: [Category](#)

## 8.10.5 Class Expression Language

A language for expressions. e.g., OCL, ALF, Java, English.

## 8.10.51 Direct Supertypes

[Category](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Rules

## 8.10.52 Associations

 : [Expression](#) *Redefines*: categorizes: [Anything](#)

## **8.10.6 Class Rule**

A statement that defines or constrains some aspect or behavior of an entity (type of entity) or state of a situation (or type of situation). A contextualized rule only applies to that context.

### **8.10.61 Direct Supertypes**

[Means](#), [State](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Rules

### **8.10.62 Attributes**

◊ condition : [Expression](#) [0..1]

An expression that must be true for a rule to "fire"

### **8.10.63 Associations**

↙ restricted to : [Context](#) [\*] Subsets: in context of: [Context](#)

Restriction as to the applicability of a rule.

↙ constrains : [Metric](#)

Entities a rule applies to.

## **8.10.7 Class Text Expression**

A textual representation of a calculation returning a value.

### **8.10.71 Direct Supertypes**

[Expression](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Rules

### **8.10.72 Attributes**

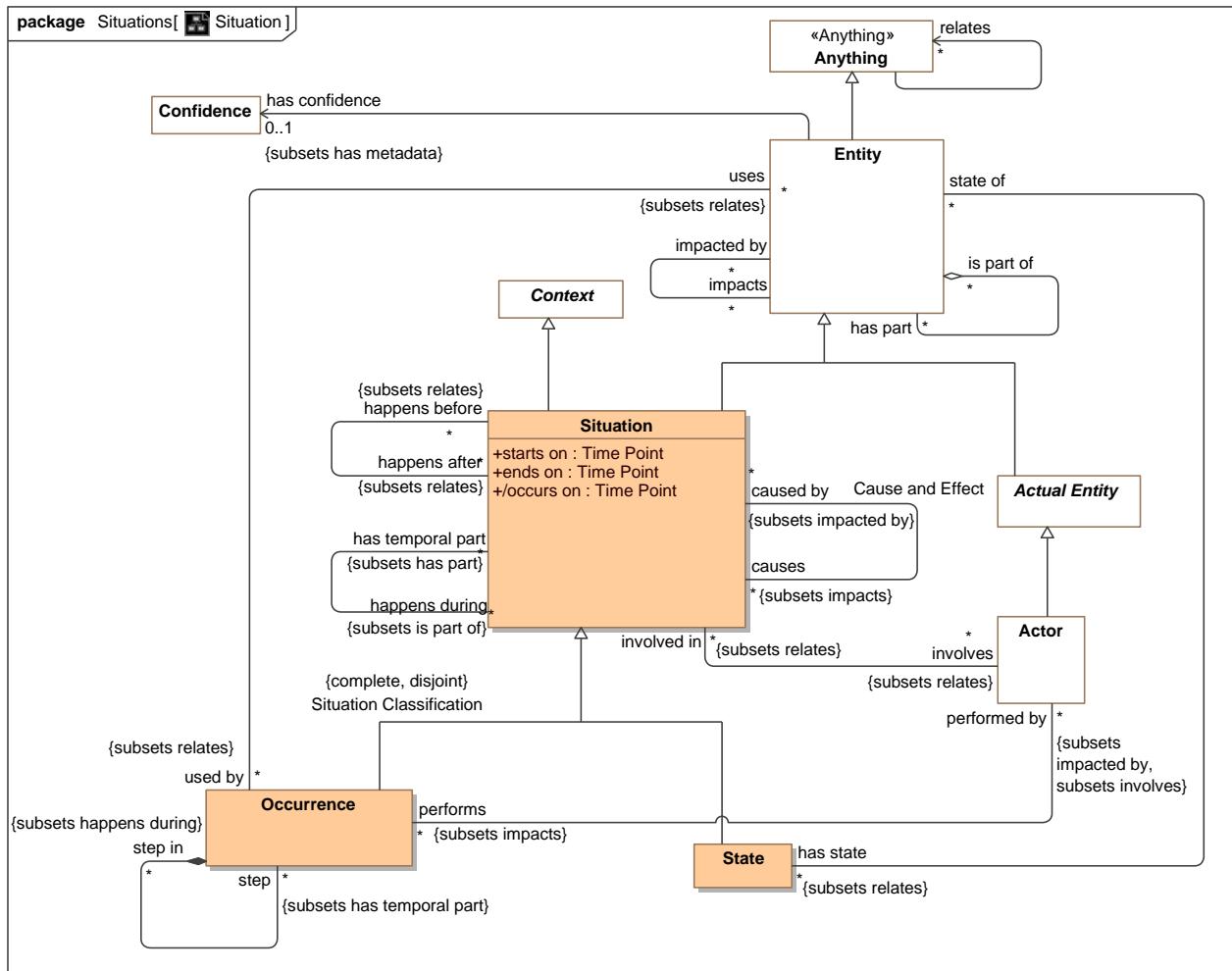
◊ expression text : [Text](#)

Text representation of an expression.

## **8.11 Threat-risk-conceptual-model::Foundational Concepts::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.

### **8.11.1 Diagram: Situation**



**Figure 14.** Situation

### 8.11.2 Association Cause and Effect

The causality relation where `<causes>` is `<caused by>`.

**package** Threat-risk-conceptual-model::Foundational Concepts::Situations

**8.11.21 Association Ends**

/ caused by : [Situation](#) [\*]

One of situations that causes the subject situation.

/ causes : [Situation](#) [\*]

A situation caused by another.

**8.11.3 Class Occurrence**

Anything that happens. A dynamic situation (past, present or future) of a set of things changing over a period of time {Perdurant}. e.g., a rock falling.

An occurrence that is "performed by" an actor can be considered an activity.

**8.11.31 Direct Supertypes**

[Situation](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Situations

**8.11.32 Associations**

/ uses : [Entity](#) [\*] Subsets: relates:[Anything](#)

Things used by the occurrence.

/ step in : [Entity](#) [\*] Subsets: relates:[Anything](#)

A more granular occurrence of which this is a part.

/ step : [Entity](#) [\*] Subsets: relates:[Anything](#)

A part of an occurrence, one step in its execution.

/ performed by : [Actor](#) [\*] Subsets: involves:[Actor](#) impacted by:[Entity](#)

The performer of an activity.

**8.11.4 Class Situation**

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 include property values and instances of associations.

Situations may be static (the things on a desk) or dynamic (eating lunch), these are called occurrences and states, respectively.

Situations may be in the past, present or future and include both possible and actual situations.

Situation is a fundamental concept that spans and connects different domains and concerns.

A situation is a context for the entities involved in that situation. Note also that any entity may be part of a situation and as such defines properties and relationships within that situation - it may have parts, which form the composition of the situation.

#### 8.11.41 Direct Supertypes

[Context](#), [Entity](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Situations

#### 8.11.42 Attributes

⌚ starts on : [Time Point](#)

Time the situation started.

⌚ ends on : [Time Point](#)

Time the situation ended or will end.

⌚ occurs on : [Time Point](#)

When something happens. Derived from starts on and ends on.

#### 8.11.43 Associations

✓ has impact : [Impact](#) [\*] Subsets: has part:[Entity](#) caused by:[Situation](#)

A consequence of a situation that impacts the objectives of a stakeholder.

✓ matches : [Pattern](#) [\*] Subsets: categorized by:[Category](#)

Situations that match a pattern.

✓ happens before : [Pattern](#) [\*] Subsets: categorized by:[Category](#)

Situations that end before the subject situation starts.

✓ happens after : [Pattern](#) [\*] Subsets: categorized by:[Category](#)

Situations that start after the subject situation ends.

☰ conditionally caused by : [Pattern](#) [\*] Subsets: categorized by:[Category](#)

Things that may cause the situation.

✓ caused by : [Pattern](#) [\*] Subsets: categorized by:[Category](#)

One of situations that causes the subject situation.

✓ causes : [Pattern](#) [\*] Subsets: categorized by:[Category](#)

A situation caused by another.

☰ conditional causes : [Pattern](#) [\*] Subsets: categorized by:[Category](#)

When a situation occurs.

☰ initiates : [Course of Action](#) [\*] Subsets: conditional causes:[Situation](#)

The situation that triggers a course of action.

✓ achieved by : [Course of Action](#) [\*] Subsets: caused by:[Situation](#)

A course of action that leads to a situation.

✓ happens during : [Course of Action](#) [\*] Subsets: caused by:[Situation](#)

Situations with overlapping duration.

✓ has temporal part : [Course of Action](#) [\*] Subsets: caused by:[Situation](#)

Sub-durations of an occurrence, parts in time.

 situated at : [Place](#) [\*] Subsets: relates:[Anything](#)

Place where something or some occurrence is located.

 involves : [Actor](#) [\*] Subsets: relates:[Anything](#)

Actors involved in a situation in any way.

 has value binding : [Value Binding](#)

Values bound to the situation.

## 8.11.5 Class State

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}

### 8.11.51 Direct Supertypes

[Situation](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Situations

### 8.11.52 Associations

 state of : [Entity](#) [\*] Subsets: relates:[Anything](#)

The endurant entity for which the state is a snapshot.

## 8.11.6 Association Time Order

Ordering in time

**package** Threat-risk-conceptual-model::Foundational Concepts::Situations

### 8.11.61 Association Ends

 happens after : [Situation](#) [\*] Subsets: relates:[Anything](#)

Situations that start after the subject situation ends.

 happens before : [Situation](#) [\*] Subsets: relates:[Anything](#)

Situations that end before the subject situation starts.

## 8.12 Threat-risk-conceptual-model::Foundational Concepts::Timeframes

*Timeframe* segregates situations into those that are in the past, are current and those that are potential. Past and current situations are *actual situations*. Potential situations are a kind of pattern for what may happen and have a likelihood.

### 8.12.1 Diagram: Actual Thing

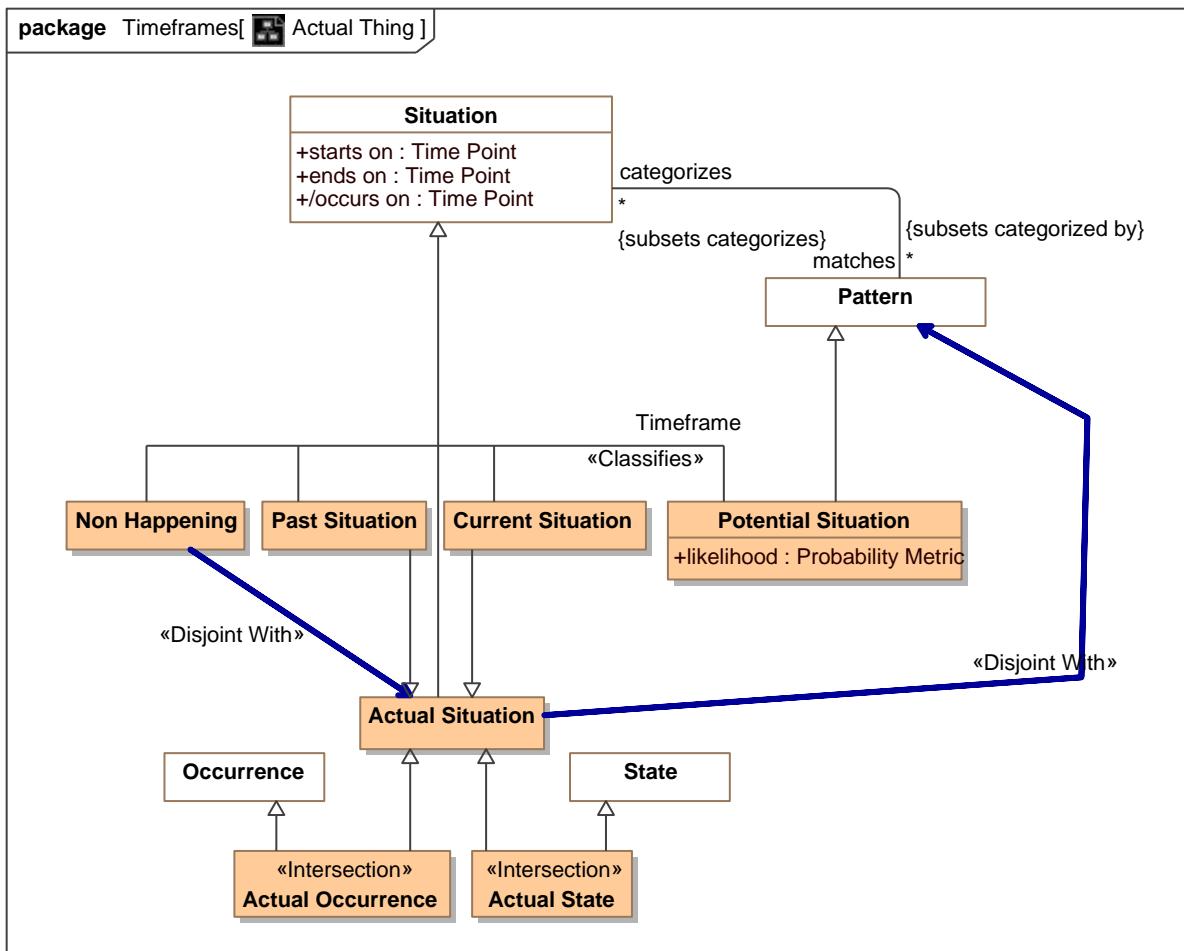


Figure 15. Actual Thing

### 8.12.2 Class Actual Occurrence

Something that has or is happening.

### 8.12.21 Direct Supertypes

[Actual Situation](#), [Occurrence](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Timeframes

### 8.12.22 Associations

/ enacted by : [Invoke Process](#) [0..1] Subsets: caused by:[Situation](#)

Enactment act that created a process instance.

## 8.12.3 Class Actual Situation

An individual situation that actually exists, happened in the past or will exist, not a template or process definition.

### 8.12.31 Direct Supertypes

[Actual Entity](#), [Situation](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Timeframes

### 8.12.32 Associations

/ has sighting : [Sighting](#) [\*] Subsets: relates:[Anything](#)

Sightings that have sighted an actual situation.

/ observed by : [Observation](#) [\*] Subsets: relates:[Anything](#)

Observations of an entity.

## 8.12.4 Class Actual State

A condition that has or does exist.

### 8.12.41 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Foundational Concepts::Timeframes

## 8.12.5 Class Current Situation

A situation that is actually occurring at the moment.

### 8.12.51 Direct Supertypes

[Actual Situation](#), [Situation](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Timeframes

## 8.12.6 Class Non Happening

Situations that have not and will not happen.

### 8.12.61 Direct Supertypes

[Situation](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Timeframes

### 8.12.7 Class Past Situation

A situation that has actually occurred in the past (recognizing that all such statements are subject to confidence).

### 8.12.71 Direct Supertypes

[Actual Situation](#), [Situation](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Timeframes

### 8.12.8 Class Potential Situation

A situation that has not yet happened but has a potential to happen.

### 8.12.81 Direct Supertypes

[Pattern](#), [Situation](#)

**package** Threat-risk-conceptual-model::Foundational Concepts::Timeframes

### 8.12.82 Attributes

 likelihood : [Probability Metric](#)

Possibility that the containing element represents reality.

### 8.12.83 Associations

 indicated by : [Indicator](#) [\*] Subsets: relates:[Anything](#)

Indicator of a possible situation.

 predicted by : [Prediction](#) [\*] Subsets: relates:[Anything](#)

Entity making a prediction.

## 8.13 Threat-risk-conceptual-model::Generic Concepts

Concepts that are common across many domains and purposes. Intended as a reuse library.

### 8.13.1 Diagram: Generic Concept Library

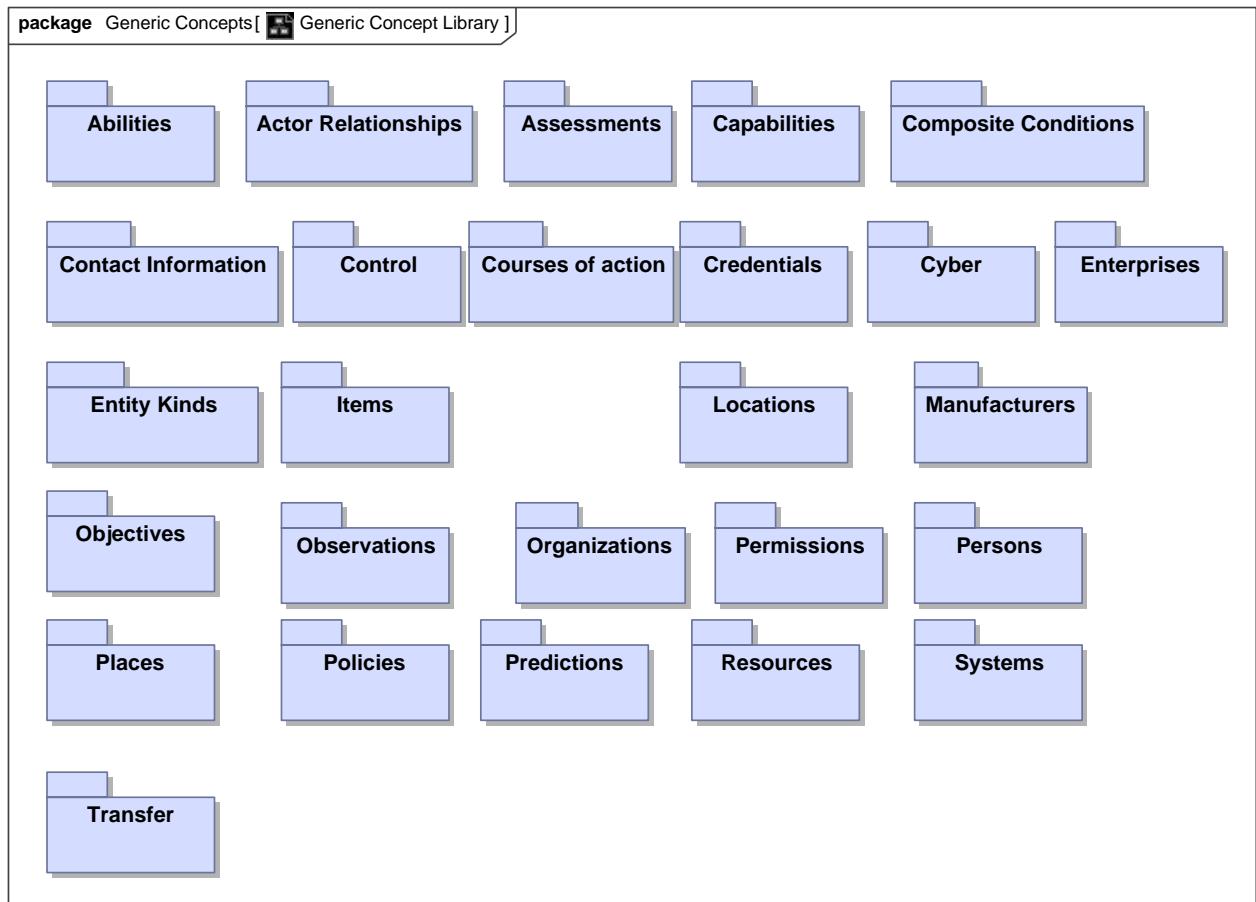


Figure 16. Generic Concept Library

## 8.14 Threat-risk-conceptual-model::Generic Concepts::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* occurrence. When an actor alters an Ability (of themselves or others) they are playing the role of a *Facilitator* who performs an *Alter Capacity*.

Abilities are the instantiation of a capability.

### 8.14.1 Diagram: Ability

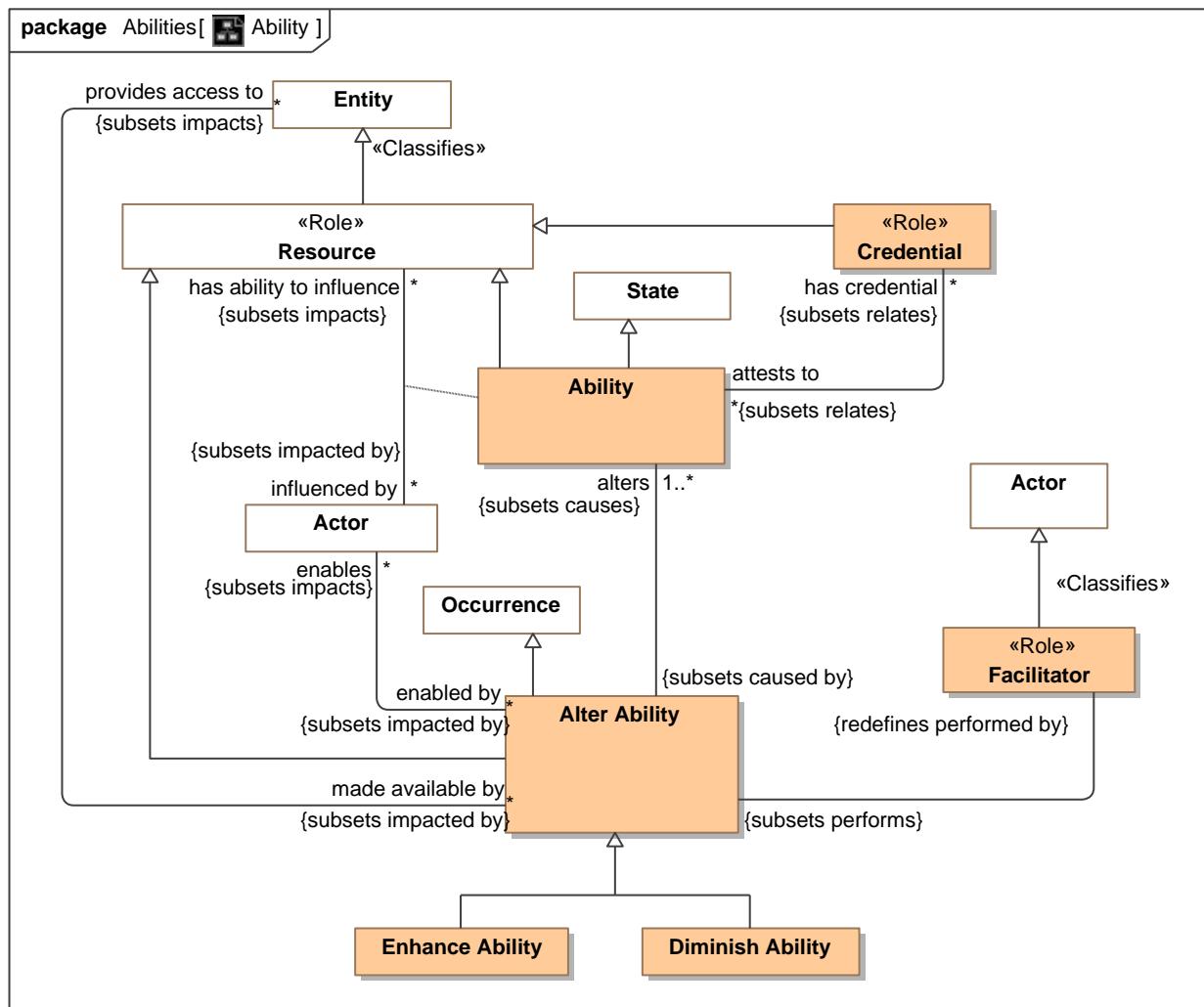


Figure 17. Ability

## **8.14.2 Association Class Ability**

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

Note that as with any entity, an Ability can also be categorized as a resource. In some context called a capability.

### **8.14.21 Direct Supertypes**

Resource, State

**package** Threat-risk-conceptual-model::Generic Concepts::Abilities

### **8.14.21 Association Ends**

 influenced by : Actor [\*] Subsets: relates:Anything

A resource made available to an actor as a part of a capability.

 has ability to influence : Resource [\*] Subsets: relates:Anything

The resource an actor can utilize as part of a capability.

### **8.14.22 Associations**

 : Alter Ability Subsets: caused by:Situation

 has credential : Credential [\*] Subsets: relates:Anything

Provides proof of a capability.

## **8.14.3 Class Alter Ability**

The occurrence of providing or removing abilities - the access of an actor to resources.

### **8.14.31 Direct Supertypes**

Occurrence, Resource

**package** Threat-risk-conceptual-model::Generic Concepts::Abilities

### **8.14.32 Associations**

 alters : Ability [1..\*] Subsets: causes:Situation

A capability which is enhanced/created or reduced/removed.

 provides access to : Entity [\*] Subsets: impacts:Entity

The entity that will be used as the capability of an actor.

 enables : Actor [\*] Subsets: impacts:Entity

A resource made available to an actor by an occurrence of the Alter Capability.

 : Facilitator Redefines: performed by:Actor

#### **8.14.4 Class Diminish Ability**

The reduction of the capabilities of an actor.

##### 8.14.4.1 Direct Supertypes

[Alter Ability](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Abilities

#### **8.14.5 Class Enhance Ability**

Any occurrence that increases the resources available to an actor.

##### 8.14.5.1 Direct Supertypes

[Alter Ability](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Abilities

#### **8.14.6 Class Facilitator**

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

##### 8.14.6.1 Direct Supertypes

[Actor](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Abilities

##### 8.14.6.2 Associations

 : [Alter Ability](#) Subsets: performs:[Occurrence](#)

## 8.15 Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

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.

### 8.15.1 Diagram: Actor Identifiers

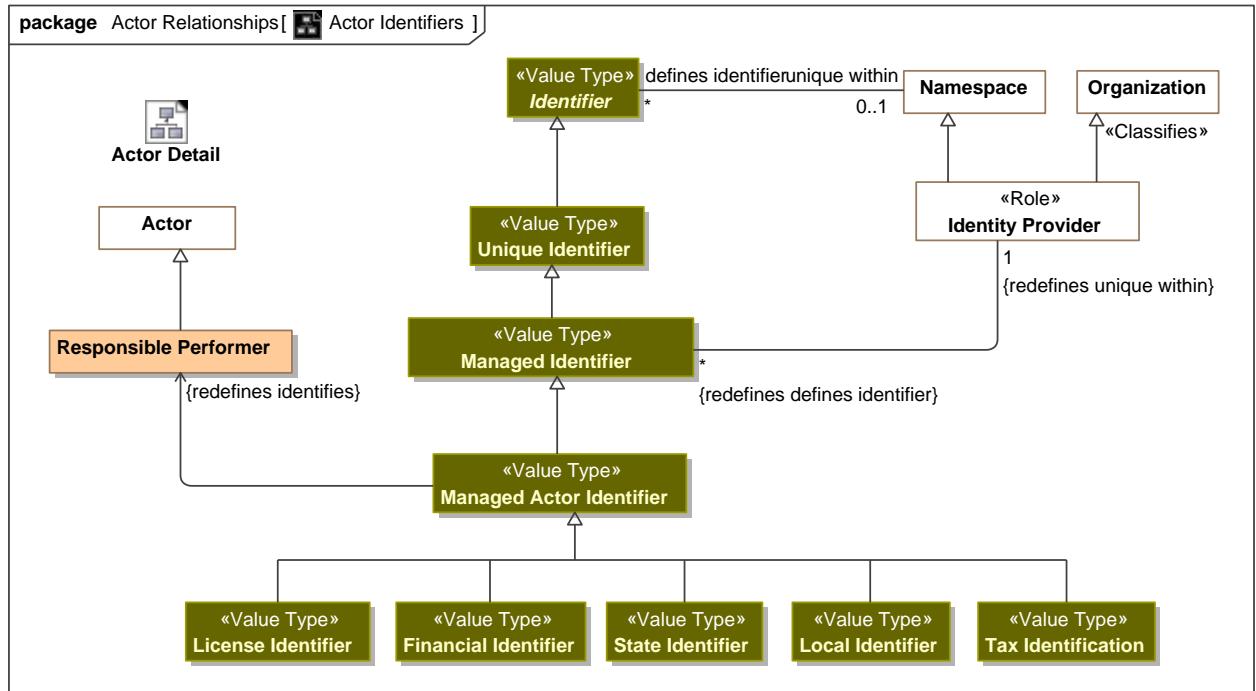


Figure 18. Actor Identifiers

## 8.15.2 Diagram: Actor/Organization Relations

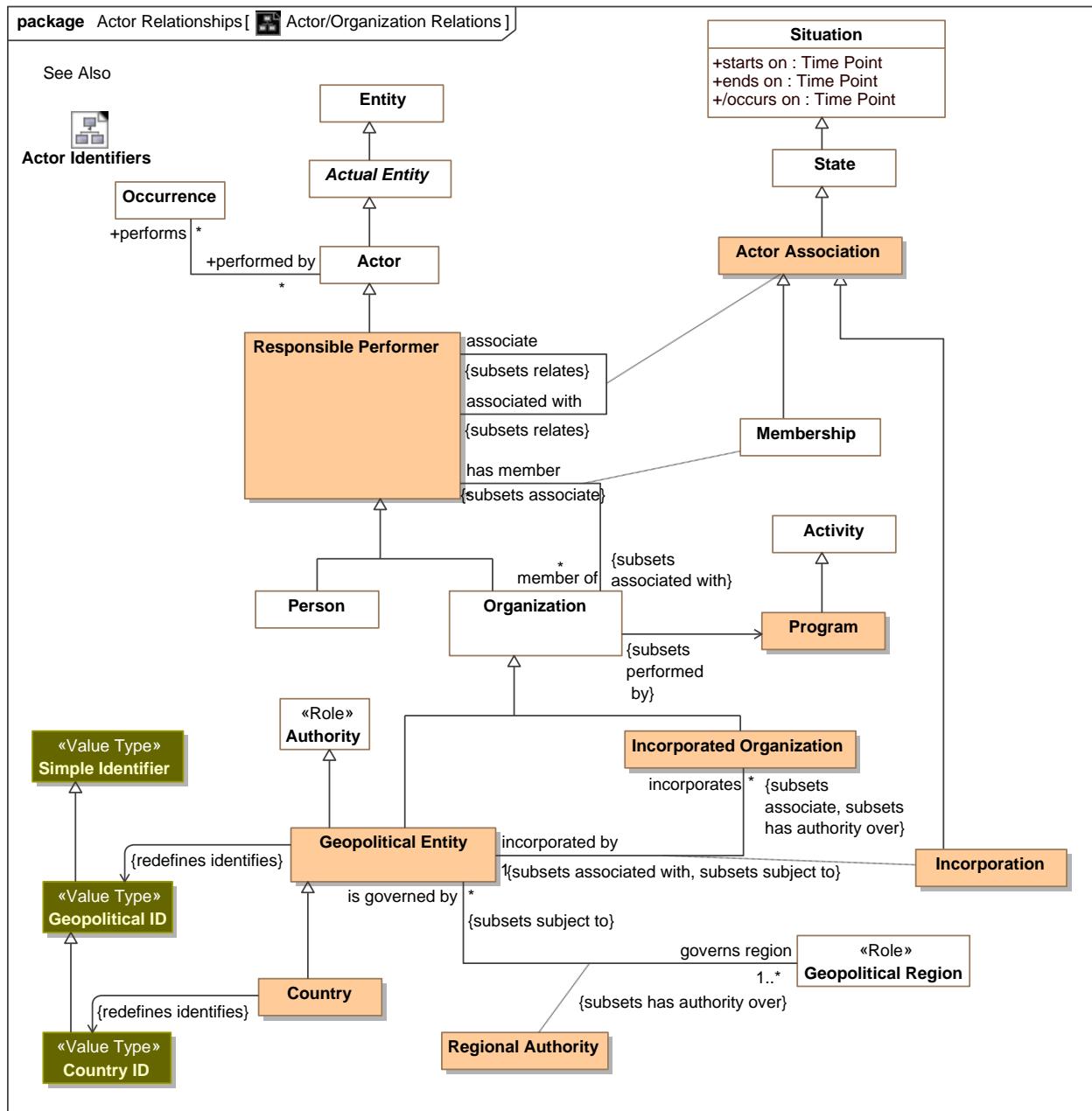


Figure 19. Actor/Organization Relations

Actor associations define the concept of an organization and provide a general framework for associations between actors with the use of an Actor Association.

### **8.15.3 Association Class Actor Association**

An *Actor Association* defines some 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.

#### **8.15.31 Direct Supertypes**

[State](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

#### **8.15.31 Association Ends**

 associate : [Responsible Performer](#) Subsets: performs:[Occurrence](#)

The actor associated with another.

 associated with : [Responsible Performer](#) Subsets: performs:[Occurrence](#)

Another actor the actor is associated with.

### **8.15.4 Class Country**

A nation with its own government, occupying a particular territory (not necessarily contiguous).

#### **8.15.41 Direct Supertypes**

[Geopolitical Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

#### **8.15.42 Associations**

 : [Country ID](#)

### **8.15.5 Class Country ID**

A code, ID, or name for a country.

#### **8.15.51 Direct Supertypes**

[Geopolitical ID](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

### **8.15.6 Class Geopolitical Entity**

The governing body of a nation, state, tribe or community. A Geopolitical organization.

#### **8.15.61 Direct Supertypes**

[Authority, Organization](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

### 8.15.62 Associations

 governs region : [Geopolitical Region](#) [1..\*] Subsets: has authority over:[Controlled Entity](#)

Region governed by a geopolitical authority.

 incorporates : [Incorporated Organization](#) [\*] Subsets: associate:[Responsible Performer](#) has authority over:[Controlled Entity](#)

Organizations incorporated by a government.

 : [Geopolitical ID](#)

### 8.15.7 Class Geopolitical ID

A code/ID/administered name for a geopolitical organization with governmental authority e.g., city, state, county, tribe. There is a specific subtype for countries.

### 8.15.71 Direct Supertypes

[Simple Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

### 8.15.8 Class Incorporated Organization

An organization recognized by and incorporated by a recognized government.

### 8.15.81 Direct Supertypes

[Organization](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

### 8.15.82 Associations

 incorporated by : [Geopolitical Entity](#) [1] Subsets: associated with:[Responsible Performer](#) subject to:[Authority](#)

Geopolitical entity incorporating an organization.

### 8.15.9 Association Class Incorporation

Process by which individuals are voluntarily united into a new entity through the creation of an artificial, intangible, and legal person called a corporation.

### 8.15.91 Direct Supertypes

[Actor Association](#), [Subject to Authority](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

### **8.15.91 Association Ends**

 incorporated by : [Geopolitical Entity](#) [1] Subsets: associated with:[Responsible Performer](#) subject to:[Authority](#)

Geopolitical entity incorporating an organization.

 incorporates : [Incorporated Organization](#) [\*] Subsets: associated with:[Responsible Performer](#) subject to:[Authority](#)

Organizations incorporated by a government.

### **8.15.10 Class License Identifier**

An identification that references a license certification or registration of a person or organization for some purpose.[NIEM]

#### **8.15.101 Direct Supertypes**

[Managed Actor Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

### **8.15.11 Class Local Identifier**

An identification assigned at a local level to a person or organization.

#### **8.15.111 Direct Supertypes**

[Managed Actor Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

### **8.15.12 Class Managed Actor Identifier**

An identifier for an actor where the identifier is managed by some authority.

#### **8.15.121 Direct Supertypes**

[Managed Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

#### **8.15.122 Associations**

 : [Responsible Performer](#) Redefines: identifies:[Entity](#)

### **8.15.13 Association Class Regional Authority**

The authority over a region.

#### **8.15.131 Direct Supertypes**

[Subject to Authority](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

### **8.15.131 Association Ends**

 governs region : [Geopolitical Region](#) [1..\*] *Redefines:* identifies: [Entity](#)

Region governed by a geopolitical authority.

 is governed by : [Geopolitical Entity](#) [\*] *Redefines:* identifies: [Entity](#)

A governing authority for a region.

### **8.15.14 Class State Identifier**

An identification of a person based on a state-issued ID.[NIEM]

#### **8.15.141 Direct Supertypes**

[Managed Actor Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

### **8.15.15 Class Tax Identification**

A tax identification assigned to a person or organization.

#### **8.15.151 Direct Supertypes**

[Managed Actor Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Actor Relationships

## 8.16 Threat-risk-conceptual-model::Generic Concepts::Assessments

Concepts relating to evaluation of an entity.

### 8.16.1 Diagram: Assessment

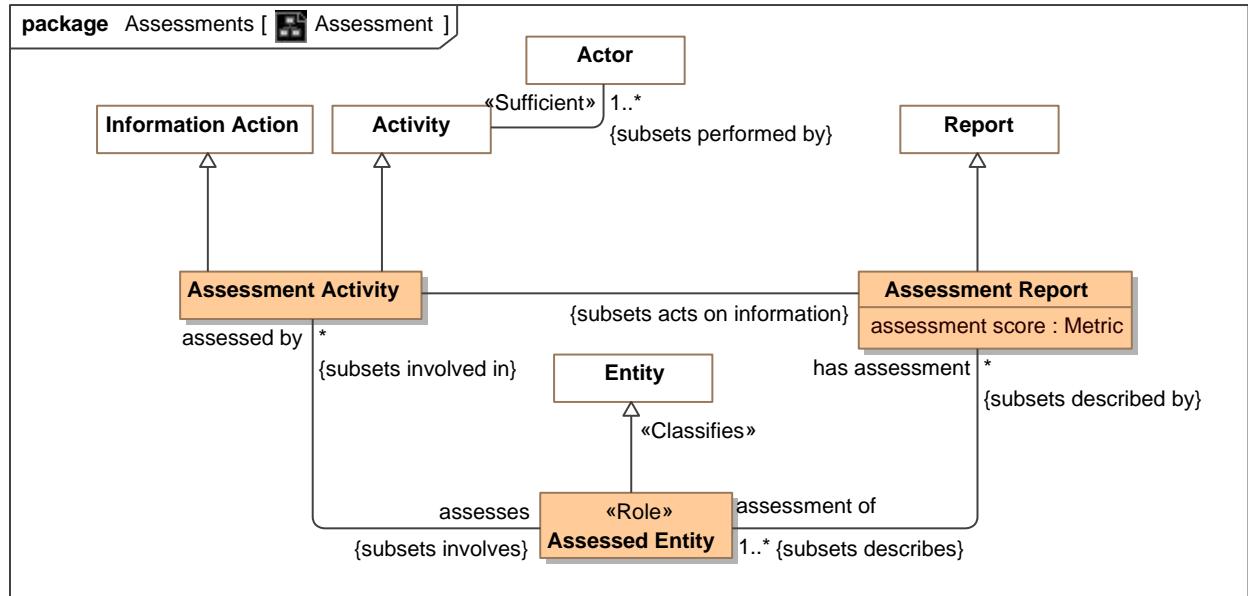


Figure 20. Assessment

The evaluation or estimation of the nature, quality, or ability of someone or something.

### 8.16.2 Class Assessed Entity

Role of an entity that is assessed.

#### 8.16.21 Direct Supertypes

[Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Assessments

#### 8.16.22 Associations

/ assessed by : [Assessment Activity](#) [\*] Subsets: involved in:[Situation](#)

Entity performing an assessment.

/ has assessment : [Assessment Report](#) [\*] Subsets: described by:[Information Object](#)

Assessments of an entity.

### **8.16.3 Class Assessment Activity**

The act of evaluating or estimating the nature, ability, or quality of something.

An evaluation, appraisal, or assessment of something or someone.[NIEM]

#### 8.16.31 Direct Supertypes

[Activity](#), [Information Action](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Assessments

#### 8.16.32 Associations

/ : [Assessment Report](#) Subsets: acts on information:[Information Object](#)

/ assesses : [Assessed Entity](#) Subsets: involves:[Actor](#)

Entity assessed by an assessment activity

### **8.16.4 Class Assessment Report**

The evaluation or estimation of the nature, quality, or ability of someone or something.

#### 8.16.41 Direct Supertypes

[Report](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Assessments

#### 8.16.42 Attributes

○ assessment score : [Metric](#)

An evaluation score of an assessment.[NIEM]

#### 8.16.43 Associations

/ : [Assessment Activity](#)

/ assessment of : [Assessed Entity](#) [1..\*] Subsets: describes:[Anything](#)

Entity assessed by an assessment.

## 8.17 Threat-risk-conceptual-model::Generic Concepts::Capabilities

Concepts relating to the capability of actors to have a desired effect.

### 8.17.1 Diagram: Capability

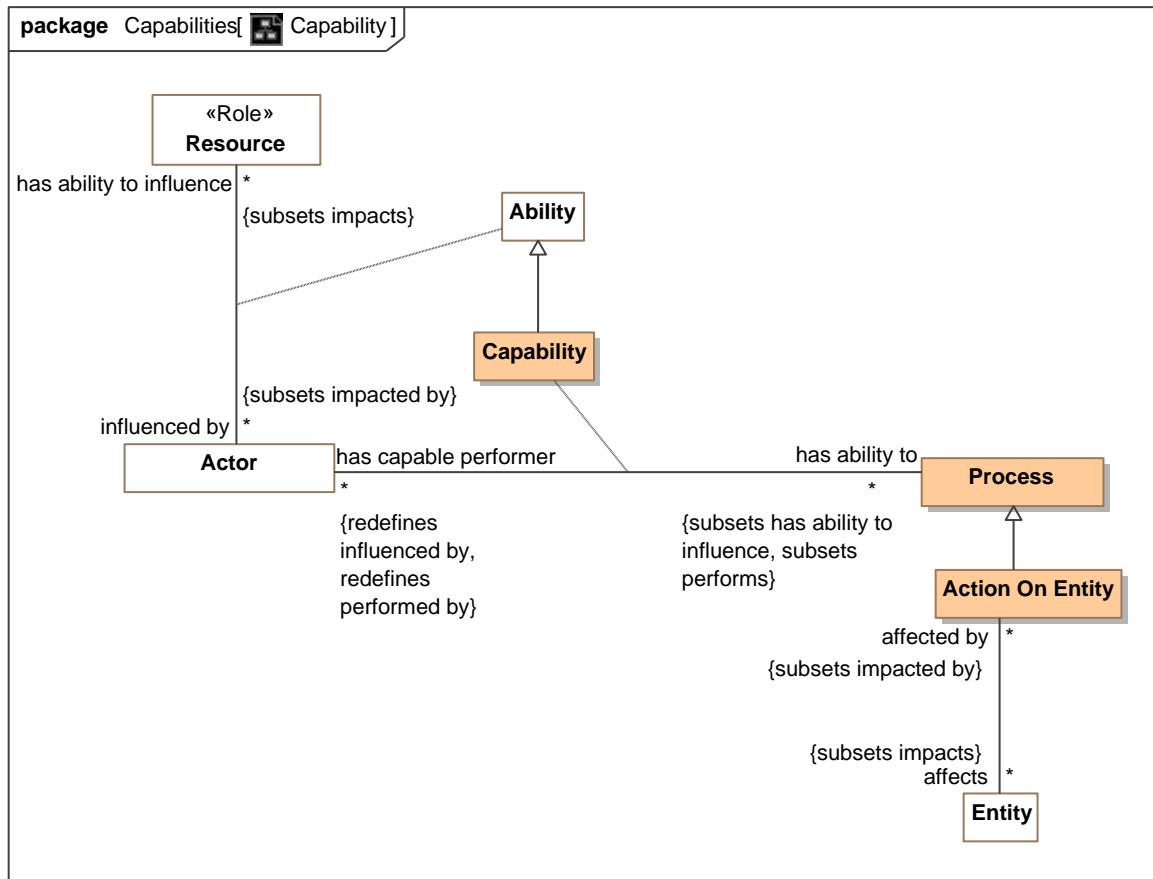


Figure 21. Capability

### 8.17.2 Association Class Capability

A capability is the ability of an actor to have an effect by enacting a process

#### 8.17.21 Direct Supertypes

[Ability](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Capabilities

### **8.17.21 Association Ends**

 has ability to : [Process](#) [\*] Subsets: describes:[Anything](#)

The ability of an actor to perform a process.

 has capable performer : [Actor](#) [\*] Subsets: describes:[Anything](#)

Actors capable of performing an process.

## 8.18 Threat-risk-conceptual-model::Generic Concepts::Composite Conditions

Composite conditions provide for "and"/"or" evaluation of causality between situations.

### 8.18.1 Diagram: Composite Condition

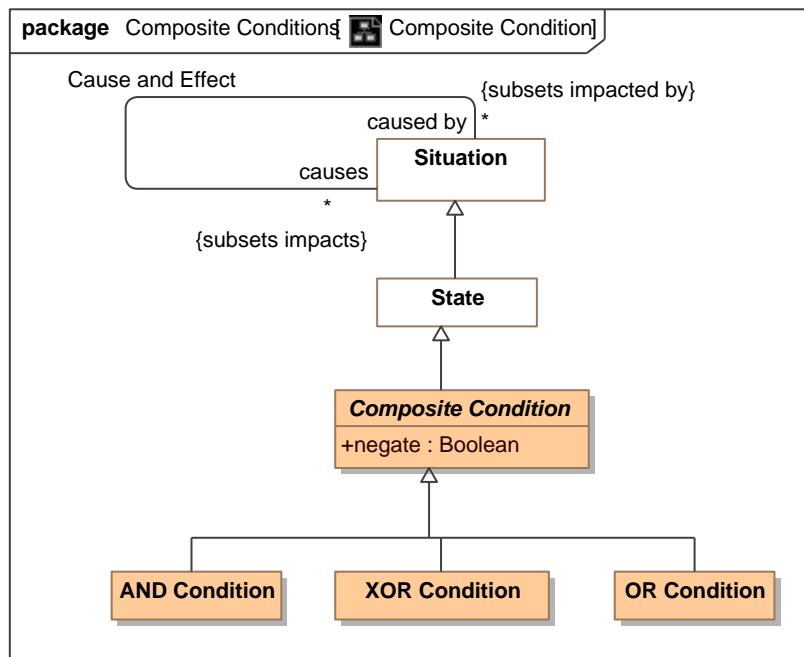


Figure 22. Composite Condition

### 8.18.2 Class AND Condition

True only when all causes are true - AND

#### 8.18.21 Direct Supertypes

[Composite Condition](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Composite Conditions

### 8.18.3 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 occurrences, states, and composite conditions can then be combined to represent fault, flow or dependency graphs.

#### 8.18.31 Direct Supertypes

[State](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Composite Conditions

#### 8.18.32 Attributes

◆ **negate** : [Boolean](#)

Negates the logic of the complex event - NOT

### 8.18.4 Class OR Condition

True when any cause is true - OR

#### 8.18.41 Direct Supertypes

[Composite Condition](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Composite Conditions

### 8.18.5 Class XOR Condition

True only when exactly one cause is true - XOR

#### 8.18.51 Direct Supertypes

[Composite Condition](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Composite Conditions

## 8.19 Threat-risk-conceptual-model::Generic Concepts::Contact Information

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

### 8.19.1 Diagram: Contact Information

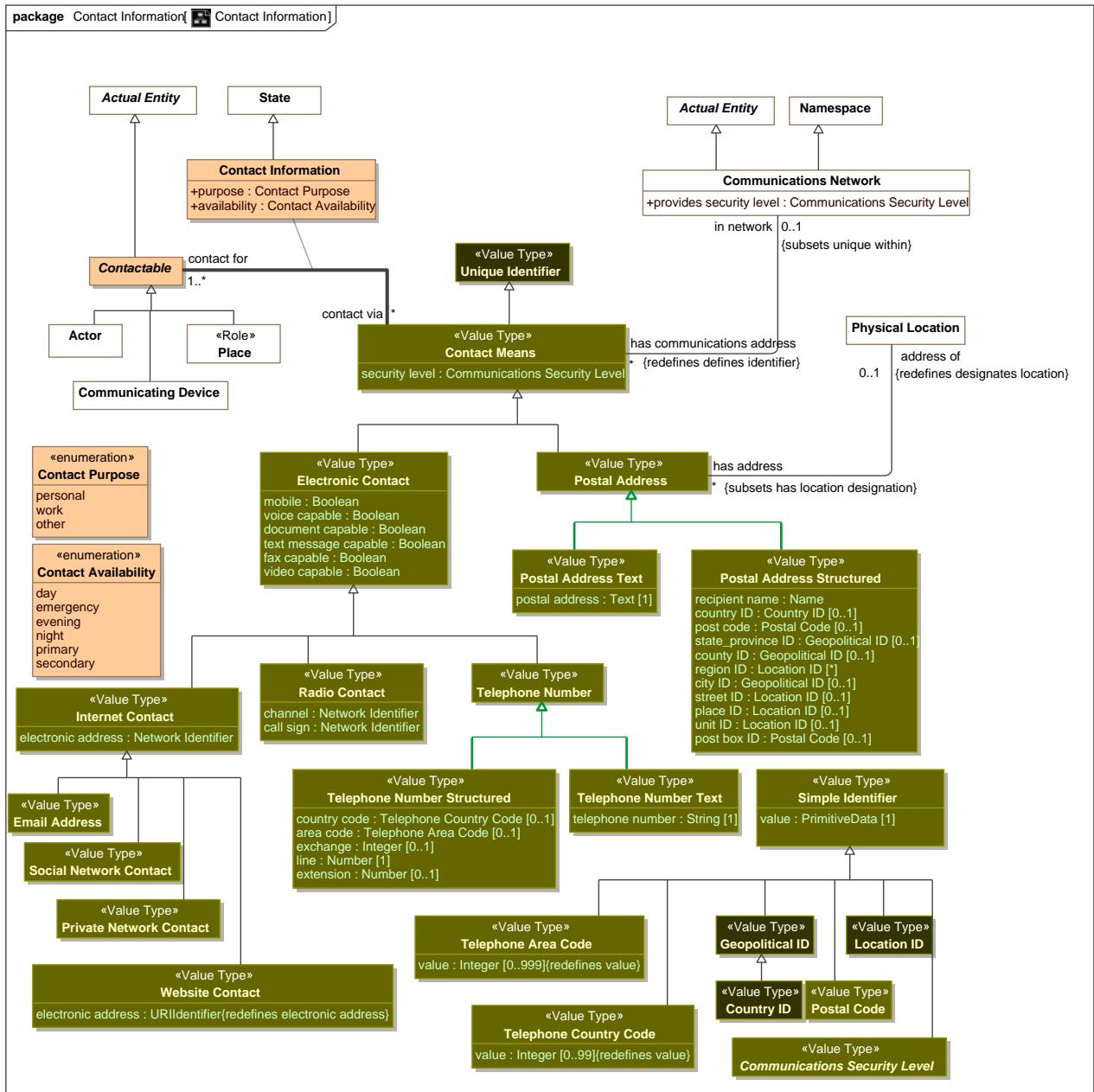


Figure 23. Contact Information

## **8.19.2 Class Communications Security Level**

An abstract type for levels of security in communications.

### 8.19.21 Direct Supertypes

Simple Identifier

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

## **8.19.3 Association Class Contact Information**

Information relative to communicating with an entity.

### 8.19.31 Direct Supertypes

State

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### **8.19.31 Association Ends**

 contact via : [Contact Means](#) [\*] Subsets: describes:[Anything](#)

A way to contact an actor or place.

 contact for : [Contactable](#) [1..\*] Subsets: describes:[Anything](#)

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

### 8.19.32 Attributes

 purpose : [Contact Purpose](#)

Purposes for contacting an entity, primarily work and personal.

 availability : [Contact Availability](#)

When a contact method is available.

## **8.19.4 Class Contact Means**

Anything that may be used to contact an individual.

### 8.19.41 Direct Supertypes

Unique Identifier

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.42 Attributes

 security level : [Communications Security Level](#)

The level of security asserted for this communications channel. May default to the security level of the communications network.

#### 8.19.43 Associations

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

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

 in network : [Communications Network](#) [0..1] Subsets: unique within:[Namespace](#)

Network authority in which a contact information identifier is defined.

#### 8.19.5 Class Contactable

Anything that can be contacted via contact information, e.g., people, organizations and places.

#### 8.19.51 Direct Supertypes

[Actual Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

#### 8.19.52 Associations

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

A way to contact an actor or place.

#### 8.19.6 Class Electronic Contact

Contact information that enables communications via electronic means.

#### 8.19.61 Direct Supertypes

[Contact Means](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

#### 8.19.62 Attributes

 mobile : [Boolean](#)

Contact method is mobile - not fixed to a location.

 voice capable : [Boolean](#)

Contact method is voice capable.

 document capable : [Boolean](#)

Contact method is capable of receiving documents, e.g., email.

 text message capable : [Boolean](#)

Contact method is voice capable of receiving text messages of limited length..

 fax capable : [Boolean](#)

Contact method is fax capable.

 video capable : [Boolean](#)

Contact method is video capable.

### **8.19.7 Class Email Address**

Information for the delivery of mail via an electronic network.

#### **8.19.7.1 Direct Supertypes**

[Internet Contact](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### **8.19.8 Class Internet Contact**

A means of contact that provides for the digital electronic transmission of information via the Internet or a private network.

#### **8.19.8.1 Direct Supertypes**

[Electronic Contact](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

#### **8.19.8.2 Attributes**

 electronic address : [Network Identifier](#)

Electronic address by which to contact the entity.

### **8.19.9 Class Postal Address**

An address able to be used to deliver physical mail which may or may not represent a static physical location.

#### **8.19.9.1 Direct Supertypes**

[Contact Means](#), [Location Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

#### **8.19.9.2 Associations**

 address of : [Physical Location](#) [0..1] *Redefines:* designates location:[Physical Location](#)

Location identified 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.

### **8.19.10 Class Postal Address Structured**

A structured representation of a postal address.

### 8.19.101 Direct Supertypes

[Postal Address](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.102 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".

◊ country ID : [Country ID](#) [0..1]

Postal country identifier.

◊ post code : [Postal Code](#) [0..1]

Postal code identifier.

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. [OGC]

◊ state\_province ID : [Geopolitical ID](#) [0..1]

Postal state identifier.

◊ county ID : [Geopolitical ID](#) [0..1]

Postal county identifier.

◊ region ID : [Location ID](#) [\*]

Postal region identifier.

◊ city ID : [Geopolitical ID](#) [0..1]

Postal city identifier.

◊ street ID : [Location ID](#) [0..1]

Postal street identifier.

◊ 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.

◊ post box ID : [Postal Code](#) [0..1]

Post box id.

### 8.19.11 Class Postal Address Text

A textual representation of a postal address.

### 8.19.111 Direct Supertypes

[Postal Address](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

#### 8.19.112 Attributes

- ◊ postal address : [Text](#) [1]

Textual postal address.

### 8.19.12 Class Postal Code

A code defined for the purposes of delivering physical mail. "Zip code" in the U.S.

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. [OGC]

#### 8.19.121 Direct Supertypes

[Simple Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.13 Class Private Network Contact

Contact via a private network.

#### 8.19.131 Direct Supertypes

[Internet Contact](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.14 Class Radio Contact

Contact via radio.

#### 8.19.141 Direct Supertypes

[Electronic Contact](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

#### 8.19.142 Attributes

- ◊ channel : [Network Identifier](#)

Radio channel.

- ◊ call sign : [Network Identifier](#)

Radio or user call sign.

### 8.19.15 Class Social Network Contact

Contact via a social network.

### 8.19.151 Direct Supertypes

[Internet Contact](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.16 Class Telephone Area Code

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.

### 8.19.161 Direct Supertypes

[Simple Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.162 Attributes

 value : [Integer](#) [0..999]

3 digit area code.

### 8.19.17 Class Telephone Country Code

2 digit Telephone codes for countries.

### 8.19.171 Direct Supertypes

[Simple Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.172 Attributes

 value : [Integer](#) [0..99]

Country code digits.

### 8.19.18 Class Telephone Number

A way to contact an actor via a telephone.

### 8.19.181 Direct Supertypes

[Electronic Contact](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.19 Class Telephone Number Structured

Structured representation of a telephone number.

### 8.19.191 Direct Supertypes

[Telephone Number](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.192 Attributes

◊ country code : [Telephone Country Code](#) [0..1]

Telephone country code.

◊ area code : [Telephone Area Code](#) [0..1]

Telephone area code.

◊ exchange : [Integer](#) [0..1]

Telephone exchange.

◊ line : [Number](#) [1]

Telephone line number.

◊ extension : [Number](#) [0..1]

Telephone extension number.

## 8.19.20 Class Telephone Number Text

Unstructured (text) representation of a telephone number.

### 8.19.201 Direct Supertypes

[Telephone Number](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.202 Attributes

◊ telephone number : [String](#) [1]

Textual telephone number.

## 8.19.21 Class Website Contact

A website that can be used to contact an individual.

### 8.19.211 Direct Supertypes

[Internet Contact](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Contact Information

### 8.19.212 Attributes

◊ electronic address : [URIIdentifier](#)

Electronic address by which to contact the entity.

### **8.19.213 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 Concepts::Contact Information  
public enum Contact Availability  
{day, emergency, evening, night, primary, secondary}
```

### **8.19.213Literals**

 day

Daytime contact.

 emergency

Emergency contact.

 evening

Late day or early night contact.

 night

Late night contact.

 primary

Primary contact.

 secondary

Secondary or alternate contact.

### **8.19.214 Enumeration Contact Purpose**

Possible purposes for contact information.[NIEM]

```
package Threat-risk-conceptual-model::Generic Concepts::Contact Information  
public enum Contact Purpose  
{personal, work, other}
```

### **8.19.214Literals**

 personal

Personal communications.

 work

Work communications.

 other

Communications other than work or personal.

## 8.20 Threat-risk-conceptual-model::Generic Concepts::Control

Concepts relating to actor's control over anything by any means.

### 8.20.1 Diagram: Control

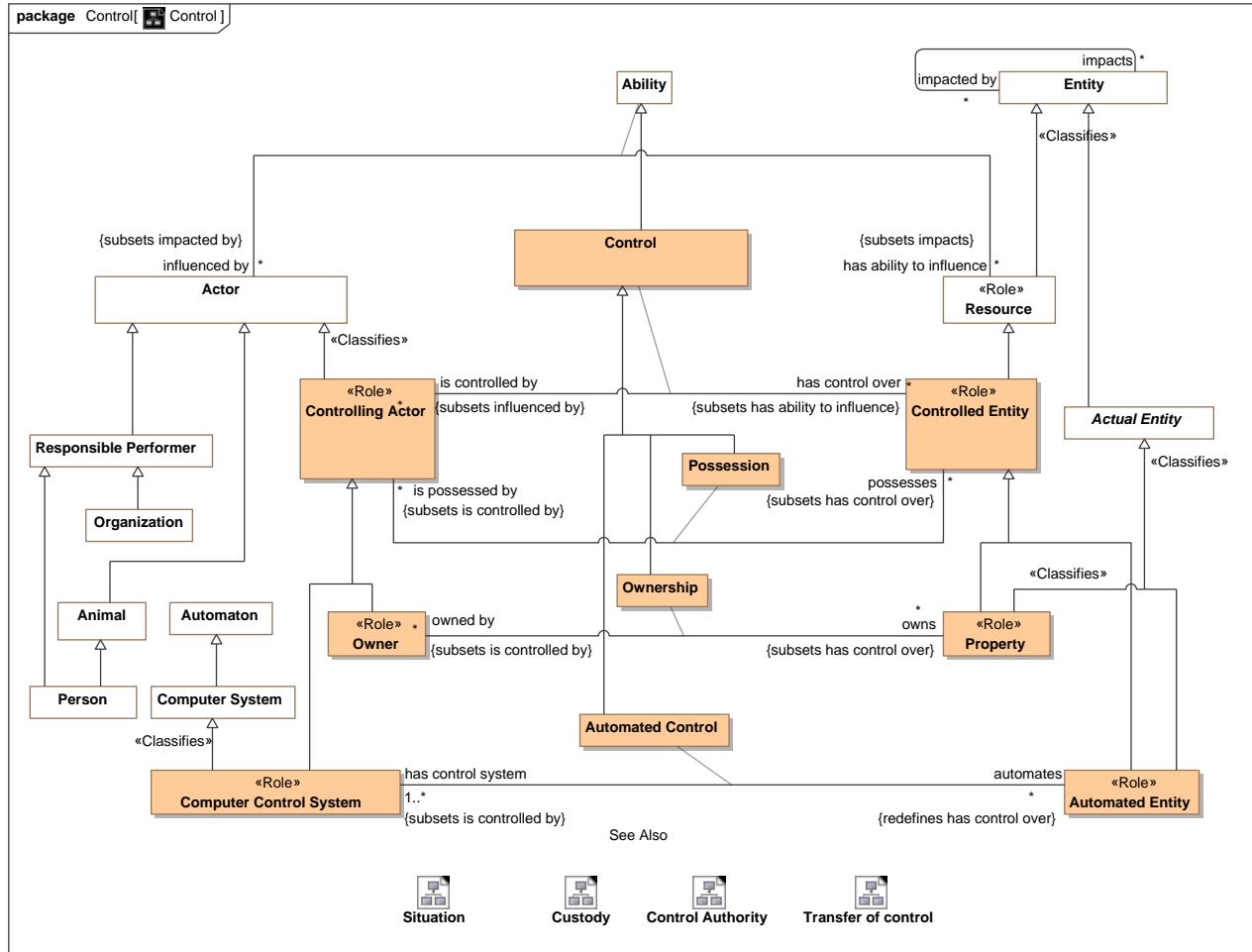


Figure 24. Control

## 8.20.2 Diagram: Control Authority

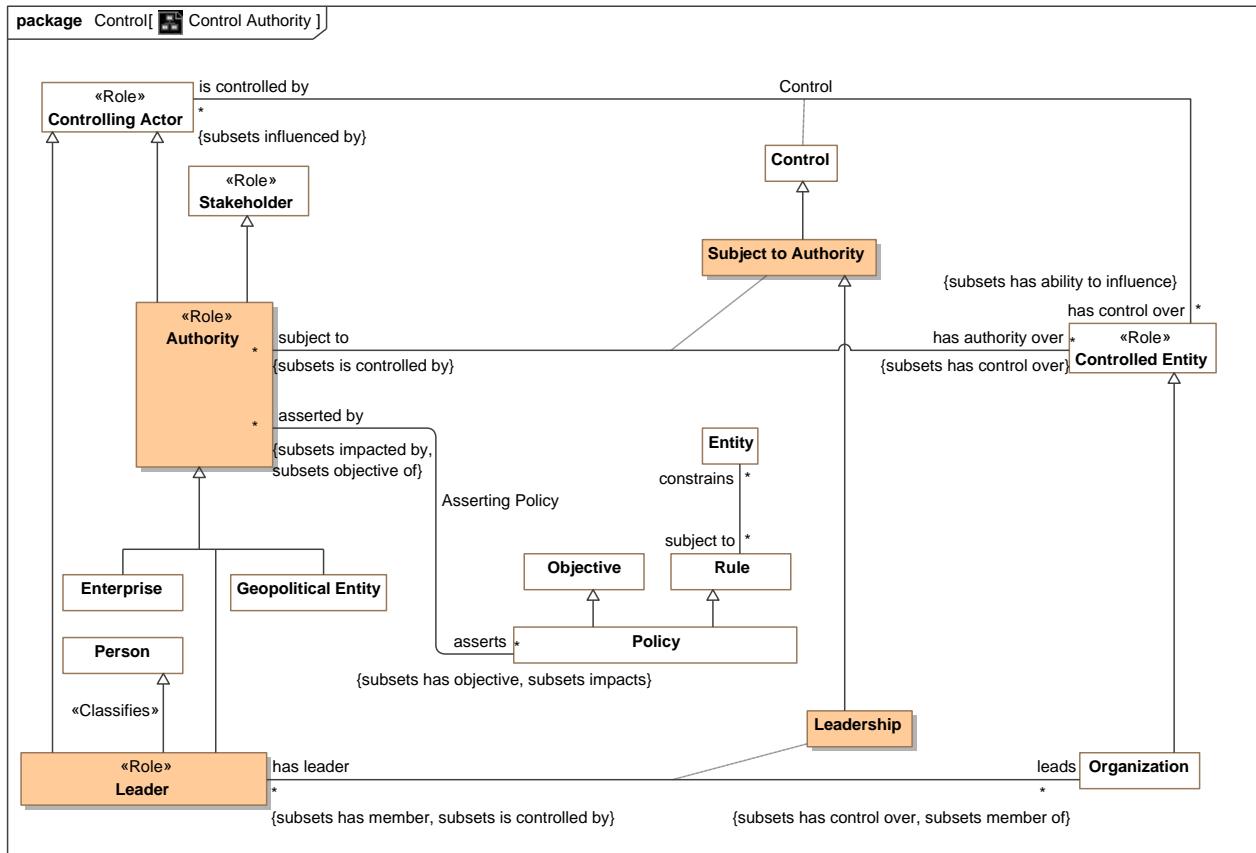
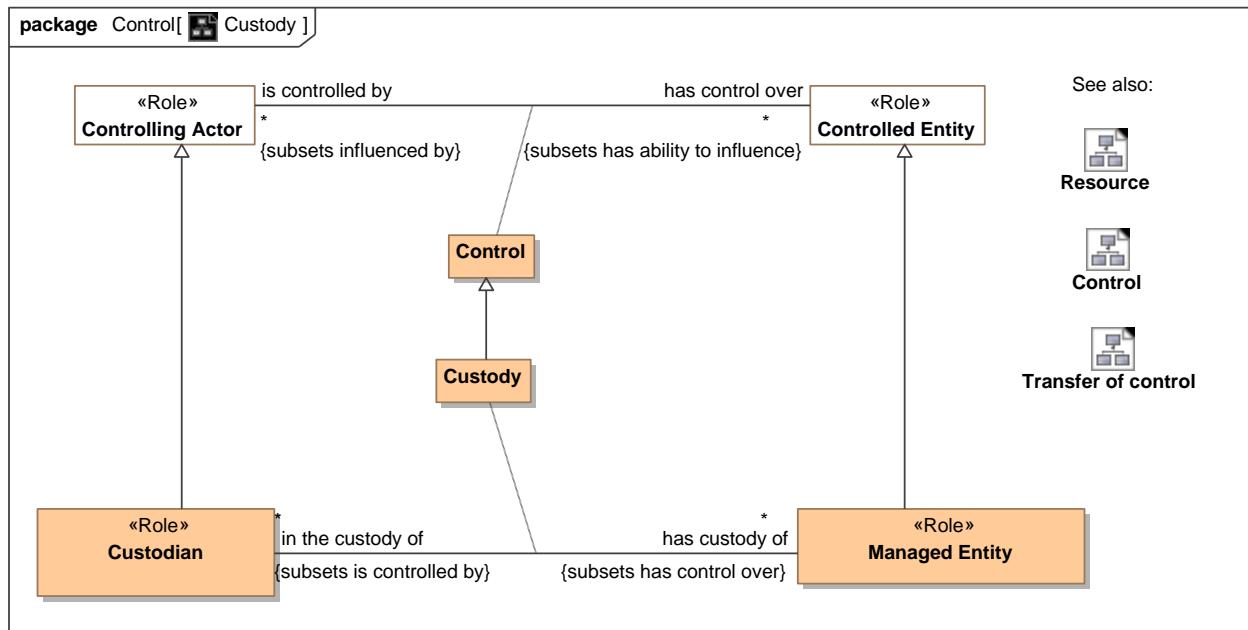


Figure 25. Control Authority

### 8.20.3 Diagram: Custody



**Figure 26. 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.

#### 8.20.4 Diagram: Transfer of control

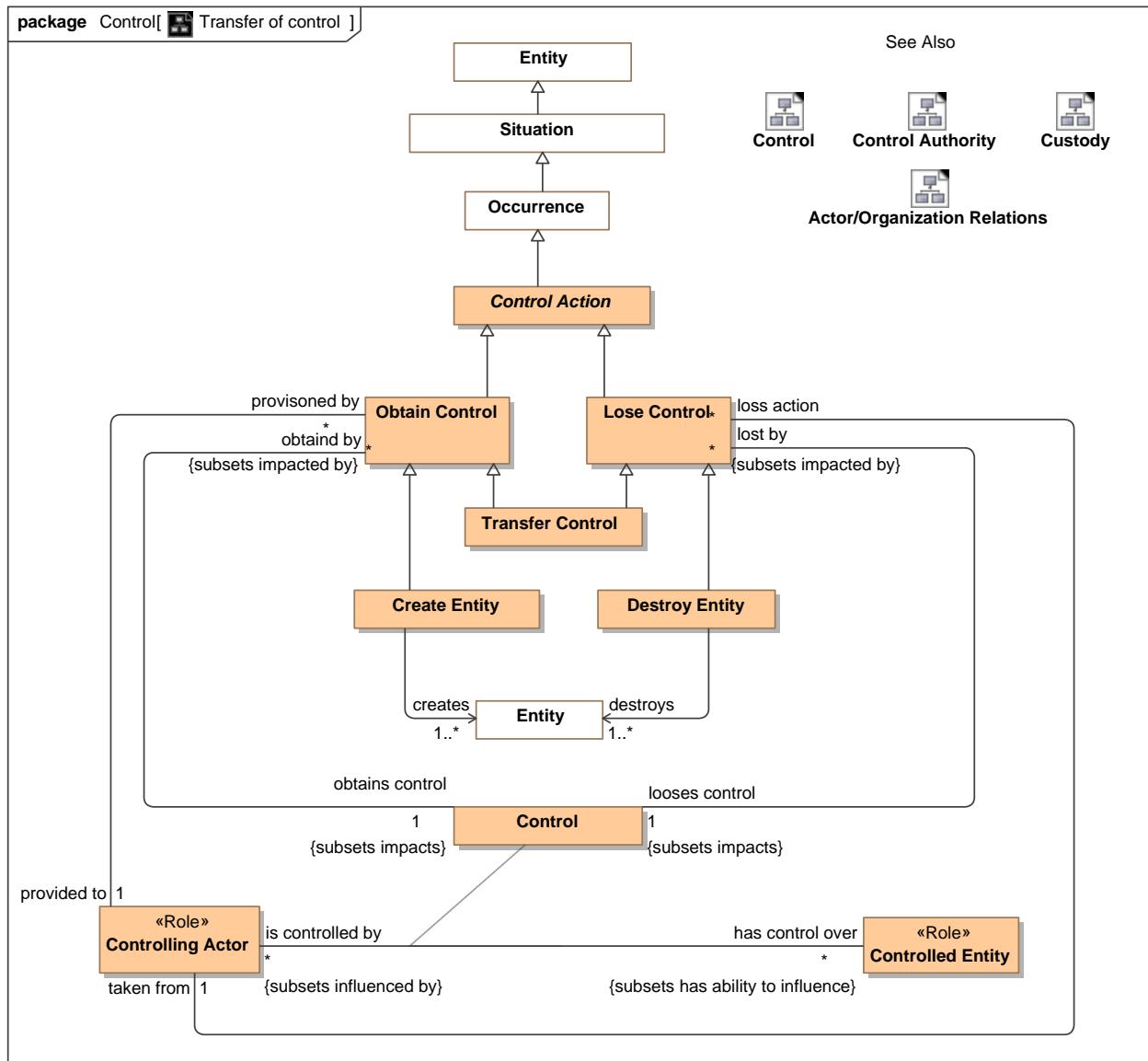


Figure 27. Transfer of control

#### 8.20.5 Association Asserting Policy

The assertion of a policy.

package Threat-risk-conceptual-model::Generic Concepts::Control

##### 8.20.51 Association Ends

 asserts : [Policy](#) [\*] Redefines: designates location: [Physical Location](#)

A policy asserted by an authority.

 asserted by : [Authority](#) [\*] Redefines: designates location: [Physical Location](#)

The authority that asserts a policy

## 8.20.6 Class Authority

An actor with authority over resources.

### 8.20.6.1 Direct Supertypes

[Controlling Actor](#), [Stakeholder](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

### 8.20.6.2 Associations

 has authority over : [Controlled Entity](#) [\*] Subsets: has control over:[Controlled Entity](#)

Resources an authority has authority over.

 asserts : [Policy](#) [\*] Subsets: impacts:[Entity](#) has objective:[Objective](#)

A policy asserted by an authority.

## 8.20.7 Association Class Automated Control

Control of an entity by an automated control system.

### 8.20.7.1 Direct Supertypes

[Control](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

### 8.20.7.1 Association Ends

 automates : [Automated Entity](#) [\*] Subsets: impacts:[Entity](#) has objective:[Objective](#)

Entity that a control system controls.

 has control system : [Computer Control System](#) [1..\*] Subsets: impacts:[Entity](#) has objective:[Objective](#)

Control system for an automated entity. e.g., an automated machine or facility.

## 8.20.8 Class Automated Entity

Any place or thing all or partially controlled by automation.

### 8.20.8.1 Direct Supertypes

[Actual Entity](#), [Controlled Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

## 8.20.82 Associations

 has control system : [Computer Control System](#) [1..\*] Subsets: is controlled by:[Controlling Actor](#)

Control system for an automated entity. e.g., an automated machine or facility.

## 8.20.9 Class Computer Control System

A 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.

## 8.20.91 Direct Supertypes

[Computer System](#), [Controlling Actor](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

## 8.20.92 Associations

 automates : [Automated Entity](#) [\*] Redefines: has control over:[Controlled Entity](#)

Entity that a control system controls.

## 8.20.10 Association Class Control

The control, use or influence of an actor over any entity. This includes subtypes representing possession, ownership, leadership, and custody.

## 8.20.101 Direct Supertypes

[Ability](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

## 8.20.101 Association Ends

 has control over : [Controlled Entity](#) [\*] Redefines: has control over: [Controlled Entity](#)

Entity which an actor controls in some way - by authority, by possession, physically, etc.

 is controlled by : [Controlling Actor](#) [\*] Redefines: has control over: [Controlled Entity](#)

Actor which controls an entity in some way.

## 8.20.102 Associations

 obtained via : [Obtain Control](#) [1]

An action providing an actor control of an entity.

 lost via : [Lose Control](#) [0..1]

The transfer of control.

 obtaind by : [Obtain Control](#) [\*] Subsets: impacted by:[Entity](#)

Method by which control is obtained.

 lost by : [Lose Control](#) [\*] Subsets: impacted by:[Entity](#)

Action that causes a loss of control.

### **8.20.11 Class Control Action**

Any action that impacts the control of an entity.

#### 8.20.111 Direct Supertypes

Occurrence

**package** Threat-risk-conceptual-model::Generic Concepts::Control

#### 8.20.112 Associations

 changes control of : [Managed Entity](#) [1..\*] Subsets: impacts:[Entity](#)

The transferred entity.

### **8.20.12 Class Controlled Entity**

An entity that is controlled by others in some way.

#### 8.20.121 Direct Supertypes

Resource

**package** Threat-risk-conceptual-model::Generic Concepts::Control

#### 8.20.122 Associations

 is controlled by : [Controlling Actor](#) [\*] Subsets: influenced by:[Actor](#)

Actor which controls an entity in some way.

 is possessed by : [Controlling Actor](#) [\*] Subsets: is controlled by:[Controlling Actor](#)

The individual that possesses something.

 subject to : [Authority](#) [\*] Subsets: is controlled by:[Controlling Actor](#)

The authority that has some control over a resource.

### **8.20.13 Class Controlling Actor**

An actor that asserts control over any entity.

#### 8.20.131 Direct Supertypes

Actor

**package** Threat-risk-conceptual-model::Generic Concepts::Control

#### 8.20.132 Associations

 has control over : [Controlled Entity](#) [\*] Subsets: has ability to influence:[Resource](#)

Entity which an actor controls in some way - by authority, by possession, physically, etc.

 possesses : [Controlled Entity](#) [\*] Subsets: has control over:[Controlled Entity](#)

Something an actor possesses.

 provisioned by : [Obtain Control](#) [\*]

The gaining of control.

 loss action : [Lose Control](#) [\*]

The loss of control.

## 8.20.14 Class Create Entity

The creation of an entity and initial control of it.

### 8.20.141 Direct Supertypes

[Obtain Control](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

### 8.20.142 Associations

 creates : [Entity](#) [1..\*] = ()

Entity created.

## 8.20.15 Class Custodian

An actor who has responsibility for or looks after some managed entity. A Custodian <has custody of> a managed entity via the Custody relation.

### 8.20.151 Direct Supertypes

[Controlling Actor](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

## 8.20.16 Association Class Custody

The act of protecting or taking care of something [merriam-webster.com]

### 8.20.161 Direct Supertypes

[Control](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

## 8.20.161 Association Ends

 has custody of : [Managed Entity](#) [\*]

The entity a custodian has custody of.

 in the custody of : [Custodian](#) [\*]

The custodian of an entity.

### **8.20.17 Class Destroy Entity**

The destruction of an entity under custody.

#### 8.20.171 Direct Supertypes

[Lose Control](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

#### 8.20.172 Associations

 destroys : [Entity](#) [1..\*]

Entity destroyed.

### **8.20.18 Class Leader**

A person who leads or commands a group, organization, or country.

#### 8.20.181 Direct Supertypes

[Authority](#), [Controlling Actor](#), [Person](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

#### 8.20.182 Associations

 leads : [Organization](#) [\*] Subsets: has control over:[Controlled Entity](#) member of:[Organization](#)

An organization a person leads.

### **8.20.19 Association Class Leadership**

The action of leading or governing an organization.

#### 8.20.191 Direct Supertypes

[Control](#), [Membership](#), [Subject to Authority](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

#### **8.20.191Association Ends**

 leads : [Organization](#) [\*] 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.

## **8.20.20 Class Lose Control**

An act resulting in loss of control of an entity.

### 8.20.201 Direct Supertypes

[Control Action](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

### 8.20.202 Associations

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

An act which loses control of an entity.

/ loses control : [Control](#) [1] Subsets: impacts:[Entity](#)

Control that is lost.

/ taken from : [Controlling Actor](#) [1]

Actor that looses control.

## **8.20.21 Class Managed Entity**

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.

### 8.20.211 Direct Supertypes

[Controlled Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

### 8.20.212 Associations

/ has custodial action : [Control Action](#) [1..\*] Subsets: impacted by:[Entity](#)

A transfer of custody for an entity.

## **8.20.22 Class Obtain Control**

The act of obtaining control of an entity.

### 8.20.221 Direct Supertypes

[Control Action](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

### 8.20.222 Associations

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

An act that provides control of an entity.

 obtains control : [Control](#) [1] Subsets: impacts:[Entity](#)

Control obtained by an action.

 provided to : [Controlling Actor](#) [1]

Actor that gains control.

### **8.20.23 Class Owner**

An actor that owns property.

#### 8.20.231 Direct Supertypes

[Controlling Actor](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

#### 8.20.232 Associations

 owns : [Property](#) [\*] Subsets: has control over:[Controlled Entity](#)

Something an owner owns.

### **8.20.24 Association Class Ownership**

The ownership of property by an owner.

#### 8.20.241 Direct Supertypes

[Control](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

#### 8.20.241 Association Ends

 owns : [Property](#) [\*] Subsets: has control over:[Controlled Entity](#)

Something an owner owns.

 owned by : [Owner](#) [\*] Subsets: has control over:[Controlled Entity](#)

Owner of an entity.

### **8.20.25 Association Class Possession**

The act of possession.

#### 8.20.251 Direct Supertypes

[Control](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

## **8.20.251 Association Ends**

 possesses : [Controlled Entity](#) [\*] Subsets: has control over:[Controlled Entity](#)

Something an actor possesses.

 is possessed by : [Controlling Actor](#) [\*] Subsets: has control over:[Controlled Entity](#)

The individual that possesses something.

## **8.20.26 Class Property**

An entity which has an owner.

### **8.20.261 Direct Supertypes**

[Actual Entity](#), [Controlled Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

### **8.20.262 Associations**

 owned by : [Owner](#) [\*] Subsets: is controlled by:[Controlling Actor](#)

Owner of an entity.

## **8.20.27 Association Class Subject to Authority**

The relationship between an authority and what it has authority over.

### **8.20.271 Direct Supertypes**

[Control](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

### **8.20.271 Association Ends**

 has authority over : [Controlled Entity](#) [\*] Subsets: is controlled by:[Controlling Actor](#)

Resources an authority has authority over.

 subject to : [Authority](#) [\*] Subsets: is controlled by:[Controlling Actor](#)

The authority that has some control over a resource.

## **8.20.28 Class Transfer Control**

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

### **8.20.281 Direct Supertypes**

[Lose Control](#), [Obtain Control](#), [Occurrence](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Control

## 8.21 Threat-risk-conceptual-model::Generic Concepts::Courses of action

Courses of action are procedures to deal with specific situations that trigger the course of action. The course of action should result in a specific outcome.

### 8.21.1 Diagram: Course of Action

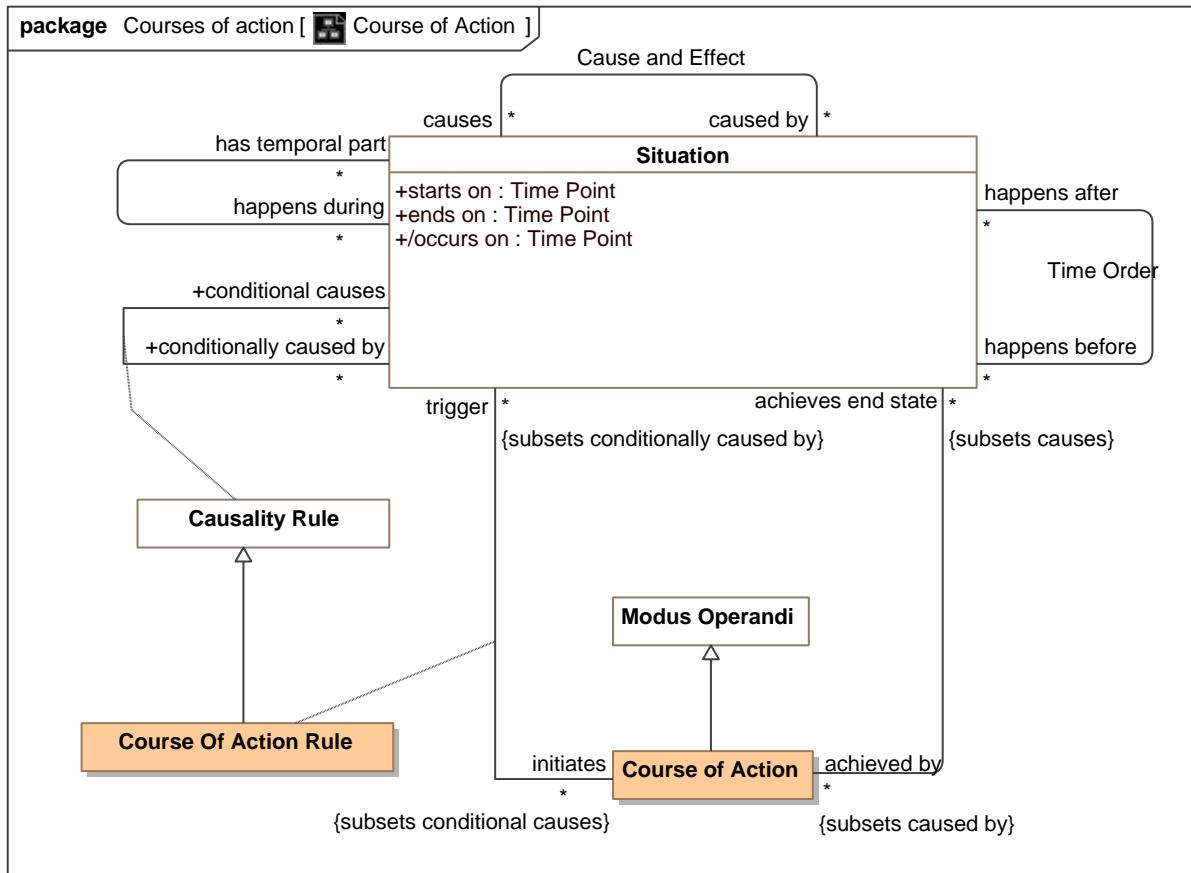


Figure 28. Course of Action

### 8.21.2 Class Course of Action

A procedure adopted to deal with a situation.

#### 8.21.21 Direct Supertypes

[Modus Operandi](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Courses of action

### 8.21.22 Associations

 achieves end state : [Situation](#) [\*] Subsets: causes:[Situation](#)

The situation a course of action results in.

 trigger : [Situation](#) [\*] Subsets: conditionally caused by:[Situation](#)

The situation(s) initiating a course of action.

### 8.21.3 Association Class Course Of Action Rule

A rule to initiate a process as a course of action triggered by a situation.

A course of action rule is an action that initiates a process to be performed by some actor or actors.

### 8.21.31 Direct Supertypes

[Causality Rule](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Courses of action

### 8.21.31 Association Ends

 trigger : [Situation](#) [\*] Subsets: conditionally caused by:[Situation](#)

The situation(s) initiating a course of action.

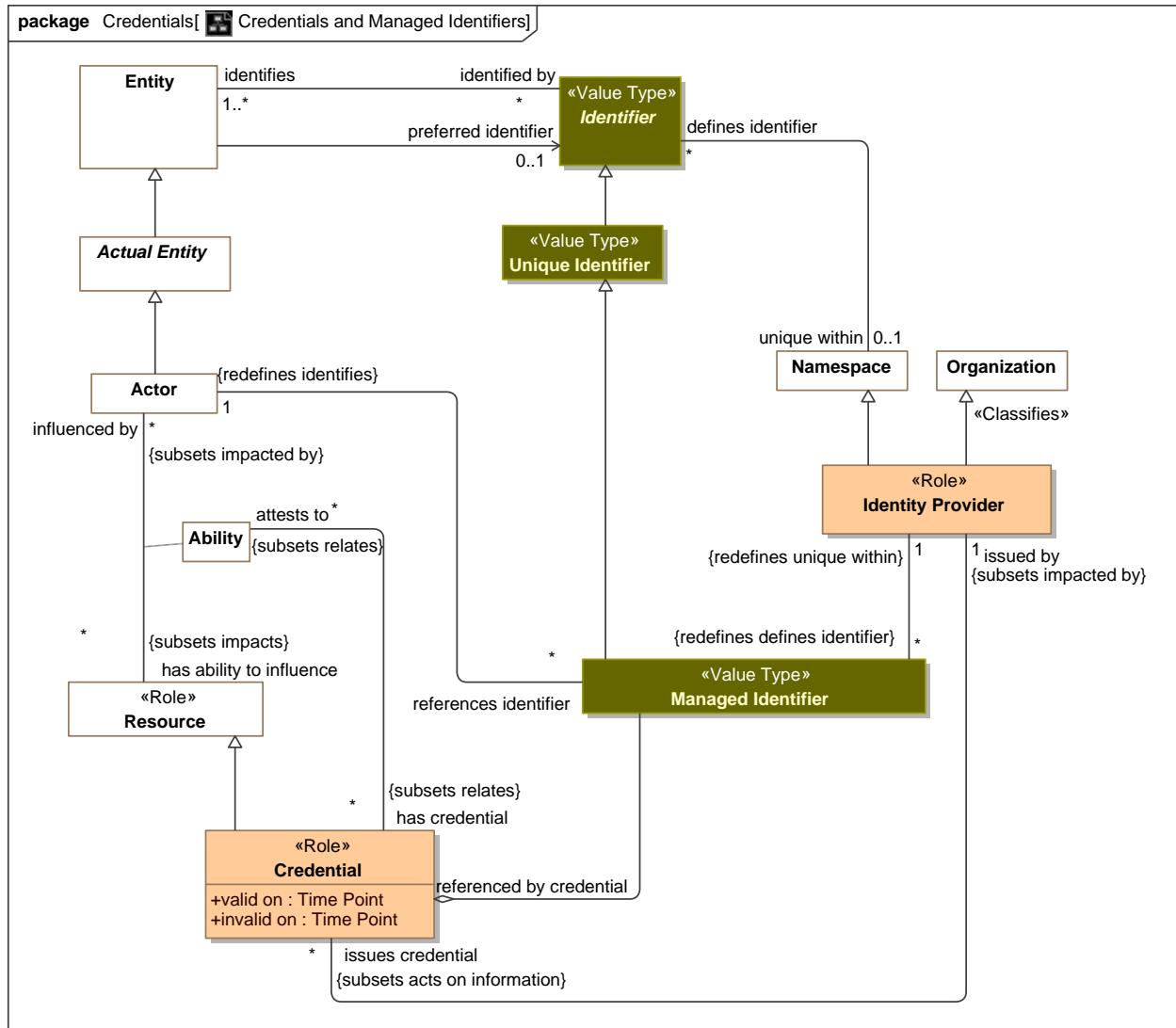
 initiates : [Course of Action](#) [\*] Subsets: conditionally caused by:[Situation](#)

The situation that triggers a course of action.

## 8.22 Threat-risk-conceptual-model::Generic Concepts::Credentials

## Concepts relating to identity management.

### **8.22.1 Diagram: Credentials and Managed Identifiers**



**Figure 29. Credentials and Managed Identifiers**

## **8.22.2 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.[Wikipedia] Credentials can be physical (a house key), documents (a certificate) or virtual (a PKI key) and may be valid for a specific timeframe and in specific context.

### **8.22.21 Direct Supertypes**

[Resource](#)

**package Threat-risk-conceptual-model::Generic Concepts::Credentials**

### **8.22.22 Attributes**

 valid on : [Time Point](#)

Time the credential becomes valid.

 invalid on : [Time Point](#)

Time the credential is no longer valid.

### **8.22.23 Associations**

 attests to : [Ability](#) [\*] Subsets: relates:[Anything](#)

Credentialed capability.

 references identifier : [Managed Identifier](#)

Identifiers used by a credential.

 issued by : [Identity Provider](#) [1] Subsets: impacted by:[Entity](#)

Issuer of a credential.

## **8.22.3 Class Identity Provider**

An organization that validates identity and issues curated identifiers and credentials.

### **8.22.31 Direct Supertypes**

[Namespace](#), [Organization](#)

**package Threat-risk-conceptual-model::Generic Concepts::Credentials**

### **8.22.32 Associations**

 : [Managed Identifier](#) [\*] Redefines: defines identifier:[Identifier](#)

 issues credential : [Credential](#) [\*] Subsets: acts on information:[Information Object](#)

Credential issued by an identity provider.

## **8.22.4 Class Managed Identifier**

An identifier managed by an identity provider. This includes technical/cyber identities as well as traditional identifiers such as passport numbers and corporate IDs.

#### 8.22.41 Direct Supertypes

Unique Identifier

**package** Threat-risk-conceptual-model::Generic Concepts::Credentials

#### 8.22.42 Associations

- ✓ : [Identity Provider](#) [1] *Redefines:* unique within:[Namespace](#)
- ✓ : [Actor](#) [1] *Redefines:* identifies:[Entity](#)
- ✗ referenced by credential : [Credential](#)

Credentials which use an identifier.

## 8.23 Threat-risk-conceptual-model::Generic Concepts::Cyber

The Cyber package defines instances and subtypes of generic threat and risk concepts specific to Cyber threats and risks.

### 8.23.1 Diagram: Cyber

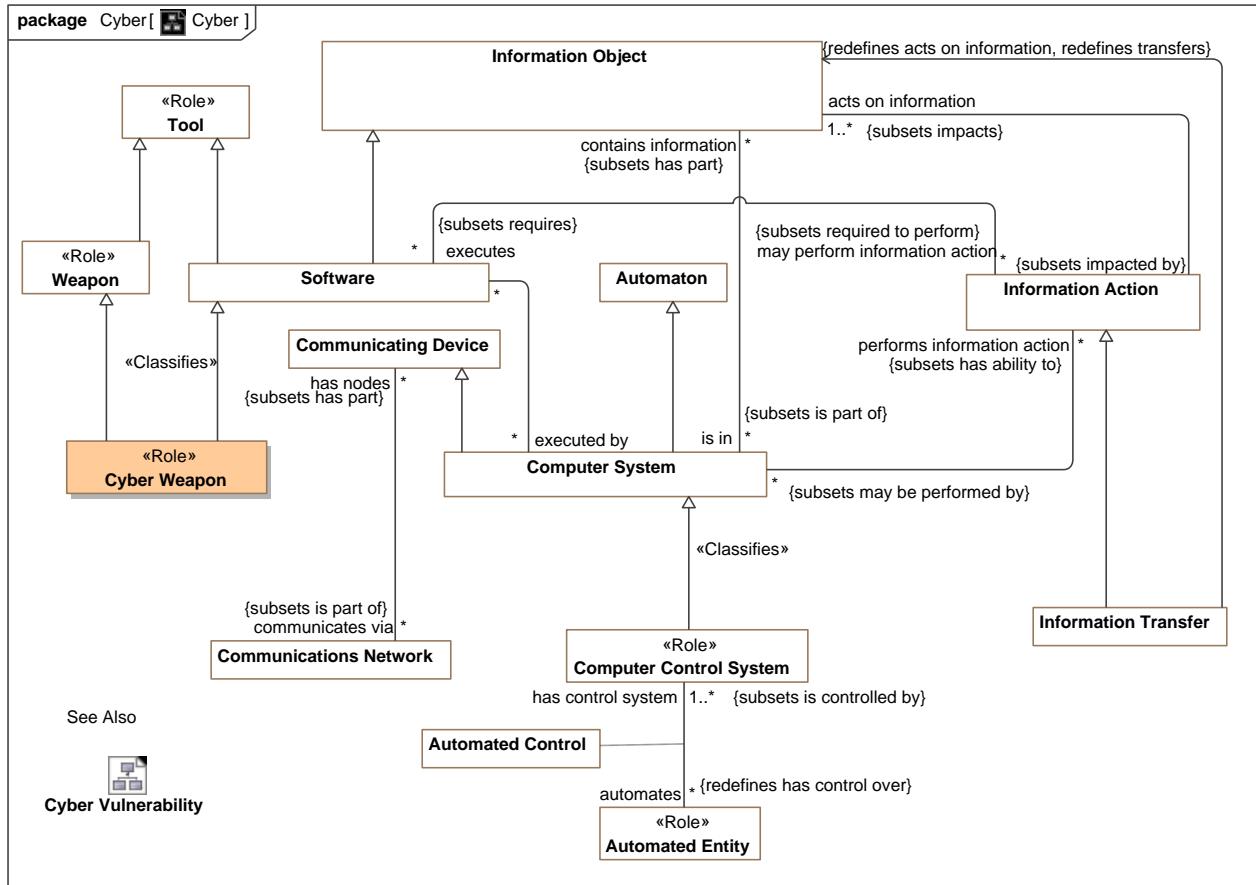


Figure 30. Cyber

### 8.23.2 Class Cyber Weapon

A software weapon.

#### 8.23.21 Direct Supertypes

[Software](#), [Weapon](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Cyber

## 8.24 Threat-risk-conceptual-model::Generic Concepts::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.

### 8.24.1 Diagram: Enterprise

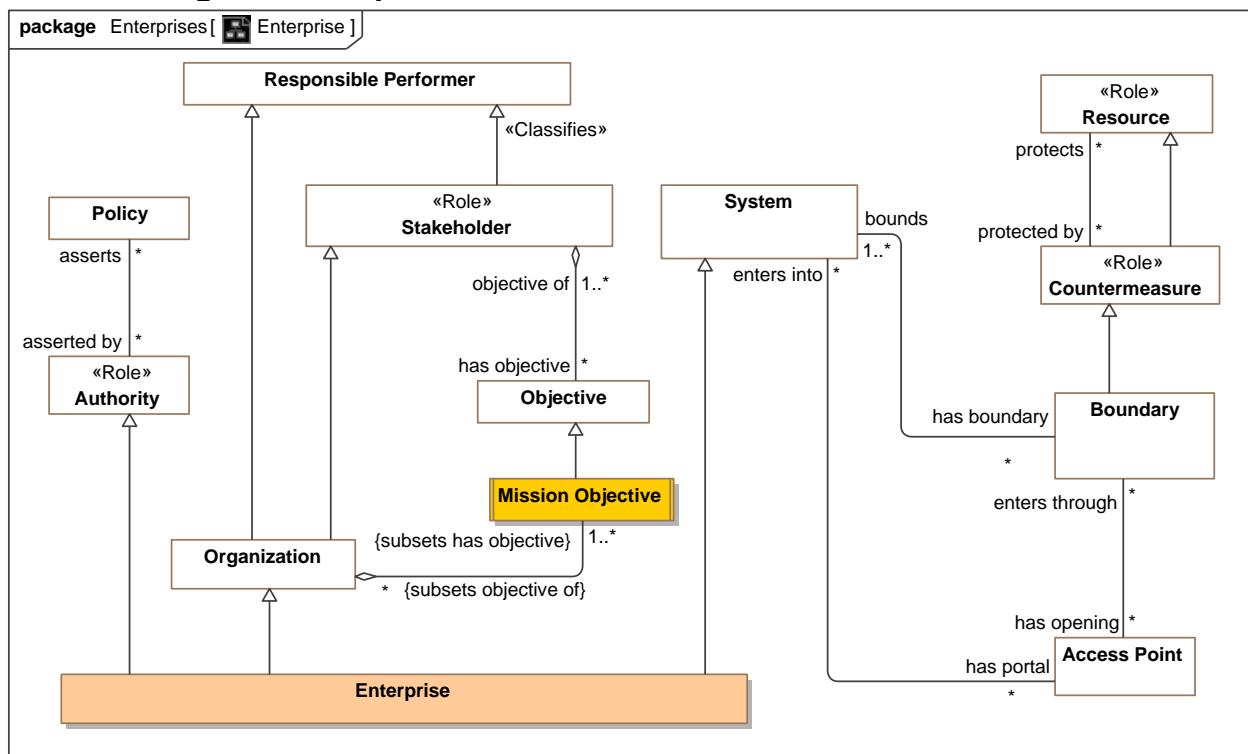


Figure 31. Enterprise

### 8.24.2 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.

#### 8.24.21 Direct Supertypes

[Authority](#), [Organization](#), [Risk Owner](#), [System](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Enterprises

## 8.25 Threat-risk-conceptual-model::Generic Concepts::Entity Kinds

Kinds of entities form a hierarchy, the upper portions of which are represented in this package.

### 8.25.1 Diagram: Entity Kinds

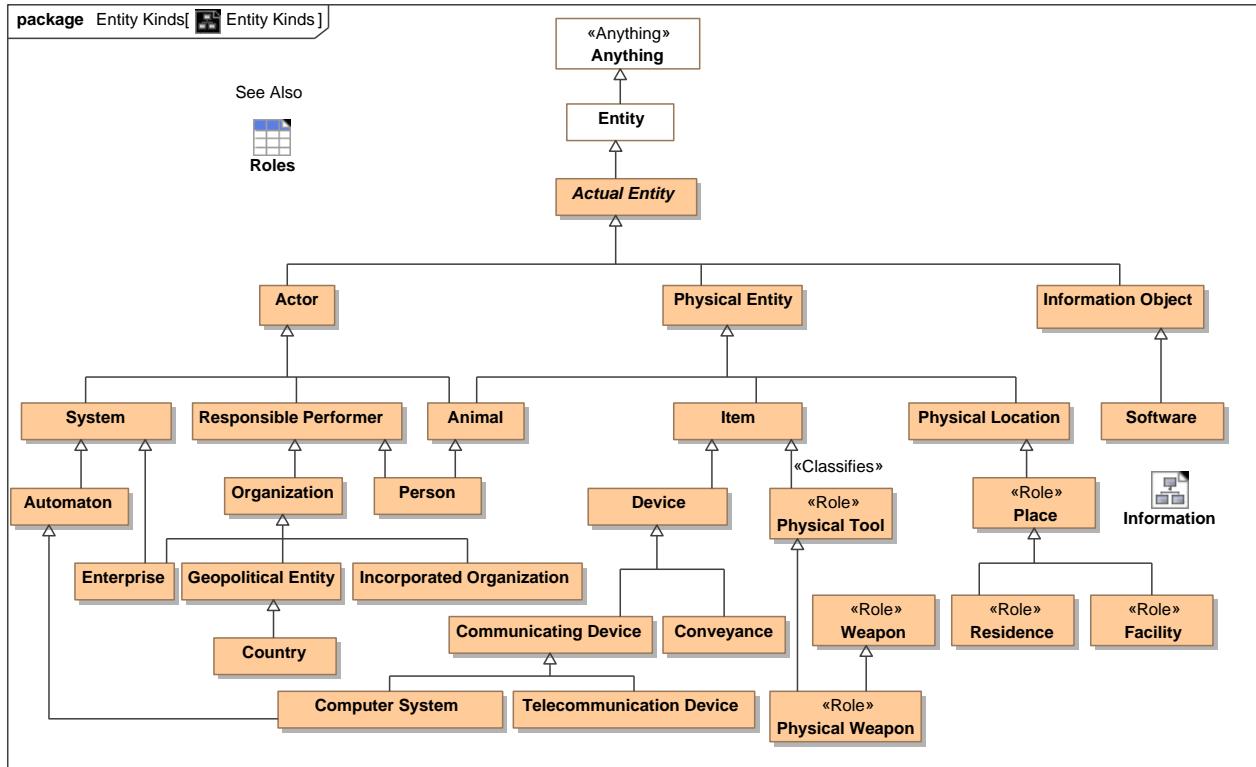
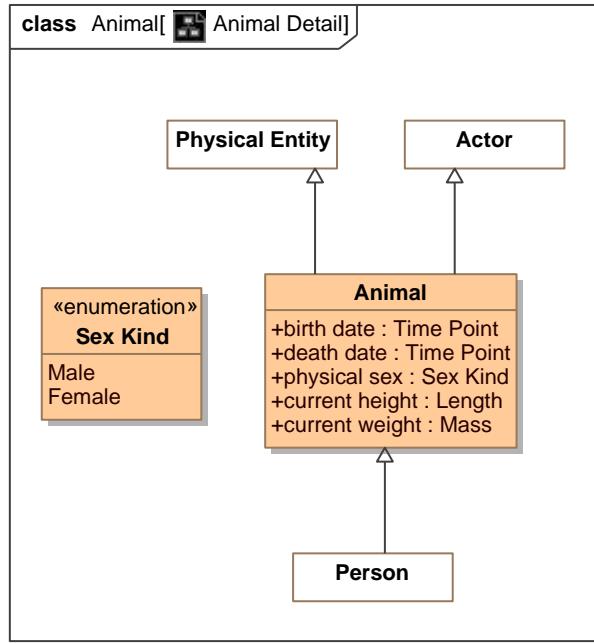


Figure 32. Entity Kinds

### 8.25.2 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 33. Animal Detail**

#### 8.25.21 Direct Supertypes

[Actor](#), [Physical Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Entity Kinds

#### 8.25.22 Attributes

birth date : [Time Point](#)

The date an animal (including a person) was born, became an independent entity.

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 in the current time frame as indicated by essential physical characteristics, primarily genitalia.

current height : [Length](#)

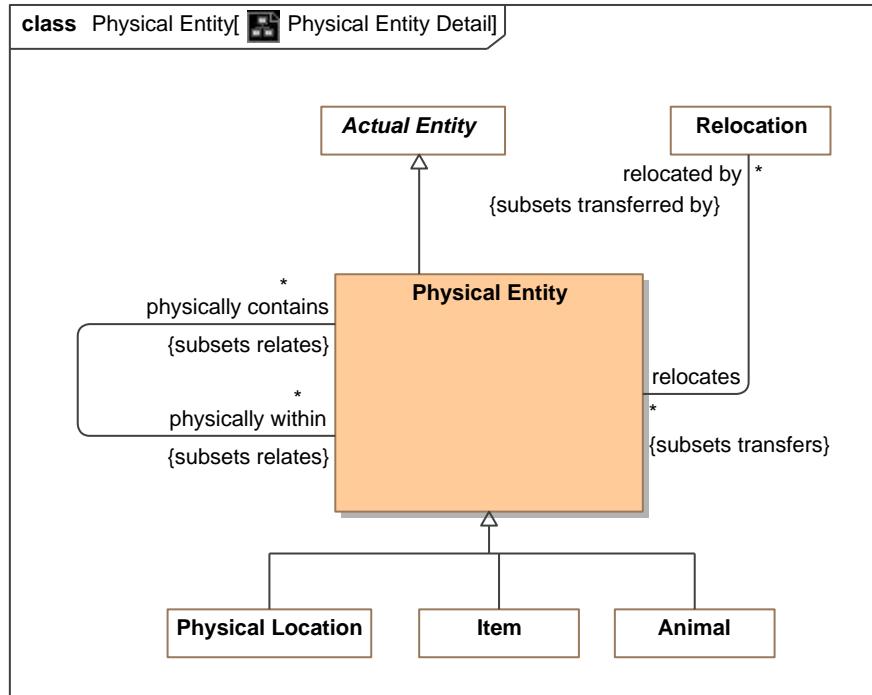
The measurement from base to top or (of a standing person) from head to foot.

current weight : [Mass](#)

Mass/weight of animal, including a person.

#### 8.25.3 Class Physical Entity

A thing that has mass and takes up space including people, places, and things.



**Figure 34. Physical Entity Detail**

### 8.25.31 Direct Supertypes

## Actual Entity

## **package** Threat-risk-conceptual-model::Generic Concepts::Entity Kinds

### 8.25.32 Associations

relocated by : [Relocation](#) [\*] Subsets: transferred by:[Transfer](#)

Entity performing the relocation of something else.

/ physically contains : Relocation [\*] Subsets: transferred by: Transfer

Physical things contained by some physical thing.{Transitive}

/ physically within : Relocation [\*] Subsets: transferred by: Transfer

An entity's physical container.{transitive}

/ : Physical Vulnerability Subsets: has vulnerability:Vulnerability

### 8.25.33 Enumeration Sex Kind

Kinds of sex. Eg. male/female.

package Threat-risk-conceptual-model::Generic Concepts::Entity Kinds

```
public enum Sex Kind
```

{Male, Female}

### **8.25.33Literals**



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:

## 8.26 Threat-risk-conceptual-model::Generic Concepts::Items

Items are inanimate material object as distinct from a living sentient being.

### 8.26.1 Diagram: Items

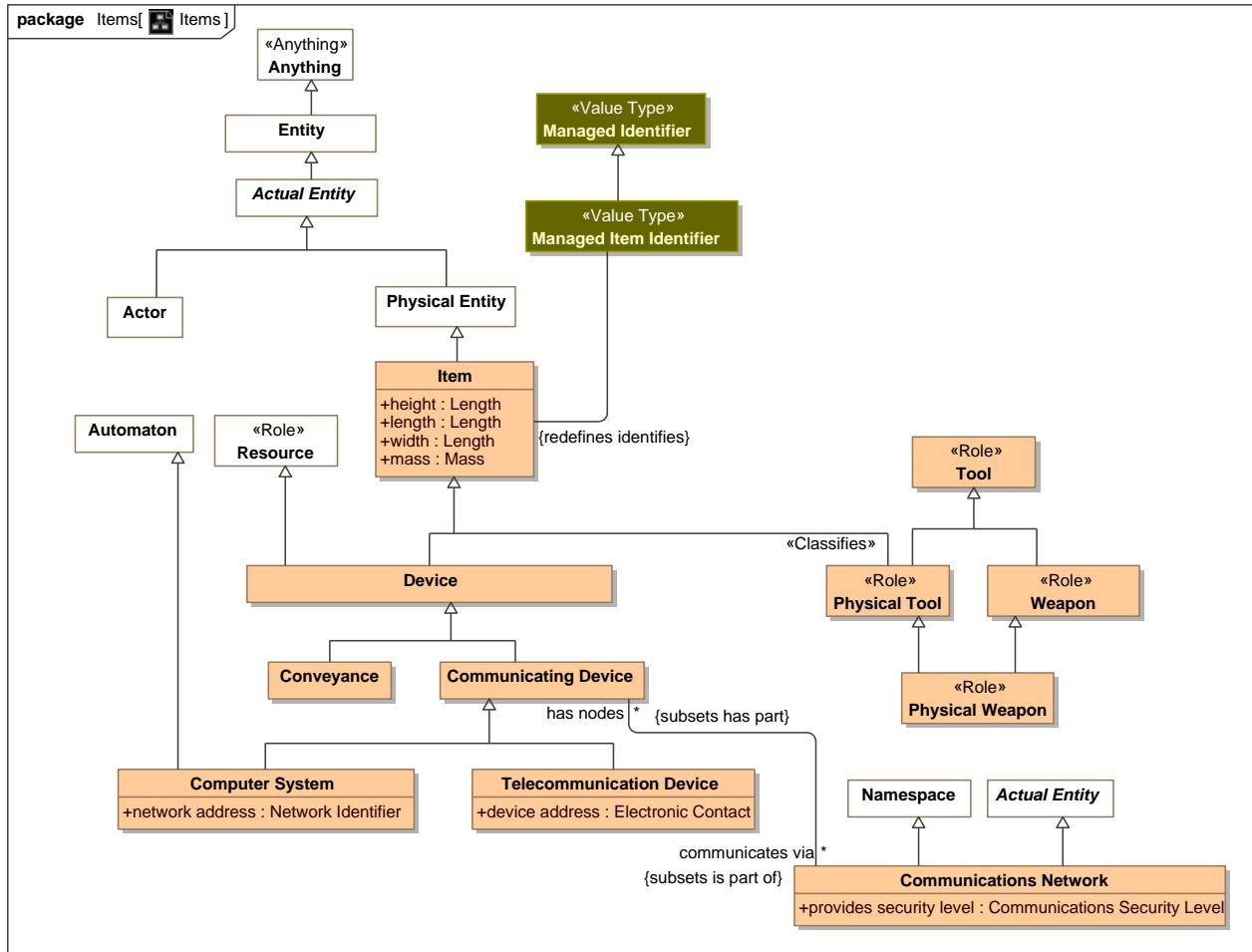


Figure 35. Items

### 8.26.2 Class Automaton

A machine or group of machines (most often a computer system, robot, or computerized swarm combined with 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).

### 8.26.21 Direct Supertypes

[System](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

### 8.26.3 Class Communicating Device

A device able to communicate or facilitate communications across a network.

#### 8.26.31 Direct Supertypes

[Contactable](#), [Device](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

#### 8.26.32 Associations

/ communicates via : [Communications Network](#) [\*] Subsets: is part of:[Entity](#)

### 8.26.4 Class Communications Network

A physical or electronic system intended to facilitate communications between entities. Includes communications channels.

#### 8.26.41 Direct Supertypes

[Actual Entity](#), [Namespace](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

#### 8.26.42 Attributes

◆ provides security level : [Communications Security Level](#)

The level of security asserted for this communications network.

#### 8.26.43 Associations

/ has communications address : [Contact Means](#) [\*] Redefines: defines identifier:[Identifier](#)

Address within a communications network.

/ has nodes : [Communicating Device](#) [\*] Subsets: has part:[Entity](#)

The communicating nodes of a communications network.

/ : [Communications Vulnerability](#) Subsets: has vulnerability:[Vulnerability](#)

## **8.26.5 Class Computer System**

An identifiable and physical computer system that acts as an automaton agent performing processes.

A programmable electronic device designed to accept data, perform prescribed mathematical and logical operations at high speed, and display the results of these operations. Mainframes, desktop and laptop computers, tablets, and smart phones are some of the different types of computers. [dictionary.com]

### **8.26.51 Direct Supertypes**

[Automaton](#), [Communicating Device](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

### **8.26.52 Attributes**

network address : [Network Identifier](#)

Electronic address which allows communication with a computer system.

### **8.26.53 Associations**

/ executes : [Software](#) [\*]

Software a computer system is able to execute.

/ performs information action : [Information Action](#) [\*] Subsets: has ability to:[Process](#)

Information actions a computer may perform.

/ contains information : [Information Object](#) [\*] Subsets: has part:[Entity](#)

Information stored in a computer.

/ : [Information System Vulnerability](#) Subsets: has vulnerability:[Vulnerability](#)

## **8.26.6 Class Conveyance**

A means of physical transport from place to place.

### **8.26.61 Direct Supertypes**

[Device](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

## **8.26.7 Class Device**

A thing made for a particular purpose; an invention or contrivance, especially a mechanical or electrical one.

### **8.26.71 Direct Supertypes**

[Item](#), [Resource](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

## **8.26.8 Class Item**

An inanimate material object as distinct from a living sentient being.

### **8.26.81 Direct Supertypes**

[Physical Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

### **8.26.82 Attributes**

◆ height : [Length](#)

A measurement of the height of an item.[NIEM]

A measurement in the vertical plane. For a person, from head to toe.

◆ length : [Length](#)

A measurement of the length of an item.[NIEM]

A longitudinal measurement - from end to end. Usually greater than width.

◆ width : [Length](#)

A measurement of the width of an item.[NIEM]

A horizontal measurement - from side to side.

◆ mass : [Mass](#)

A measurement of the mass of an item.

Note: "Weight" is often confused with mass. Mass is independent of gravitational force and is a property of an item - weight is dependent on location and gravity and is thus not a property of the item alone. U.S. & U.K. pounds may be used to represent weight or mass. In this model the mass interpretation is used.

### **8.26.83 Associations**

 : [Managed Item Identifier](#)

## **8.26.9 Class Managed Item Identifier**

An identification inscribed on or attached to a part, collection of parts, or complete unit by the manufacturer. Syn. ItemSerialIdentification[NIEM]

### **8.26.91 Direct Supertypes**

[Managed Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

### **8.26.92 Associations**

 : [Item](#) Redefines: identifies:[Entity](#)

### **8.26.10 Class Physical Tool**

An item intended to be used to perform some function.

#### 8.26.101 Direct Supertypes

[Item](#), [Tool](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

### **8.26.11 Class Physical Weapon**

A physical item intended to exploit a vulnerability.

#### 8.26.111 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Generic Concepts::Items

### **8.26.12 Class Telecommunication Device**

A device for communication over a distance by cable, telegraph, telephone, computer networks, or broadcasting.

#### 8.26.121 Direct Supertypes

[Communicating Device](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Items

#### 8.26.122 Attributes

 device address : [Electronic Contact](#)

Address to communicate via a telecommunications device.

## 8.27 Threat-risk-conceptual-model::Generic Concepts::Locations

Concepts about locations and places.

### 8.27.1 Diagram: Location

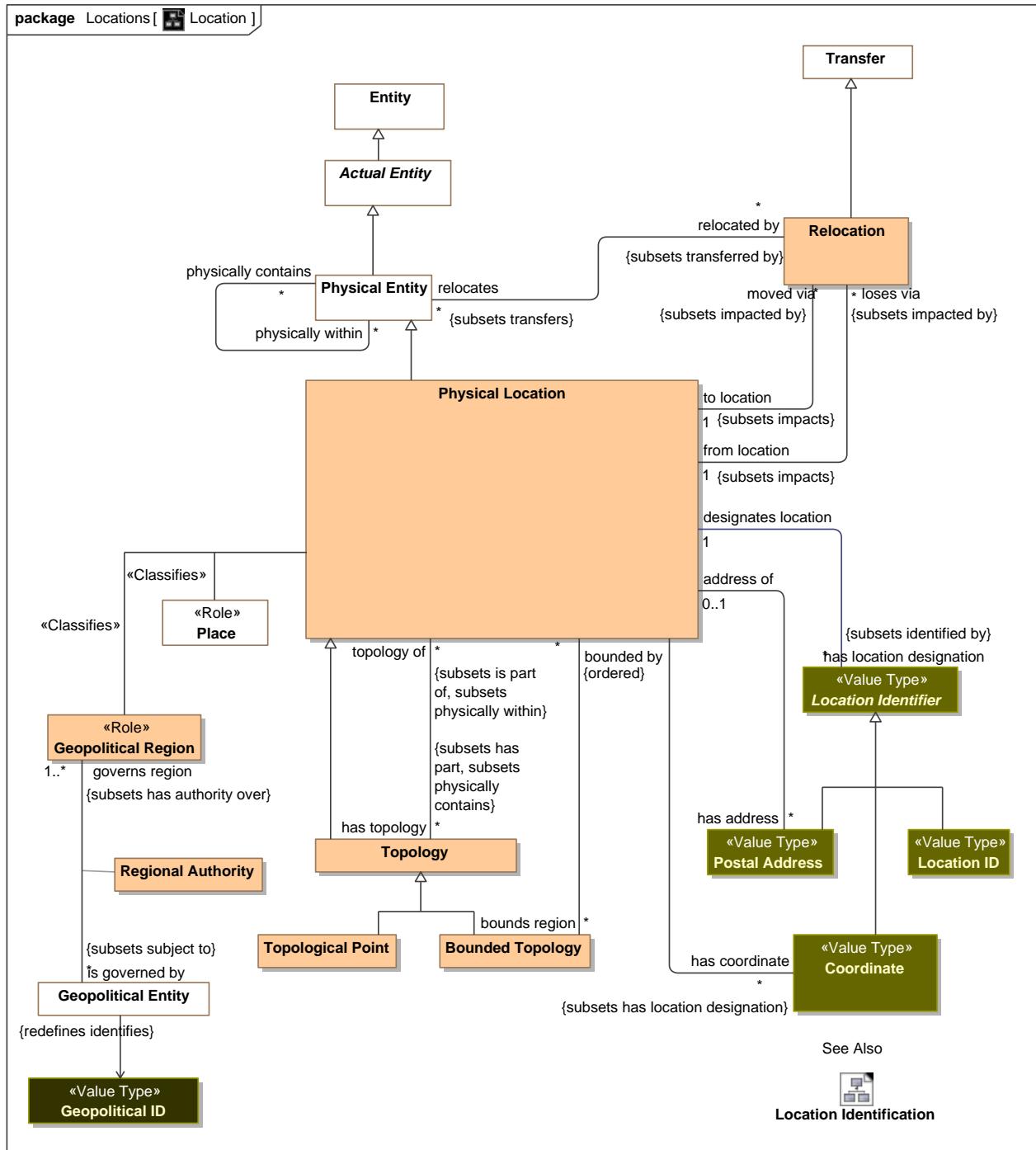


Figure 36. Location

## 8.27.2 Diagram: Location Identification

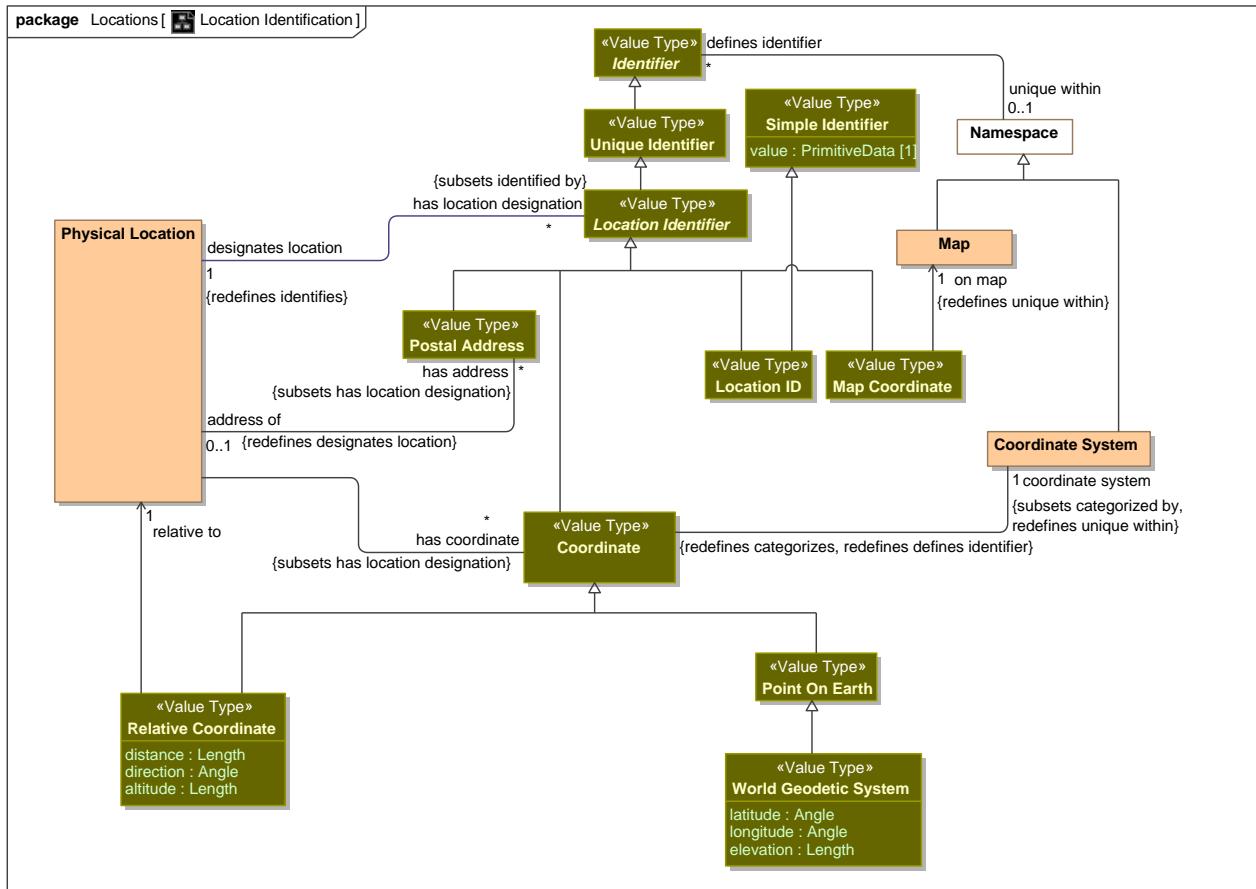


Figure 37. Location Identification

## 8.27.3 Class Bounded Topology

A contiguous location identified by geographic boundaries.

### 8.27.31 Direct Supertypes

#### Topology

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### 8.27.32 Associations

/ bounded by : [Physical Location](#) [\*]

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.

## **8.27.4 Class Coordinate**

Any coordinate point that uniquely identifies a point location relative to some coordinate system.

One of a sequence of n numbers designating the position of a point in n-dimensional space [OGC]

### **8.27.41 Direct Supertypes**

[Location Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### **8.27.42 Associations**

 : [Physical Location](#)

 coordinate system : [Coordinate System](#) [1] Subsets: categorized by:[Category](#) Redefines: unique within:[Namespace](#)

The coordinate system used for a coordinate.

## **8.27.5 Class Coordinate System**

A reference system for a coordinate. e.g., WGS-84.

Set of mathematical rules for specifying how coordinates are to be assigned to points. [OGC]

### **8.27.51 Direct Supertypes**

[Namespace](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### **8.27.52 Associations**

 : [Coordinate](#) Redefines: categorizes:[Anything](#) defines identifier:[Identifier](#)

## **8.27.6 Class Geopolitical Region**

A physical location governed by a geopolitical entity.

### **8.27.61 Direct Supertypes**

[Physical Location](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### **8.27.62 Associations**

 is governed by : [Geopolitical Entity](#) [\*] Subsets: subject to:[Authority](#)

A governing authority for a region.

## **8.27.7 Class Location ID**

A code, ID or name for a physical location.

### 8.27.7.1 Direct Supertypes

[Location Identifier](#), [Simple Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

## **8.27.8 Class Location Identifier**

Any identifier able to uniquely identify a physical location Syn. spatial reference - description of position in the real world [OGC]

### 8.27.8.1 Direct Supertypes

[Unique Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### 8.27.8.2 Associations

 designates location : [Physical Location](#) [1] *Redefines:* identifies:[Entity](#)

The location identified.

## **8.27.9 Class Map**

A representation of the features of an area of the earth or a portion of the heavens, showing them in their respective forms, sizes, and relationships according to some convention of representation: e.g., a map of Canada.

### 8.27.9.1 Direct Supertypes

[Namespace](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

## **8.27.10 Class Map Coordinate**

A data type for a location identified by map or grid coordinates.[NIEM]

### 8.27.10.1 Direct Supertypes

[Location Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### 8.27.10.2 Associations

 on map : [Map](#) [1] *Redefines:* unique within:[Namespace](#)

Map on which a coordinate is defines.

## **8.27.11 Class Physical Location**

A point or extent in physical space.

[NIEM] A geospatial location.

### **8.27.111 Direct Supertypes**

[Physical Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### **8.27.112 Associations**

/ has location designation : [Location Identifier](#) [\*] Subsets: identified by:[Identifier](#)

A way to identify a physical location.

/ has address : [Postal Address](#) [\*] Subsets: has location designation:[Location Identifier](#)

A postal address of a physical location.

/ has coordinate : [Coordinate](#) [\*] Subsets: has location designation:[Location Identifier](#)

A coordinate that identifies a location.

 located person : [Person](#) [\*] Subsets: physically contains:[Physical Entity](#)

Person who is at a location.

/ loses via : [Relocation](#) [\*] Subsets: impacted by:[Entity](#)

Relocation occurrence that causes the location to no longer contain an entity.

/ moved via : [Relocation](#) [\*] Subsets: impacted by:[Entity](#)

Relocation occurrence that causes the location to contain an entity.

/ has topology : [Topology](#) [\*] Subsets: has part:[Entity](#) physically contains:[Physical Entity](#)

Physical topology of a location.

/ bounds region : [Bounded Topology](#) [\*]

A location identified by geographic boundaries.

## **8.27.12 Class Point On Earth**

A point that defines a location on earth where the point is within the bounds of <designates location>.

### **8.27.121 Direct Supertypes**

[Coordinate](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### **8.27.13 Class Relative Coordinate**

A coordinate described relative to another. e.g., 5 miles west of the empire state building.

#### **8.27.131 Direct Supertypes**

[Coordinate](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

#### **8.27.132 Attributes**

 distance : [Length](#)

Distance from <relative to>.

 direction : [Angle](#)

A angle to <relative to>..

 altitude : [Length](#)

Measure of how much something is above <relative to>, usually the earth.

#### **8.27.133 Associations**

 relative to : [Physical Location](#) [1]

Where the position of something is relative to another, the reference element.

### **8.27.14 Class Relocation**

The act of moving something from one location to another.

#### **8.27.141 Direct Supertypes**

[Transfer](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

#### **8.27.142 Associations**

 relocates : [Physical Entity](#) [\*] Subsets: transfers:[Entity](#)

Entity that is relocated.

 from location : [Physical Location](#) [1] Subsets: impacts:[Entity](#)

Location a physical entity is moved from.

 to location : [Physical Location](#) [1] Subsets: impacts:[Entity](#)

Location a physical entity is moved to.

### **8.27.15 Class Topological Point**

A dimensionless physical point in space or on the surface of the earth such as a corner or center point.

### 8.27.151 Direct Supertypes

[Topology](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### 8.27.16 Class Topology

A contiguous 1, 2 or 3 dimensioned area defined by geographic features. Subtypes of topology may define specific ways of describing such an area.

### 8.27.161 Direct Supertypes

[Physical Location](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### 8.27.162 Associations

 topology of : [Physical Location](#) [\*] *Subsets:* is part of:[Entity](#) physically within:[Physical Entity](#)

Physical location which a topology represents all or part of.

### 8.27.17 Class World Geodetic System

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]

### 8.27.171 Direct Supertypes

[Point On Earth](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Locations

### 8.27.172 Attributes

 latitude : [Angle](#)

Latitude based on the prime meridian.

 longitude : [Angle](#)

Longitude based on the prime meridian.

 elevation : [Length](#)

Height above nominal sea level.

## 8.28 Threat-risk-conceptual-model::Generic Concepts::Manufacturers

Concepts relating to manufacturers and manufactured things.

### 8.28.1 Diagram: Manufacturer

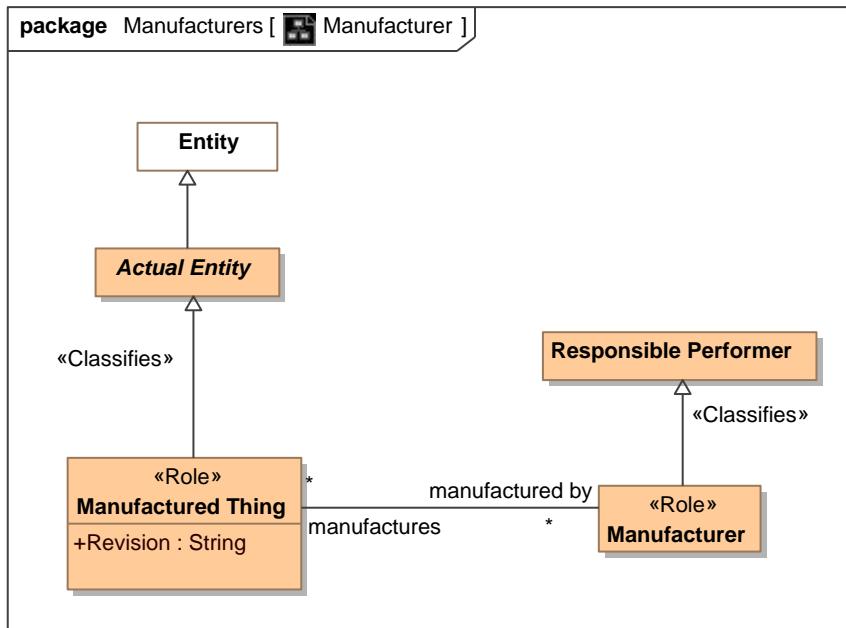


Figure 38. Manufacturer

### 8.28.2 Class Manufactured Thing

Role of a thing as being made or manufactured.

#### 8.28.21 Direct Supertypes

[Actual Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Manufacturers

#### 8.28.22 Attributes

Revision : [String](#)

The revision of a product or good.

#### 8.28.23 Associations

/ manufactured by : [Manufacturer](#) [\*]

Entity which manufactured a thing.

### **8.28.3 Class Manufacturer**

Maker of goods or products, usually for sale.

#### 8.28.31 Direct Supertypes

[Responsible Performer](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Manufacturers

#### 8.28.32 Associations

 manufactures : [Manufactured Thing](#) [\*]

Products or goods made by a manufacturer.

## 8.29 Threat-risk-conceptual-model::Generic Concepts::Objectives

*Intent* captures how the *objectives* 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.

### 8.29.1 Diagram: Impact

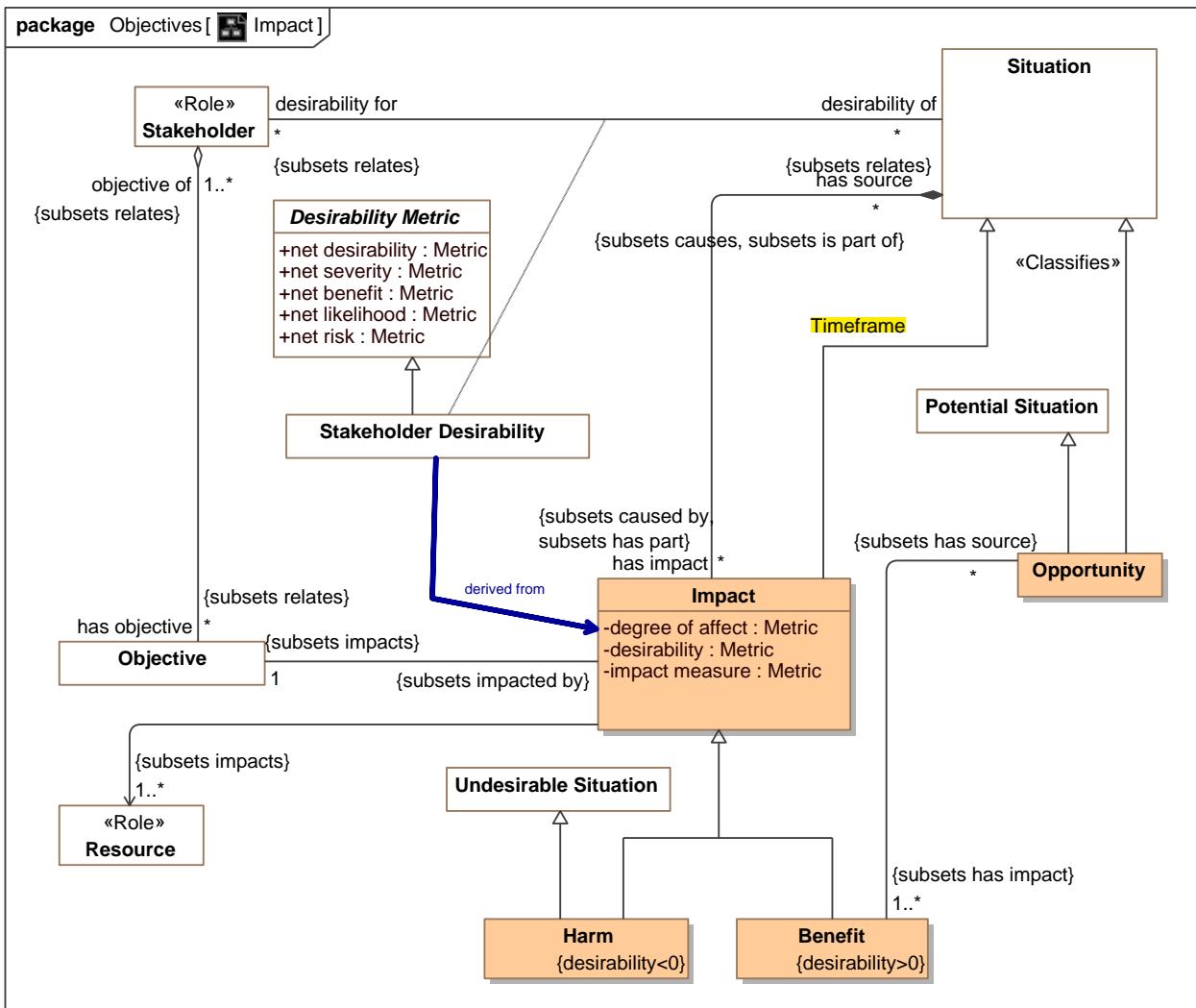


Figure 39. Impact

## 8.29.2 Diagram: Objectives

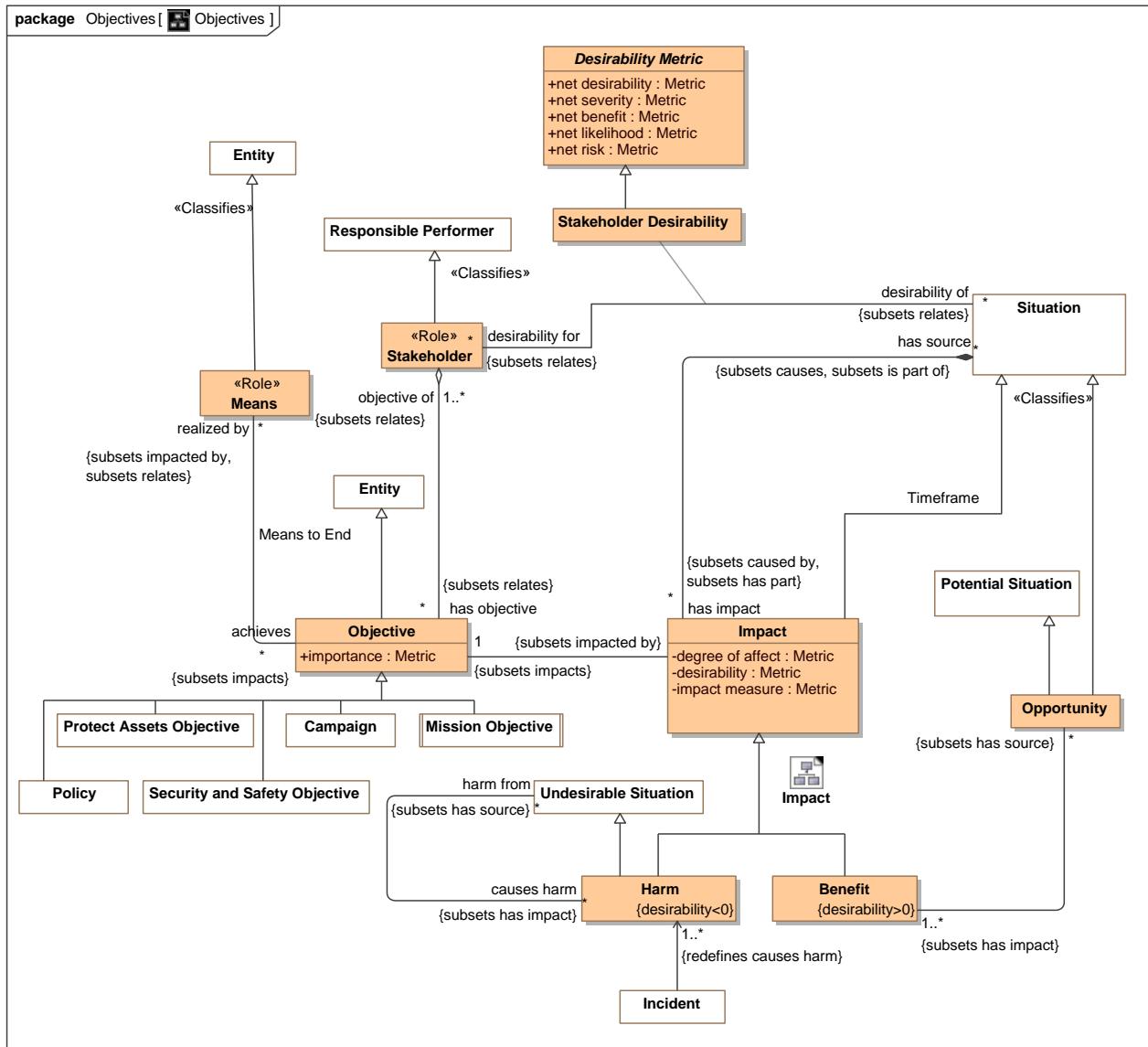


Figure 40. Objectives

## 8.29.3 Class Benefit

A benefit is a consequence of a situation having positive desirability.

### 8.29.31 Direct Supertypes

[Impact](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

### 8.29.32 Associations

: [Opportunity](#) [\*] Subsets: has source:[Situation](#)

A situation that may result in an opportunity.

### 8.29.4 Class Desirability Metric

Desirability characteristics of any 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. Such a risk may be subject to risk requirements and may contribute to incidents (realized risks).

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

### 8.29.41 Attributes

net desirability : [Metric](#)

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](#)

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](#)

Computed as likelihood\*impact.

### 8.29.5 Class Harm

Harm is a consequence of a situation having negative desirability.

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. [Firesmith 2003]

### 8.29.51 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

## 8.29.52 Associations

 harm from : [Undesirable Situation](#) [\*] Subsets: has source:[Situation](#)

Danger which is the source of harm.

## 8.29.6 Class Impact

A consequence or impact of the outcome of a situation affecting objectives of a stakeholder.

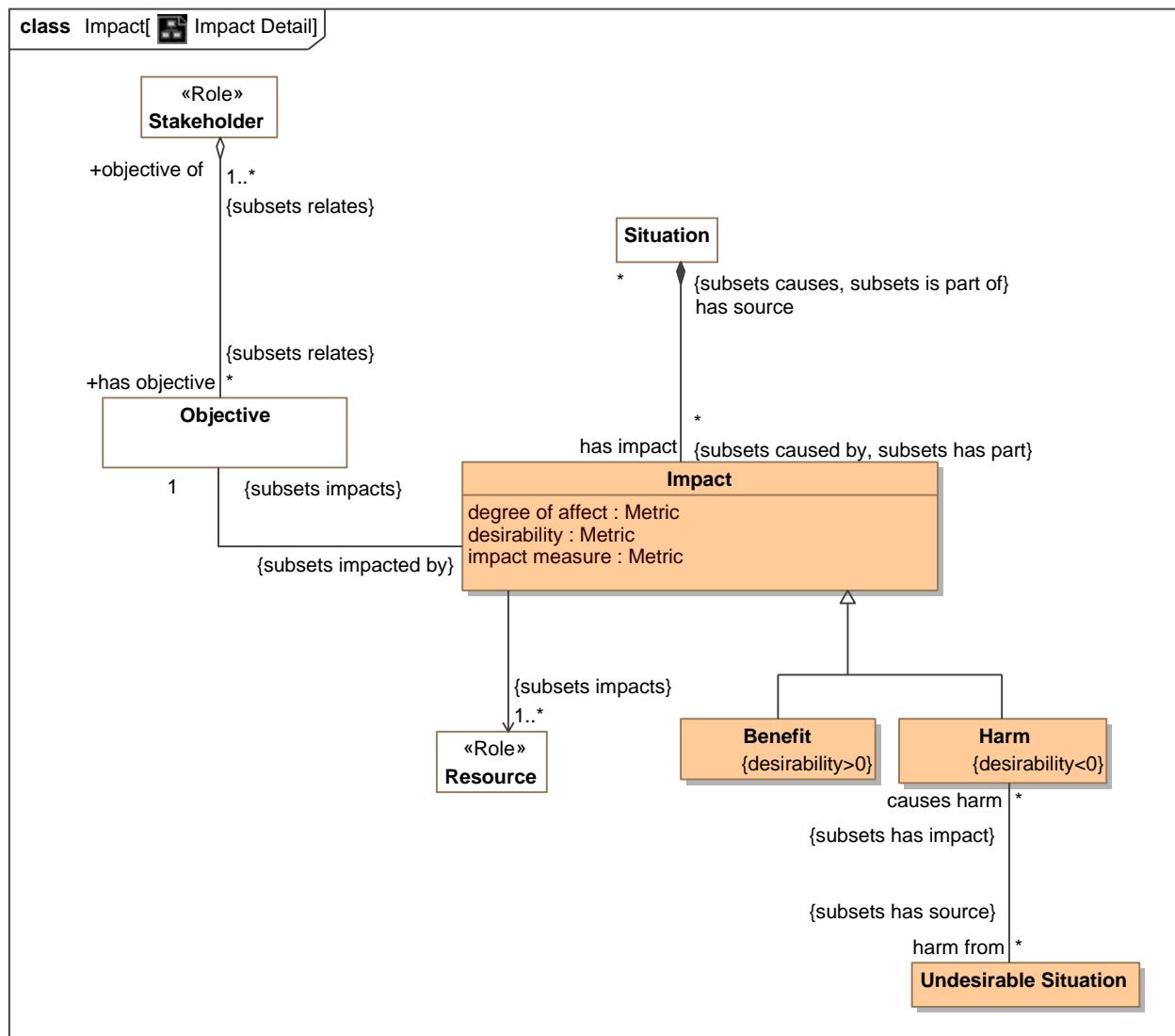
NOTE 1 An event can lead to a range of consequences.

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 41. Impact Detail**

### 8.29.61 Direct Supertypes

Situation

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

### 8.29.62 Attributes

◦ degree of affect : [Metric](#)

A metric for how much the consequence affects the objective - how much harm or benefit.

◦ desirability : [Metric](#)

The desirability of the consequence as importance times degree of affect. May be positive or negative.

◦ impact measure : [Metric](#)

Impact = desirability \* likelihood

### 8.29.63 Associations

↙ : [Objective](#) [1] Subsets: impacts:[Entity](#)

↙ has source : [Situation](#) [\*] Subsets: is part of:[Entity](#) causes:[Situation](#)

Cause of a consequence.

↗ : [Resource](#) [1..\*] Subsets: impacts:[Entity](#)

Resource a consequence may affect.

## 8.29.7 Class Means

A means represents any device, capability, regime, technique, restriction, agency, instrument, or method that may be called upon, activated, or enforced to achieve Ends. [BMM]

### 8.29.71 Direct Supertypes

Entity

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

### 8.29.72 Associations

↙ achieves : [Objective](#) [\*] Subsets: impacts:[Entity](#)

Objectives supported by a means.

## 8.29.8 Association Means to End

The relation between a means and an objective.

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

### 8.29.81 Association Ends

/ achieves : [Objective](#) [\*] Subsets: impacts:[Entity](#)

Objectives supported by a means.

/ realized by : [Means](#) [\*] Subsets: impacts:[Entity](#)

Anything that helps obtain an objective.

### 8.29.9 Class Objective

Something that means are intended to attain or accomplish; purpose; goal; target.

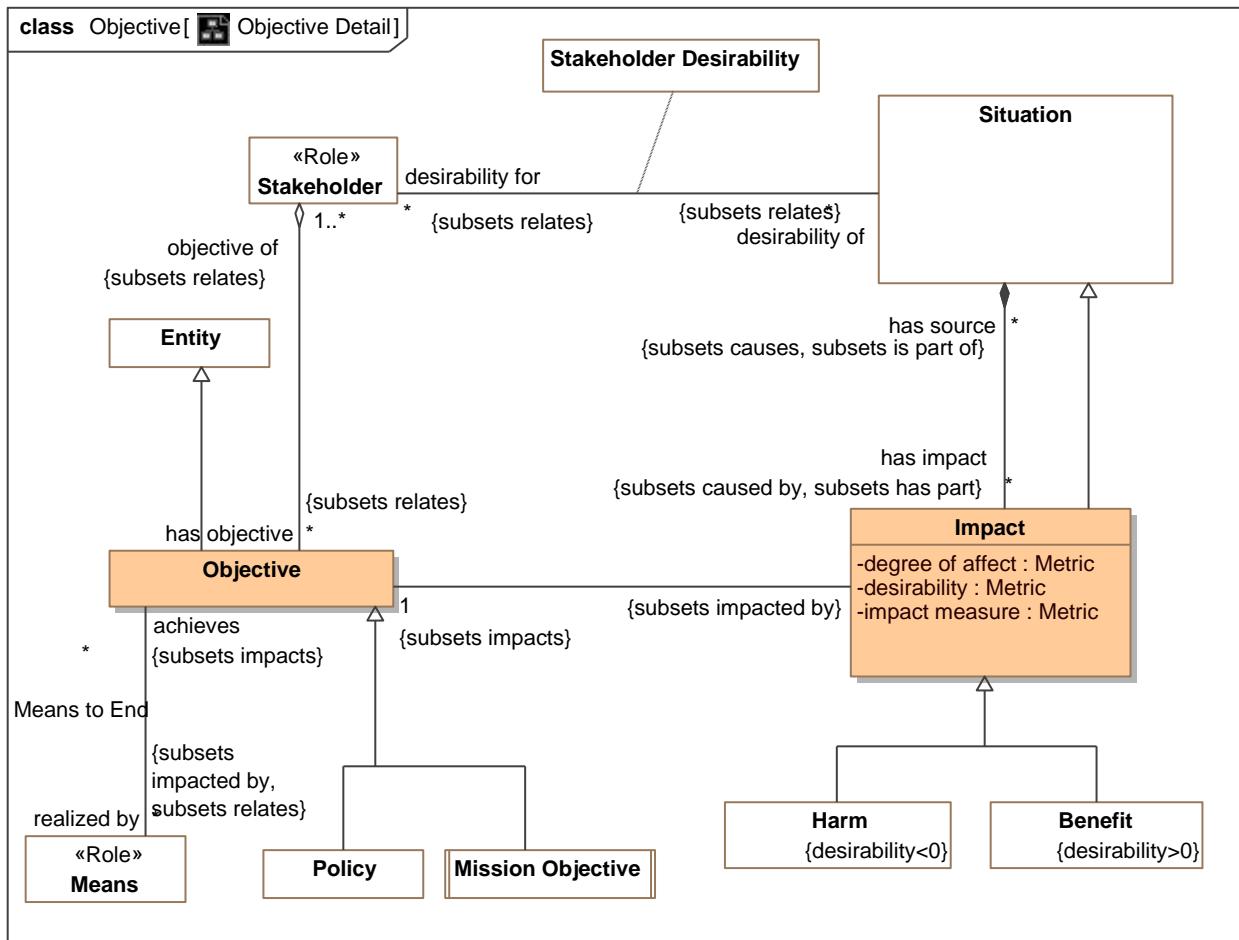


Figure 42. Objective Detail

### 8.29.91 Direct Supertypes

[Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

### 8.29.92 Attributes

importance : [Metric](#)

Importance of an intent to a stakeholder.

### 8.29.93 Associations

: [Impact](#) Subsets: impacted by: [Entity](#)

/ realized by : [Means](#) [\*] Subsets: relates: [Anything](#) impacted by: [Entity](#)

Anything that helps obtain an objective.

✓ objective of : [Stakeholder](#) [1..\*] Subsets: relates: [Anything](#)

The stakeholder having an intent.

/ : [Disrupt Objective](#) Subsets: affected by: [Action On Entity](#)

## 8.29.10 Class Opportunity

An opportunity is any potential future situation having beneficial consequences.

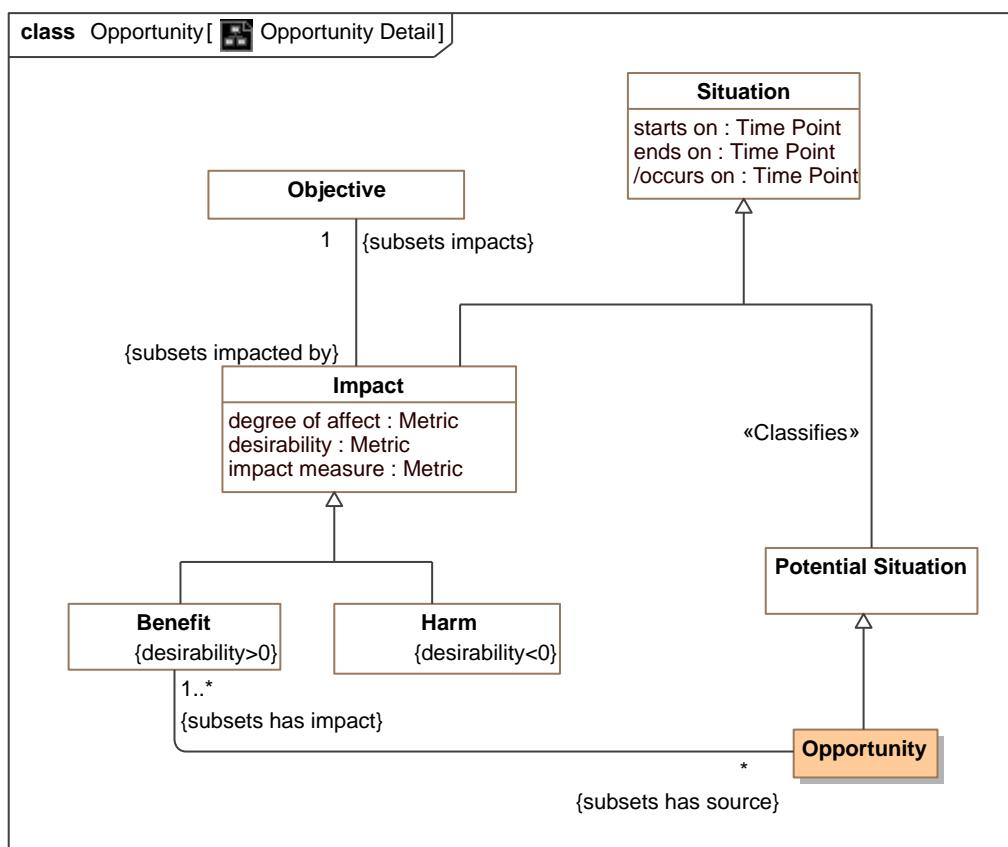


Figure 43. Opportunity Detail

## 8.29.101 Direct Supertypes

[Potential Situation](#), [Situation](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

## 8.29.102 Associations

 : [Benefit](#) [1..\*] Subsets: has impact:[Impact](#)

A consequence of a situation that impacts the objectives of a stakeholder.

## 8.29.11 Class Stakeholder

A responsible performer having objectives.

## 8.29.111 Direct Supertypes

[Responsible Performer](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

## 8.29.112 Associations

 has objective : [Objective](#) [\*] Subsets: relates:[Anything](#)

Intent of a stakeholder.

 assumes risk from : [Transfer Risk](#) Subsets: impacted by:[Entity](#)

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

## 8.29.12 Association Class Stakeholder Desirability

Net desirability of any situation for any stakeholder.

## 8.29.121 Direct Supertypes

[Desirability Metric](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Objectives

## 8.29.121 Association Ends

 desirability of : [Situation](#) [\*] Subsets: impacted by:[Entity](#)

What is desired.

 desirability for : [Stakeholder](#) [\*] Subsets: impacted by:[Entity](#)

The stakeholder with a desire.

## 8.30 Threat-risk-conceptual-model::Generic Concepts::Observations

Observations are acts where an observer notes some entity (including situations and individuals) that are observed in a situation.

### 8.30.1 Diagram: Observability

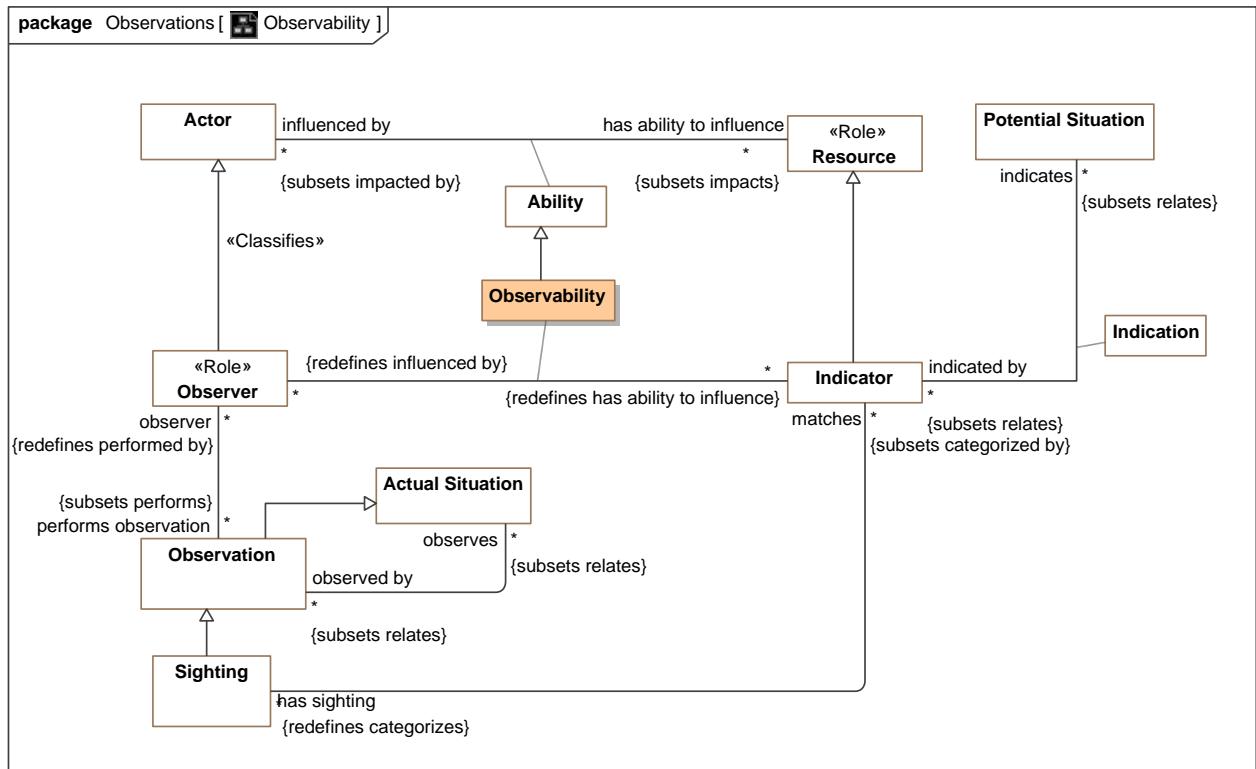
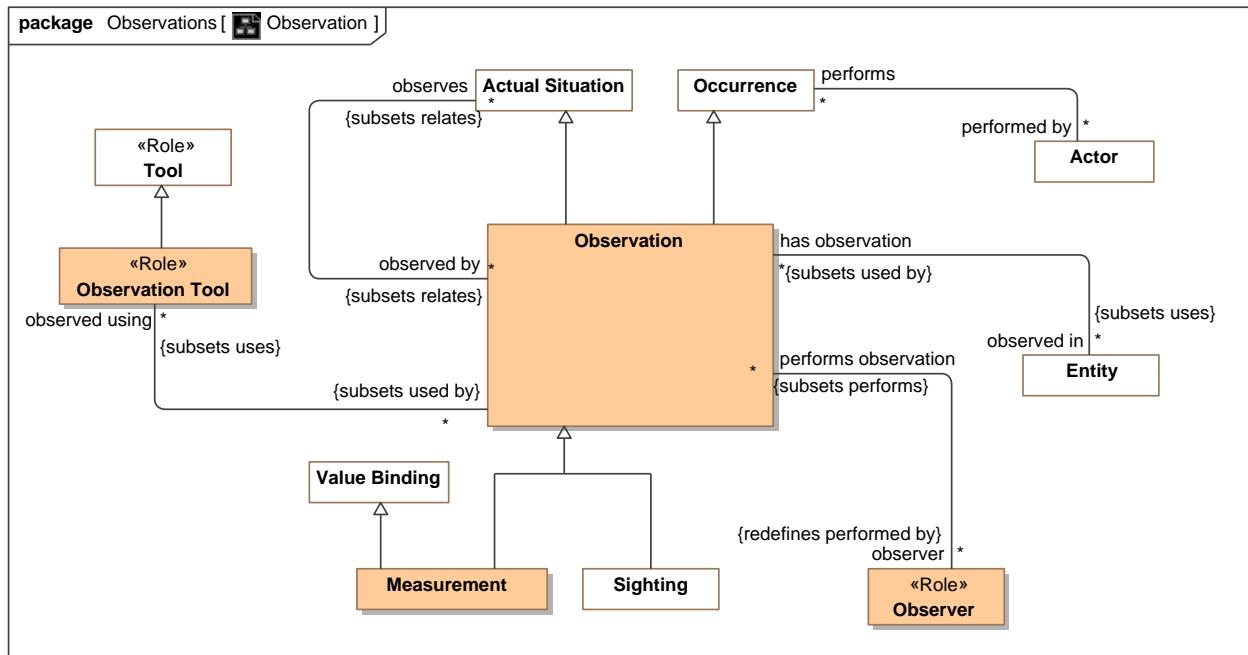


Figure 44. Observability

### **8.30.2 Diagram: Observation**



**Figure 45.** Observation

### **8.30.3 Class Measurement**

The act of determining a quantity via a repeatable and objective process.

### 8.30.31 Direct Supertypes

## Observation, Value Binding

**package** Threat-risk-conceptual-model::Generic Concepts::Observations

#### **8.30.4 Association Class Observability**

The capability to observe an indicator.

### 8.30.41 Direct Supertypes

## Ability

## **package** Threat-risk-conceptual-model::Generic Concepts::Observations

### **8.30.41 Association Ends**

 : Indicator [\*] Subsets: impacted by: Entity

: Observer [\*] Subsets: impacted by: Entity

## **8.30.5 Class Observation**

The act of observing something or someone carefully in order to gain information.

### 8.30.51 Direct Supertypes

[Actual Situation](#), [Occurrence](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Observations

### 8.30.52 Attributes

 number observed : [Numeric](#)

The number of individual observations aggregated into a single observation.

### 8.30.53 Associations

 observes : [Actual Situation](#) [\*] Subsets: relates:[Anything](#)

The observed entity (individual or situation).

 observer : [Observer](#) [\*] Redefines: performed by:[Actor](#)

The observer.

 observed using : [Observation Tool](#) [\*] Subsets: uses:[Entity](#)

Anything used to facilitate observation.

 observed in : [Entity](#) [\*] Subsets: uses:[Entity](#)

The context of an observation, what environment or system is being observed.

## **8.30.6 Class Observation Tool**

Any tools that assists in observation.

### 8.30.61 Direct Supertypes

[Tool](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Observations

### 8.30.62 Associations

 used by : [Observation](#) [\*] Subsets: used by:[Occurrence](#)

Uses of an observation tool.

## **8.30.7 Class Observer**

An actor that can or has observed anything.

### 8.30.71 Direct Supertypes

[Actor](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Observations

### 8.30.72 Associations

 performs observation : [Observation](#) [\*] Subsets: performs:[Occurrence](#)

Observations of something.

 : [Indicator](#) [\*] Redefines: has ability to influence:[Resource](#)

## 8.31 Threat-risk-conceptual-model::Generic Concepts::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.

### 8.31.1 Diagram: Organization

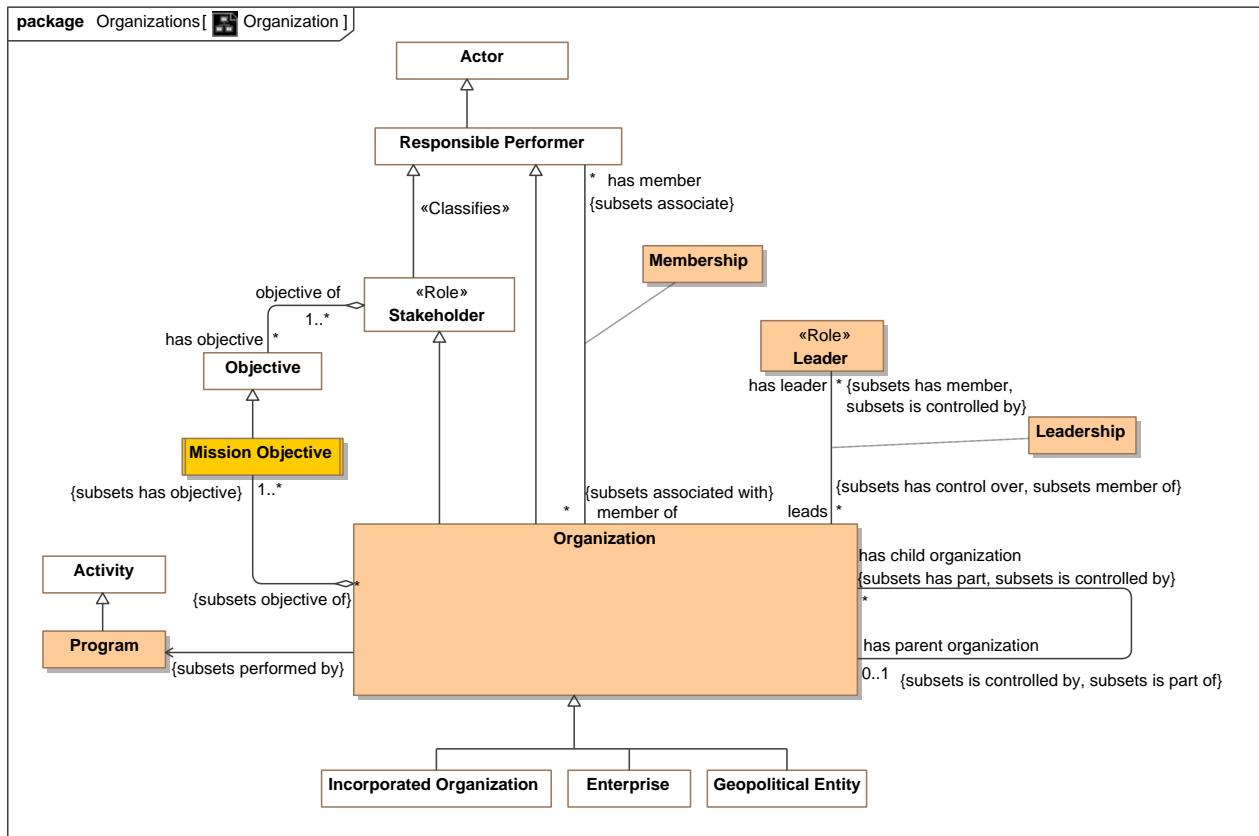


Figure 46. Organization

### 8.31.2 Association Class Membership

The participation of an actor in an *organization*. Subtypes of membership provide more explicit membership kinds.

#### 8.31.21 Direct Supertypes

[Actor Association](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Organizations

### **8.31.21 Association Ends**

 has member : [Responsible Performer](#) [\*] *Redefines:* has ability to influence: [Resource](#)  
member of an organization.

 member of : [Organization](#) [\*] *Redefines:* has ability to influence: [Resource](#)  
Organization a performer belongs to.

### **8.31.3 Class Mission Objective**

A mission is a core objective of an enterprise.

#### **8.31.31 Direct Supertypes**

[Objective](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Organizations

#### **8.31.32 Associations**

 : [Organization](#) [\*] *Subsets:* objective of: [Stakeholder](#)

### **8.31.4 Class Organization**

An *Organization* is group of persons and/or other actors and resources organized for some end or work

#### **8.31.41 Direct Supertypes**

[Controlled Entity](#), [Responsible Performer](#), [Stakeholder](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Organizations

#### **8.31.42 Associations**

 : [Program](#)

 : [Mission Objective](#) [1..\*] *Subsets:* has objective: [Objective](#)

 has leader : [Leader](#) [\*] *Subsets:* is controlled by: [Controlling Actor](#) has member: [Responsible Performer](#)

A person leading or directing an organization.

 has child organization : [Leader](#) [\*] *Subsets:* is controlled by: [Controlling Actor](#) has member: [Responsible Performer](#)

An organization organized as a component of another.

 has parent organization : [Leader](#) [\*] *Subsets:* is controlled by: [Controlling Actor](#) has member: [Responsible Performer](#)

The parent (controlling organization) of an organization.

### **8.31.5 Class Program**

A set of projects, activities, or services of an organization that are intended to meet a need.

### 8.31.51 Direct Supertypes

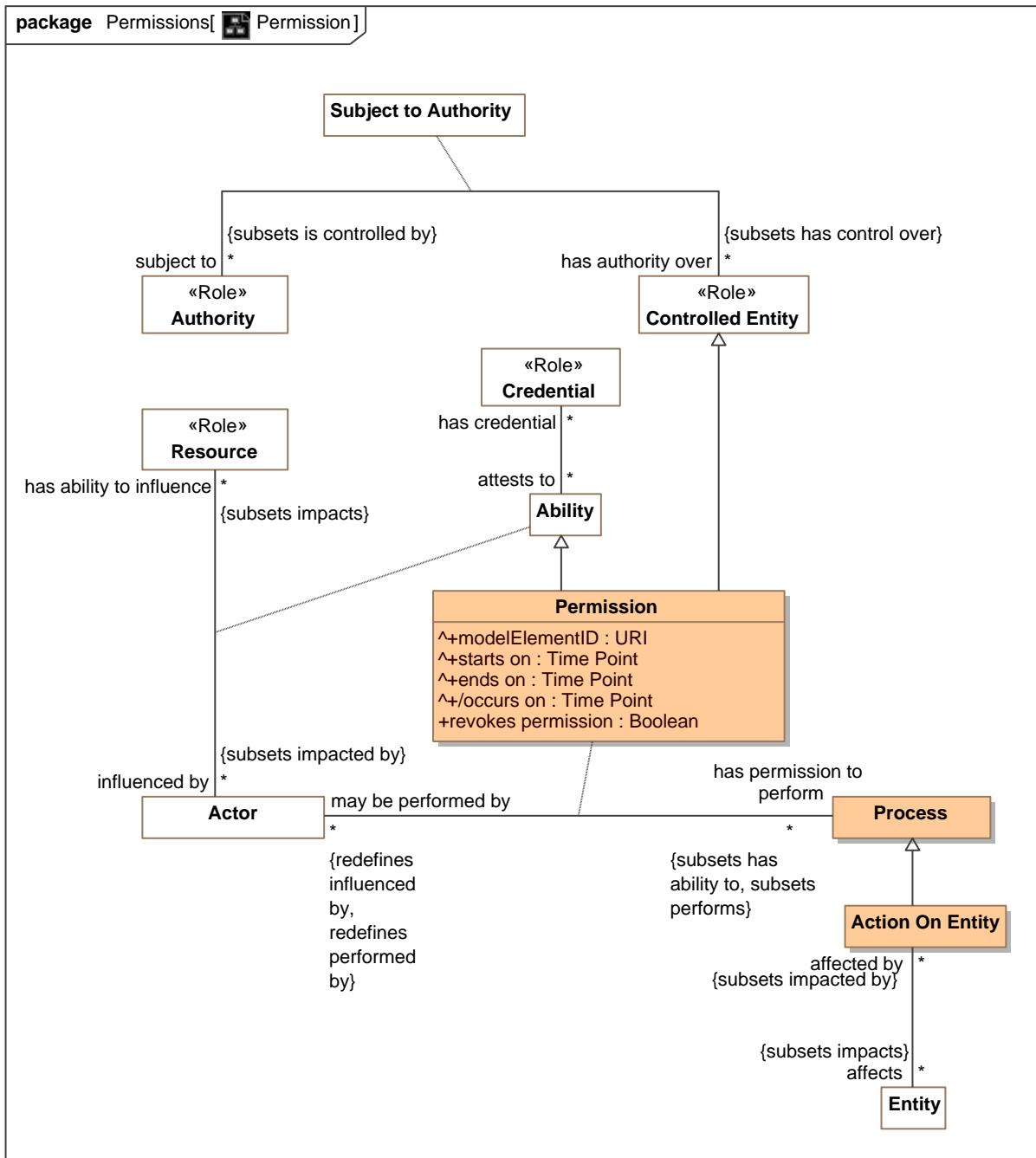
[Activity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Organizations

## 8.32 Threat-risk-conceptual-model::Generic Concepts::Permissions

Concepts relating to the permission an actor has to do something.

### 8.32.1 Diagram: Permission



**Figure 47. Permission**

### **8.32.2 Association Class Permission**

Authorization granted by an authority to an actor to perform some process.

#### 8.32.21 Direct Supertypes

[Ability](#), [Controlled Entity](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Permissions

#### **8.32.21 Association Ends**

 has permission to perform : [Process](#) [\*] Subsets: is controlled by:[Controlling Actor](#) has member:[Responsible Performer](#)

Process actor has the permission to perform.

 may be performed by : [Actor](#) [\*] Subsets: is controlled by:[Controlling Actor](#) has member:[Responsible Performer](#)

Actors that have permission to perform a process.

#### 8.32.22 Attributes

 revokes permission : [Boolean](#)

Inverts or removes the permission

## 8.33 Threat-risk-conceptual-model::Generic Concepts::Persons

The person module defines foundation concepts of people such as their location and name. More specific person attributes may augment this specification.

### 8.33.1 Diagram: Person

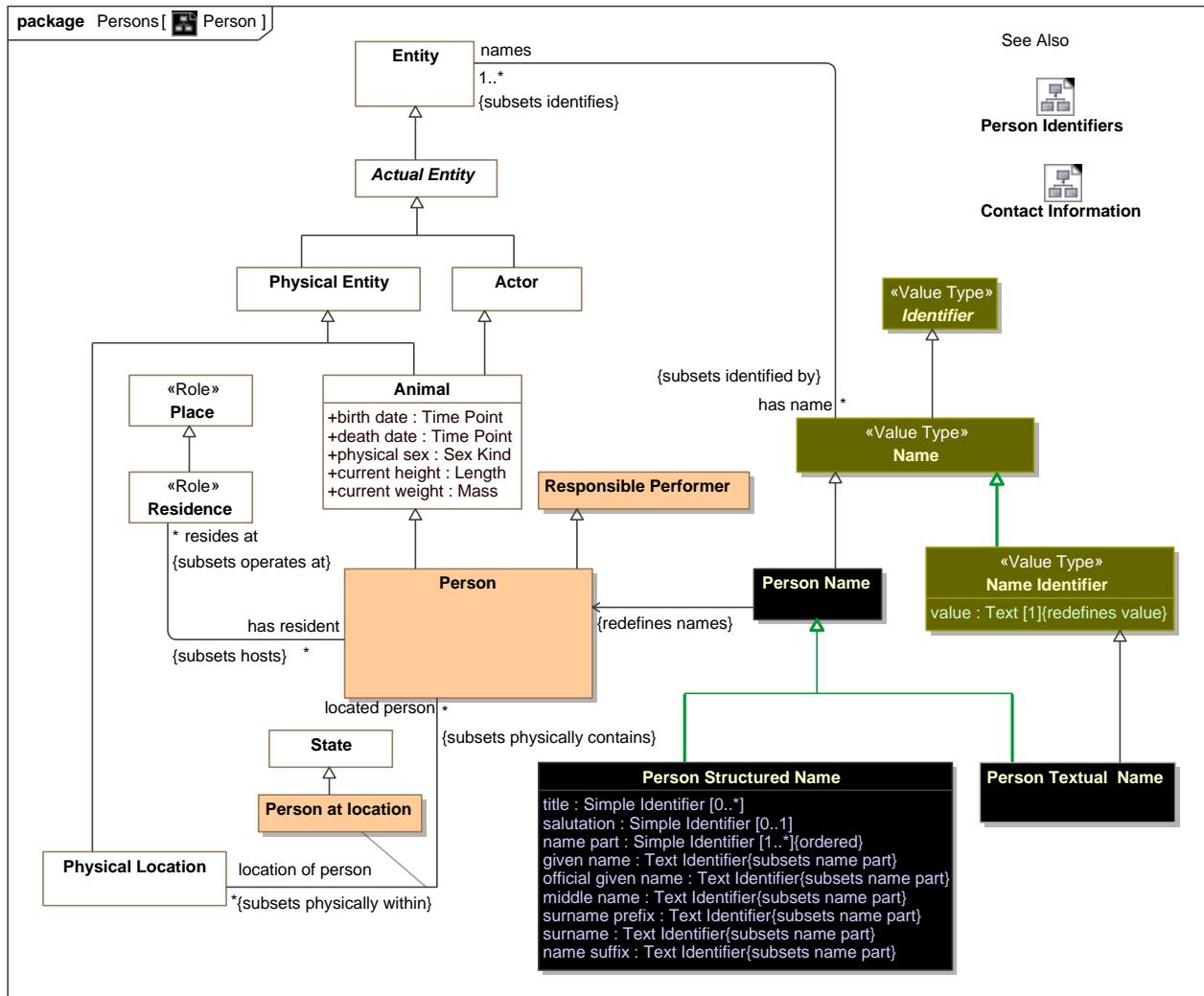
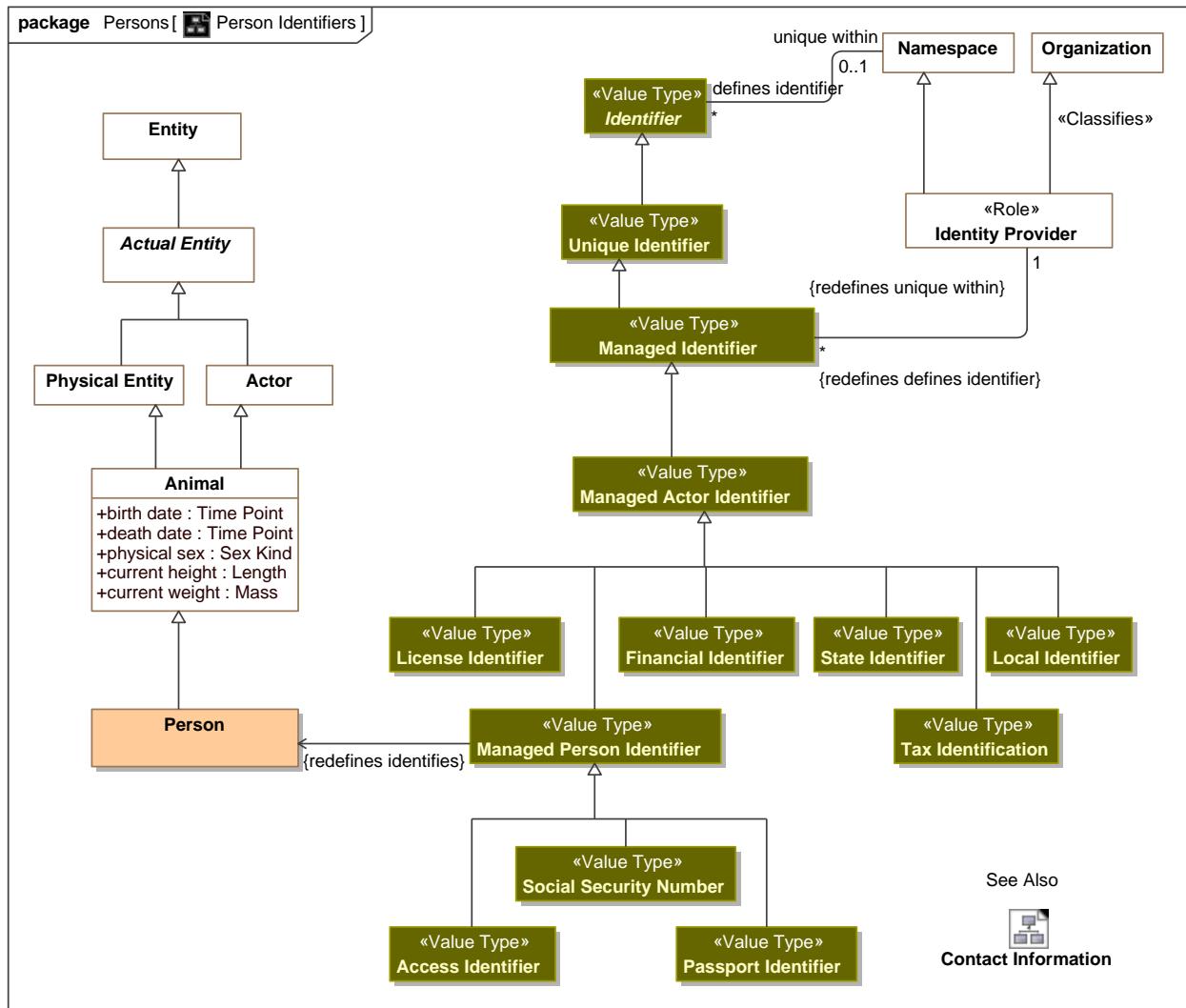


Figure 48. Person

### **8.33.2 Diagram: Person Identifiers**



**Figure 49. Person Identifiers**

### **8.33.3 Class Access Identifier**

An identification that identifies a person for access to a resource.

### 8.33.31 Direct Supertypes

## Managed Person Identifier

## **package** Threat-risk-conceptual-model::Generic Concepts::Persons

#### **8.33.4 Class Financial Identifier**

An identifier for purposes of making financial transactions, such as a credit card number or bank account.

##### **8.33.4.1 Direct Supertypes**

[Managed Actor Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Persons

#### **8.33.5 Class Managed Person Identifier**

An identifier for a person managed by some identity provider, frequently but not always a government organization.

##### **8.33.5.1 Direct Supertypes**

[Managed Actor Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Persons

##### **8.33.52 Associations**

 : [Person](#) Redefines: identifies:[Entity](#)

#### **8.33.6 Class Passport Identifier**

An identification of a passport issued to a person.[NIEM]

##### **8.33.61 Direct Supertypes**

[Managed Person Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Persons

#### **8.33.7 Class Person**

An individual human being.

##### **8.33.71 Direct Supertypes**

[Actor](#), [Animal](#), [Responsible Performer](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Persons

##### **8.33.72 Associations**

 resides at : [Residence](#) [\*] Subsets: operates at:[Place](#)

A residence of a person.

 location of person : [Physical Location](#) [\*] Subsets: physically within:[Physical Entity](#)

Where a person is located.

## **8.33.8 Association Class Person at location**

The location of a person at a particular time.

### 8.33.81 Direct Supertypes

State

**package** Threat-risk-conceptual-model::Generic Concepts::Persons

### **8.33.81 Association Ends**

 location of person : [Physical Location](#) [\*] Subsets: physically within:[Physical Entity](#)

Where a person is located.

 located person : [Person](#) [\*] Subsets: physically within:[Physical Entity](#)

Person who is at a location.

## **8.33.9 Class Person Name**

A name identifying a person.

### 8.33.91 Direct Supertypes

Name

**package** Threat-risk-conceptual-model::Generic Concepts::Persons

### 8.33.92 Associations

 : [Person](#) Redefines: names:[Entity](#)

## **8.33.10 Class Person Structured Name**

A full name of a person in a structured form.

Note: Conversion between structured and textual names is provided by the implementation.

### 8.33.101 Direct Supertypes

Person Name

**package** Threat-risk-conceptual-model::Generic Concepts::Persons

### 8.33.102 Attributes

 title : [Simple Identifier](#) [0..\*]

A title or honorific used by a person.[NIEM]

 salutation : [Simple Identifier](#) [0..1]

A formal sign or expression of greeting that is appropriate for this person.[NIEM]

 name part : [Simple Identifier](#) [1..\*]

Parts of a name, e.g., surname, given name.

◊ given name : [Text Identifier](#)

A first name of a person.[NIEM]

◊ official given name : [Text Identifier](#)

A name, out of possibly multiple given names, that a person selects to use as his or her official given name.[NIEM]

◊ middle name : [Text Identifier](#)

A middle name of a person.[NIEM]

◊ surname prefix : [Text Identifier](#)

A prefix that precedes this person's family name such as Van, Von.[NIEM]

◊ surname : [Text Identifier](#)

A last name or family name of a person.[NIEM]

◊ name suffix : [Text Identifier](#)

A term appended after the family name that qualifies the name.[NIEM]

### **8.33.11 Class Person Textual Name**

A single word or phrase used to identify a person, perhaps as part of a full name.

Note: Conversion between structured and textual names is provided by the implementation.

#### **8.33.111 Direct Supertypes**

[Name Identifier](#), [Person Name](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Persons

### **8.33.12 Class Social Security Number**

A unique identification reference to a living person; assigned by the United States Social Security Administration.[NIEM]

#### **8.33.121 Direct Supertypes**

[Managed Person Identifier](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Persons

## 8.34 Threat-risk-conceptual-model::Generic Concepts::Places

Places are buildings or localities used or intended for a purpose.

### 8.34.1 Diagram: Place

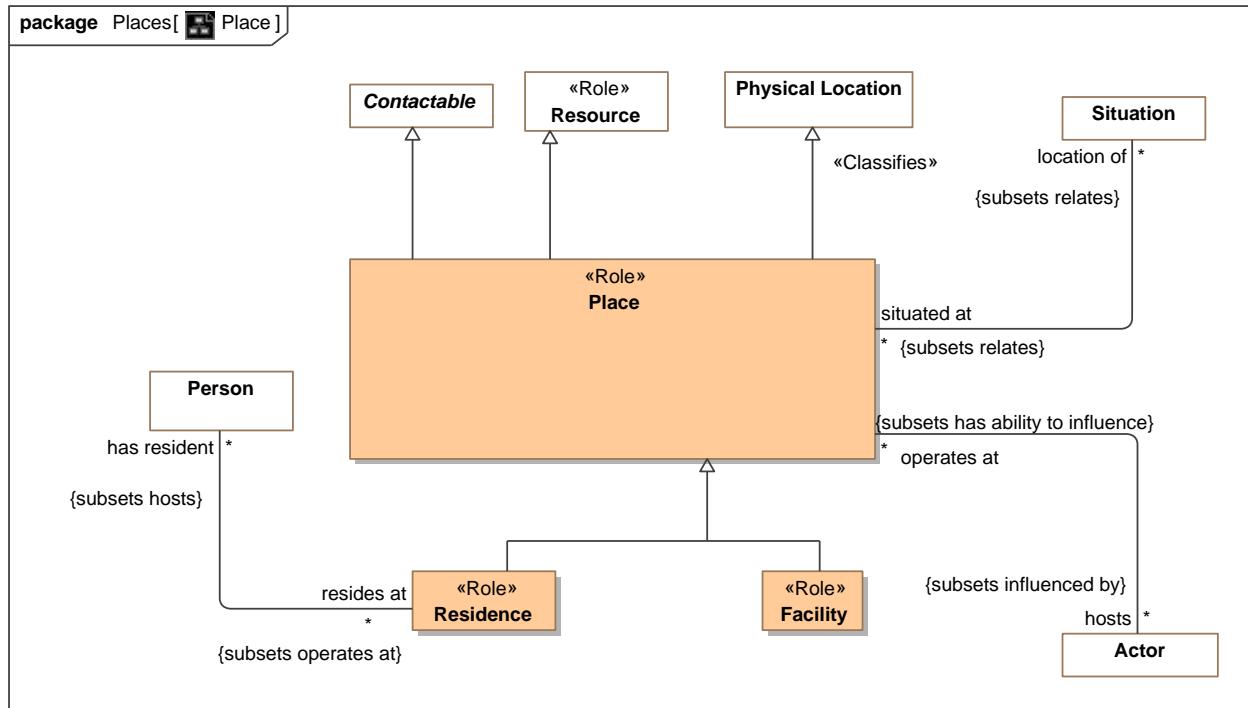


Figure 50. Place

### 8.34.2 Class Facility

A building, place, or structure that provides a particular service. [NIEM]

#### 8.34.21 Direct Supertypes

[Place](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Places

### 8.34.3 Class Place

A building or locality used or intended for a specific purpose such as a house or factory.

### 8.34.31 Direct Supertypes

[Contactable](#), [Physical Location](#), [Resource](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Places

### 8.34.32 Associations

 hosts : [Actor](#) [\*] Subsets: influenced by:[Actor](#)

Actors who utilizes a place.

 location of : [Situation](#) [\*] Subsets: relates:[Anything](#)

Situations (occurrences, incidents, static arrangements) that are located at a particular location.

## 8.34.4 Class Residence

A place where people live/reside.

### 8.34.41 Direct Supertypes

[Place](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Places

### 8.34.42 Associations

 has resident : [Person](#) [\*] Subsets: hosts:[Actor](#)

People living at a residence.

## 8.35 Threat-risk-conceptual-model::Generic Concepts::Policies

Policies deal with conditions asserted on one entity by another. This includes requirements and laws.

### 8.35.1 Diagram: Policy

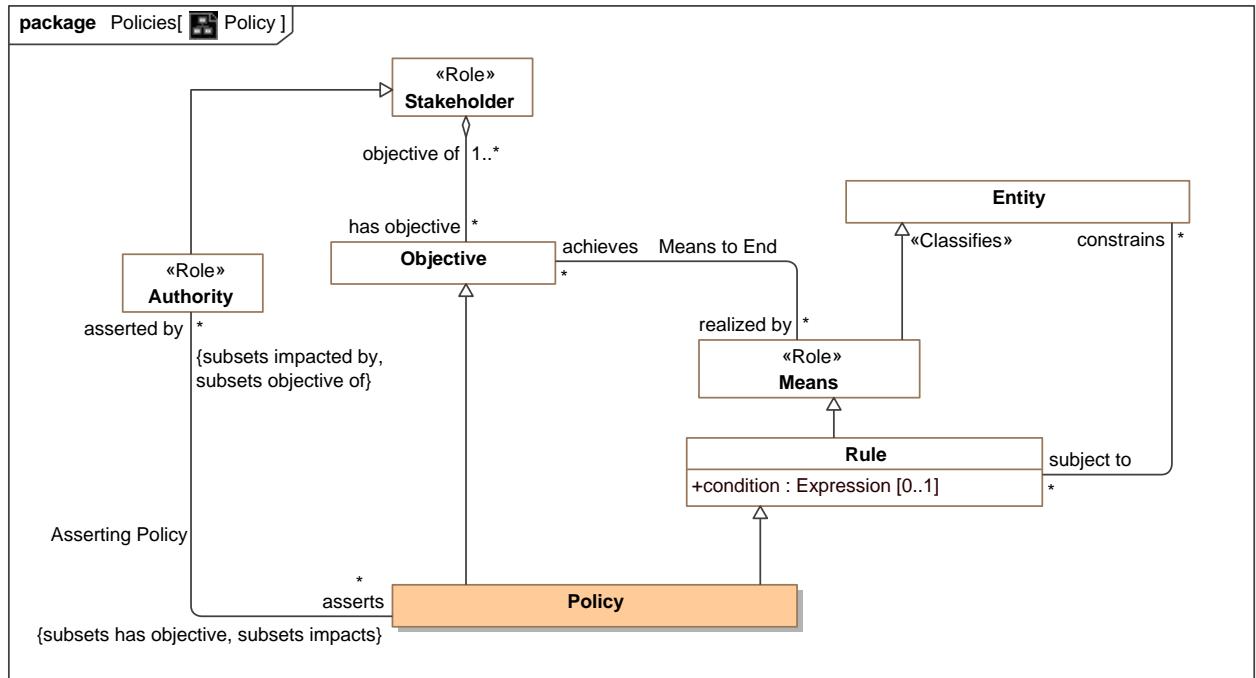


Figure 51. Policy

### 8.35.2 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.

Policies include requirements.

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.

#### 8.35.21 Direct Supertypes

[Objective](#), [Rule](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Policies

### 8.35.22 Associations

/ asserted by : [Authority](#) [\*] Subsets: impacted by:[Entity](#) objective of:[Stakeholder](#)

The authority that asserts a policy

### 8.35.3 Association Subject of Rule

A requirement an entity is subject to.

**package** Threat-risk-conceptual-model::Generic Concepts::Policies

### 8.35.31 Association Ends

/ constrains : [Entity](#) [\*] Subsets: impacted by:[Entity](#) objective of:[Stakeholder](#)

Entities a rule applies to.

/ subject to : [Rule](#) [\*] Subsets: impacted by:[Entity](#) objective of:[Stakeholder](#)

A rule that must be satisfied by an entity.

/ degree of satisfaction : [Metric](#) Subsets: impacted by:[Entity](#) objective of:[Stakeholder](#)

A metric for how much a requirement is satisfied.

## 8.36 Threat-risk-conceptual-model::Generic Concepts::Predictions

Predictions are acts where an actor predicts that some possible situation will occur.

### 8.36.1 Diagram: Prediction

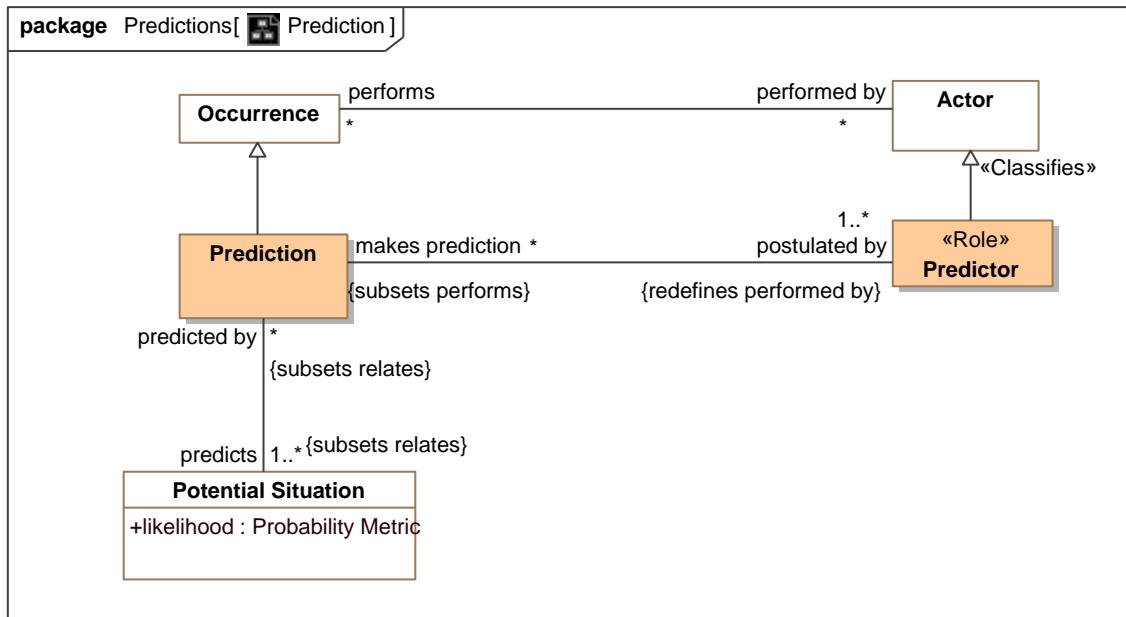


Figure 52. Prediction

### 8.36.2 Class Prediction

A prediction that potential situations will happen.

#### 8.36.21 Direct Supertypes

Occurrence

**package** Threat-risk-conceptual-model::Generic Concepts::Predictions

#### 8.36.22 Associations

predicts : Potential Situation [1..\*] Subsets: relates:Anything

The predicted situation.

postulated by : Predictor [1..\*] Redefines: performed by:Actor

Predictor making a prediction.

### **8.36.3 Class Predictor**

The role of one making predictions.

#### 8.36.31 Direct Supertypes

Actor

**package** Threat-risk-conceptual-model::Generic Concepts::Predictions

#### 8.36.32 Associations

 makes prediction : [Prediction](#) [\*] Subsets: performs:[Occurrence](#)

A prediction made by a predictor.

## 8.37 Threat-risk-conceptual-model::Generic Concepts::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.

### 8.37.1 Diagram: Resource

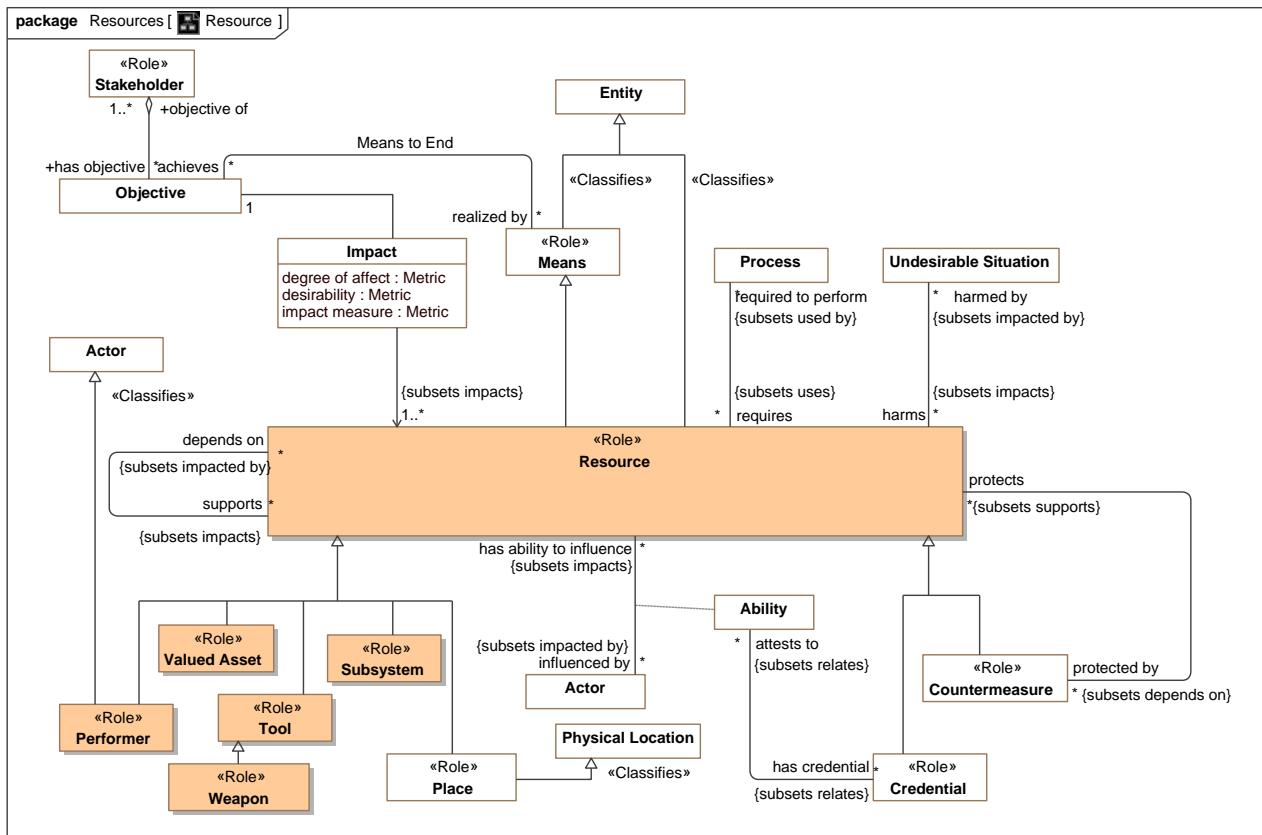


Figure 53. Resource

### 8.37.2 Class Performer

A performer is an actor that is a resource to another entity.

#### 8.37.21 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Generic Concepts::Resources

### 8.37.3 Class Resource

Anything required for or helpful to any operation, activity, process or capability - directly or indirectly. Sometimes called an "asset".

#### 8.37.31 Direct Supertypes

[Entity](#), [Means](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Resources

#### 8.37.32 Associations

/ supports : [Prediction](#) [\*] Subsets: performs:[Occurrence](#)

Other resources this resource supports in any way.

/ required to perform : [Process](#) [\*] Subsets: used by:[Occurrence](#)

A process that is required by a resource.

/ has vulnerability : [Vulnerability](#) [\*]

Vulnerabilities of a resource, or ways it may be compromised.

/ depends on : [Vulnerability](#) [\*]

Any resource that is required to support another resource.

/ harmed by : [Probability Metric](#)

Danger that damages anything.

/ protected by : [Countermeasure](#) [\*] Subsets: depends on:[Resource](#)

Safeguards of a resource.

/ has risk : [Risk](#) [\*]

Risk to a resource.

/ : [Resource Actions](#)

/ has failure : [Failure](#) [\*]

Realized or potential failures of a resource.

/ : [Attack](#)

### 8.37.4 Class Tool

The role of some inanimate thing used to facilitate a process or activity by an actor performing the process or activity.

#### 8.37.41 Direct Supertypes

[Resource](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Resources

### **8.37.5 Class Weapon**

Anything used by an actor to cause harm.

#### 8.37.51 Direct Supertypes

[Tool](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Resources

#### 8.37.52 Associations

 exploits : [Vulnerability](#) [\*]

Vulnerability that a weapon exploits.

## 8.38 Threat-risk-conceptual-model::Generic Concepts::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]

### 8.38.1 Diagram: System

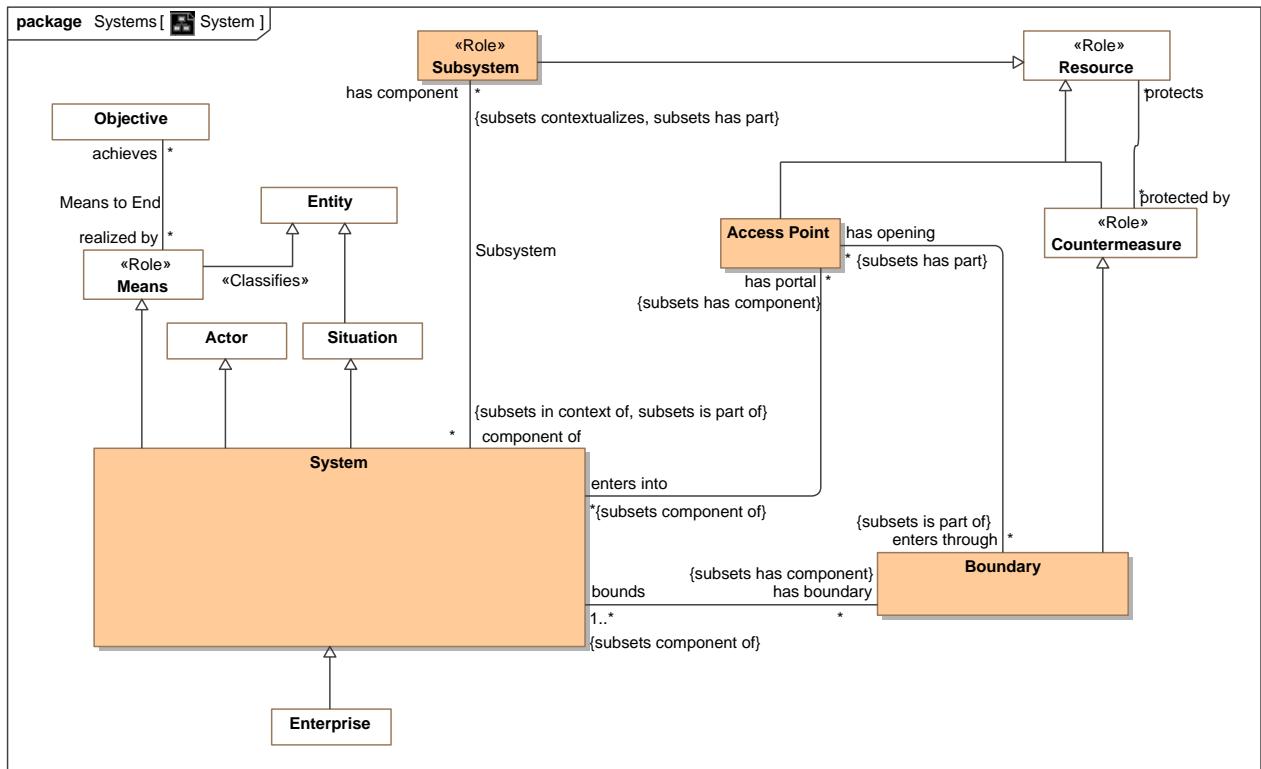


Figure 54. System

### 8.38.2 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.

### 8.38.21 Direct Supertypes

Resource

**package** Threat-risk-conceptual-model::Generic Concepts::Systems

### 8.38.22 Associations

/ enters through : [Boundary](#) [\*] Subsets: is part of:[Entity](#)

Boundary through which an entry point allows access. e.g., the wall a door goes through.

/ enters into : [System](#) [\*] Subsets: component of:[System](#)

System into which an entry point allows access.

/ traversed using : [Entry Action](#) Subsets: affected by:[Action On Entity](#)

Action that utilizes an access point for entry.

/ : [Exit Action](#) Subsets: traversed using:[Entry Action](#)

## 8.38.3 Class Boundary

Something on the edge of a system, protecting resources of the system/enterprise.

e.g., Fences, firewalls.

### 8.38.31 Direct Supertypes

Countermeasure

**package** Threat-risk-conceptual-model::Generic Concepts::Systems

### 8.38.32 Associations

/ bounds : [System](#) [1..\*] Subsets: component of:[System](#)

System bound by a boundary,

/ has opening : [Access Point](#) [\*] Subsets: has part:[Entity](#)

Entry points through a boundary.

## 8.38.4 Association Subsystem

Part of a system

**package** Threat-risk-conceptual-model::Generic Concepts::Systems

### 8.38.41 Association Ends

/ has component : [Subsystem](#) [\*] Subsets: has part:[Entity](#)

Subsystems (parts) of a system that contribute to the systems function and/or purpose.

/ component of : [System](#) [\*] Subsets: has part:[Entity](#)

System(s) of which something is a part.

## **8.38.5 Class Subsystem**

A part of a system.

### 8.38.51 Direct Supertypes

[Resource](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Systems

### 8.38.52 Associations

 component of : [System](#) [\*] Subsets: is part of:[Entity](#) in context of:[Context](#)

System(s) of which something is a part.

## **8.38.6 Class System**

A system is a collection of parts and relationships among these parts that may be organized to accomplish some purpose.  
[OMG MDA Guide]

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 some objective for some stakeholder.

### 8.38.61 Direct Supertypes

[Actor](#), [Means](#), [Situation](#)

**package** Threat-risk-conceptual-model::Generic Concepts::Systems

### 8.38.62 Associations

 has boundary : [Boundary](#) [\*] Subsets: has component:[Subsystem](#)

Boundary of a system (or enterprise).

 has portal : [Access Point](#) [\*] Subsets: has component:[Subsystem](#)

Points of possible entry into a system.

 has component : [Subsystem](#) [\*] Subsets: has part:[Entity](#) contextualizes:[Anything](#)

Subsystems (parts) of a system that contribute to the systems function and/or purpose.

## 8.39 Threat-risk-conceptual-model::Generic Concepts::Transfer

The transfer of something from one actor to another, including information transfer.

### 8.39.1 Diagram: Transfer

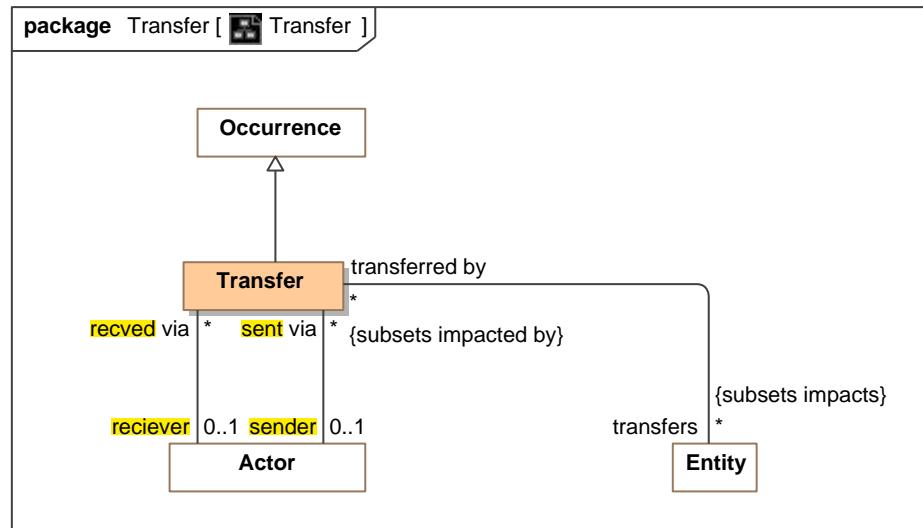


Figure 55. Transfer

### 8.39.2 Class Transfer

The **transfer** (send/receive) of something between actors.

#### 8.39.21 Direct Supertypes

Occurrence

**package** Threat-risk-conceptual-model::Generic Concepts::Transfer

#### 8.39.22 Associations

/ sender : Actor [0..1]

Sender of something transferred.

/ reciever : Actor [0..1]

Receiver of something transferred.

/ transfers : Entity [\*] Subsets: impacts:Entity

The transferred entity.

## 8.40 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 a danger 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.

This foundational information is then expanded with metrics and interrelationships such that threats and risks can be fully understood and dealt with.

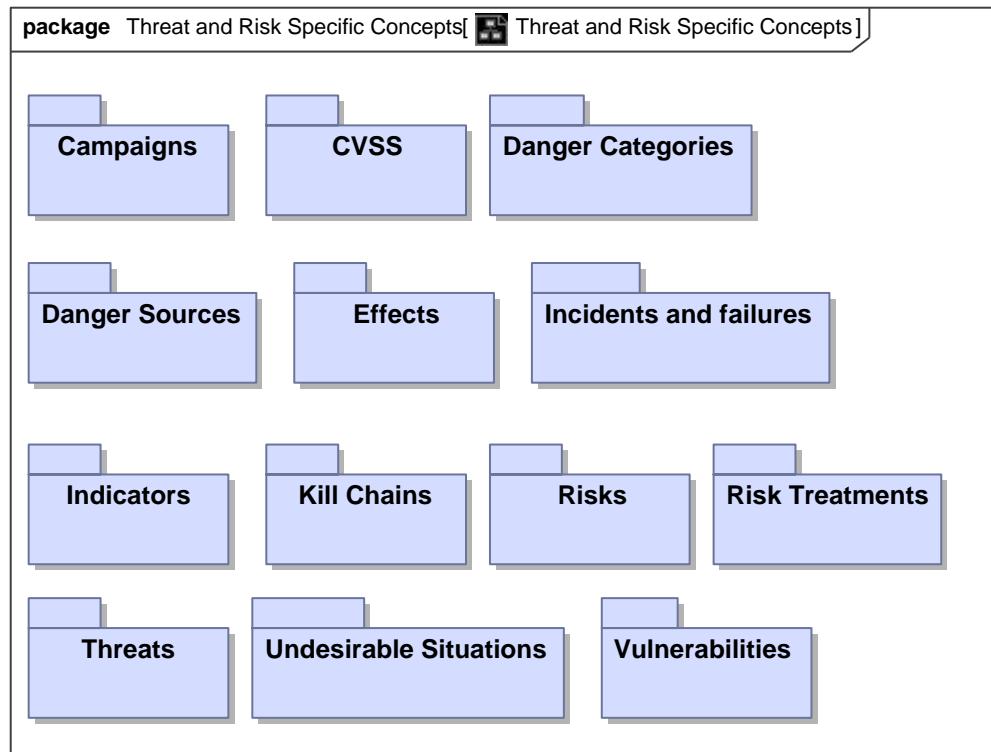
Fundamental risk/threat specific concepts include:

- [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 dangers derived from the general concept of a "situation"; which is fundamental to this specification.

### 8.40.1 Diagram: Threat and Risk Specific Concepts



**Figure 56. Threat and Risk Specific Concepts**

## **8.41 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS**

[cvss] Currently, 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.

### 8.41.1 Diagram: Vulnerability Vectors

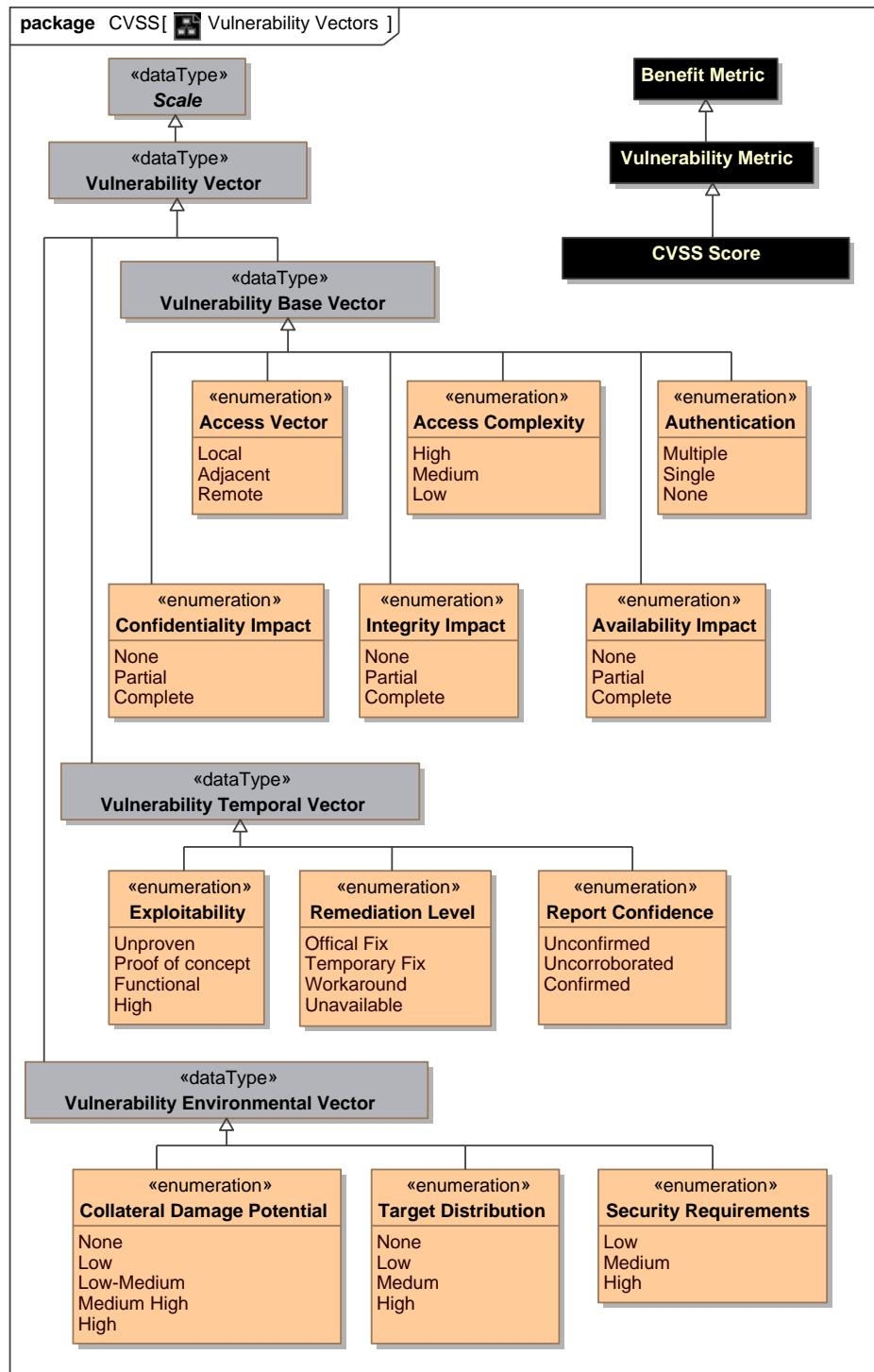


Figure 57. Vulnerability Vectors

## **8.41.2 Class CVSS Score**

Common Vulnerability Scoring System. A number in the range of 0..10.

[CVSS]

### **8.41.21 Direct Supertypes**

[Vulnerability Metric](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS

### **8.41.22 Enumeration 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.

### **8.41.22 Direct Known Superclasses**

[Vulnerability Base Vector](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS

**public enum** Access Complexity

{High, Medium, Low}

## **8.41.22 Literals**

➊ 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.

➋ 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).

### 8.41.23 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.

#### 8.41.23Direct Known Superclasses

##### Vulnerability Base Vector

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

### 8.41.23Literals

#### 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.

### 8.41.24 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.”

#### **8.41.24Direct Known Superclasses**

[Vulnerability Base Vector](#)

package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS

public enum Authentication

{Multiple, Single, None}

#### **8.41.24Literals**

 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.

#### **8.41.25 Enumeration Availability Impact**

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

#### **8.41.25Direct Known Superclasses**

[Vulnerability Base Vector](#)

package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS

public enum Availability Impact

{None, Partial, Complete}

#### **8.41.25Literals**

 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.

#### 8.41.26 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.

##### 8.41.26 Direct Known Superclasses

###### Vulnerability Environmental Vector

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS
```

```
public enum Collateral Damage Potential
```

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

#### 8.41.26 Literals



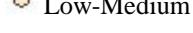
None

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



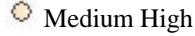
Low

[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.

#### 8.41.27 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.

#### **8.41.27Direct Known Superclasses**

[Vulnerability Base Vector](#)

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

#### **8.41.27Literals**

 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.)

#### **8.41.28 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.

#### **8.41.28Direct Known Superclasses**

[Vulnerability Temporal Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS
public enum Exploitability
{Unproven, Proof of concept, Functional, High}
```

#### **8.41.28Literals**

 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).

#### 8.41.29 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.

#### 8.41.29Direct Known Superclasses

[Vulnerability Base Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS
```

```
public enum Integrity Impact
```

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

#### 8.41.29Literals

- 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.

#### 8.41.210 Enumeration Remediation Level

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

#### 8.41.210Direct Known Superclasses

[Vulnerability Temporal Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS
```

```
public enum Remediation Level
```

{Official Fix, Temporary Fix, Workaround, Unavailable}

#### 8.41.210Literals



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

#### 8.41.211 Enumeration Report Confidence

[CVSS] Confidence in a report.

#### 8.41.211Direct Known Superclasses

[Vulnerability Temporal Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS
```

```
public enum Report Confidence
```

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

#### 8.41.211Literals



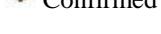
Unconfirmed

[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.

#### 8.41.212 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).

#### 8.41.212 Direct Known Superclasses

##### [Vulnerability Environmental Vector](#)

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

#### 8.41.212 Literals



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).



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).



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)

#### 8.41.213 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.

#### 8.41.213 Direct Known Superclasses

##### [Vulnerability Environmental Vector](#)

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::CVSS
```

public enum Target Distribution

{None, Low, Medium, High}

### 8.41.213 Literals

ⓘ 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.

ⓘ 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.

## 8.42 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.

### 8.42.1 Diagram: Campaign

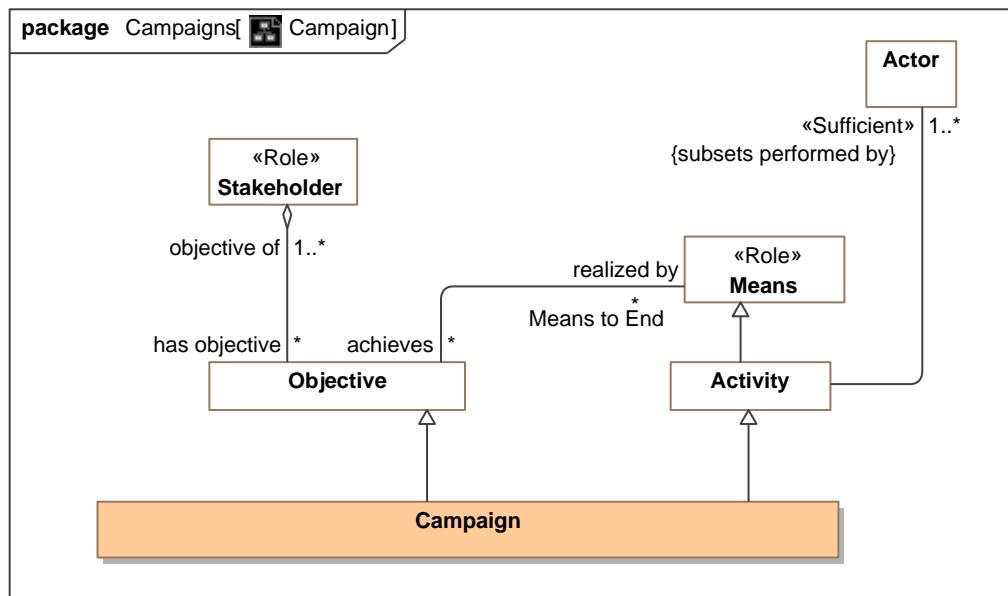


Figure 58. Campaign

### 8.42.2 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.

#### 8.42.21 Direct Supertypes

[Activity](#), [Objective](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Campaigns

## 8.43 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.

### 8.43.1 Diagram: Danger Categories

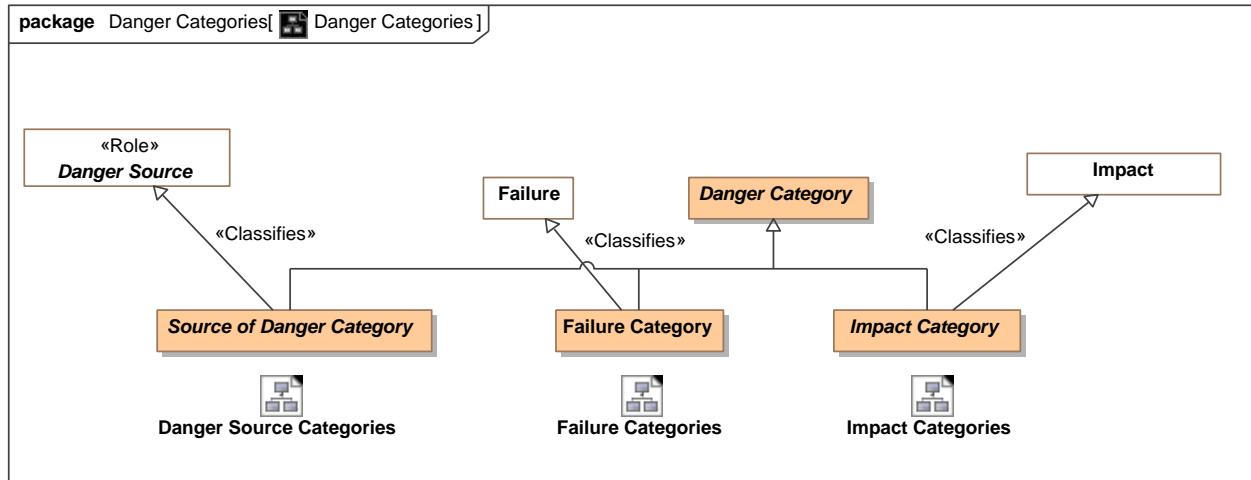


Figure 59. Danger Categories

### 8.43.2 Diagram: Danger Source Categories

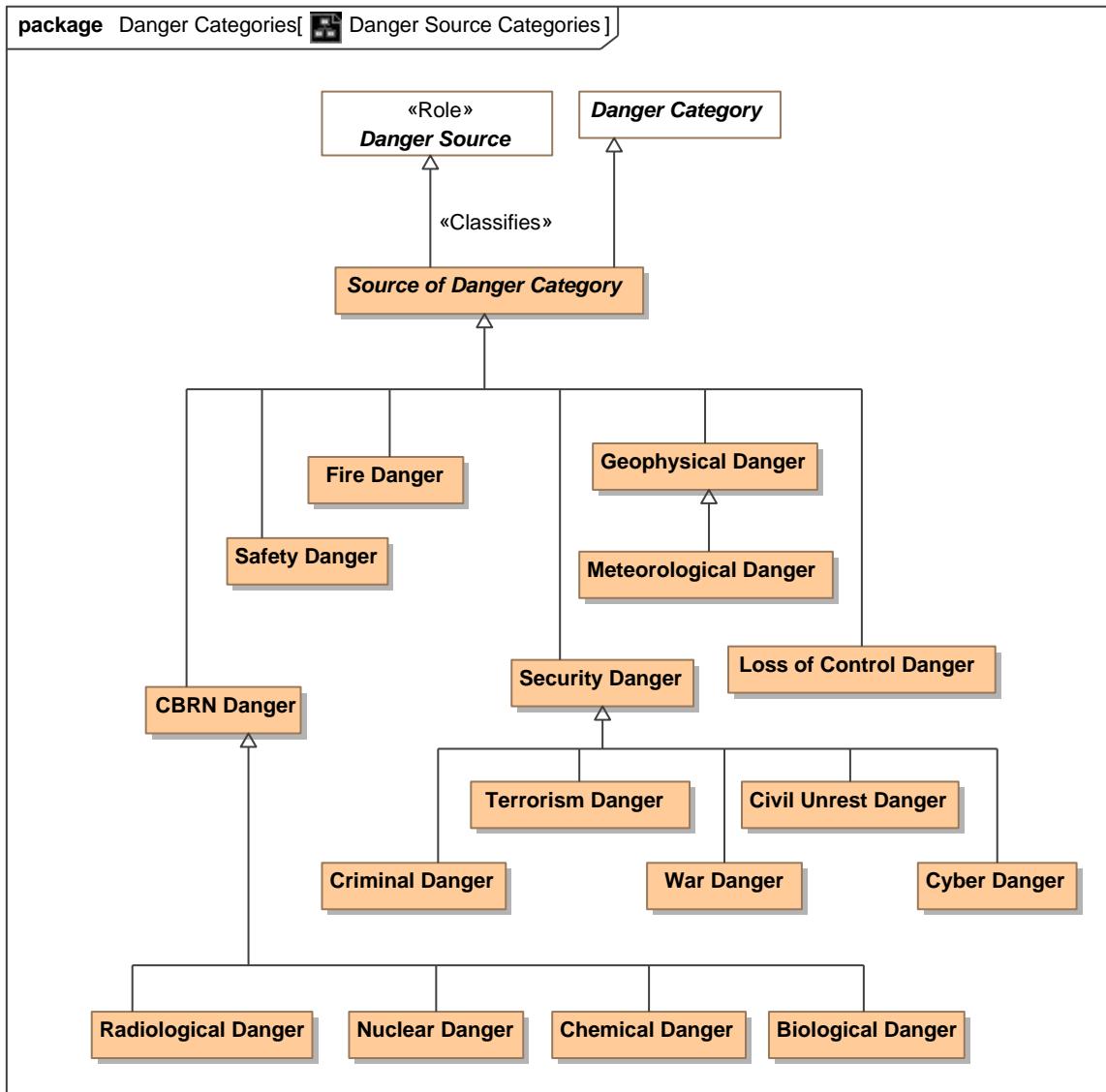


Figure 60. Danger Source Categories

### 8.43.3 Diagram: Failure Categories

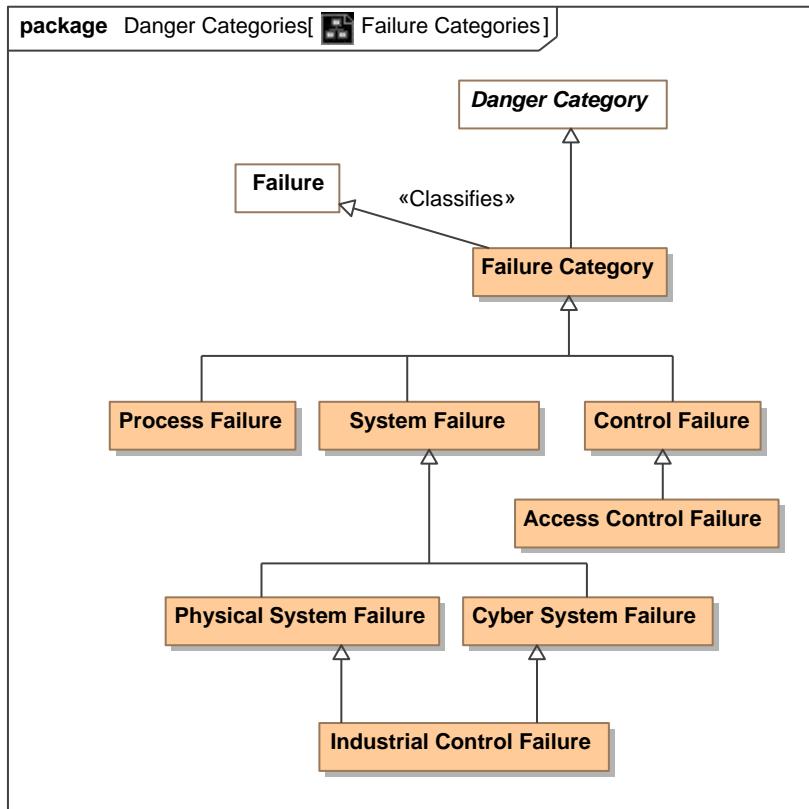


Figure 61. Failure Categories

#### 8.43.4 Diagram: Impact Categories

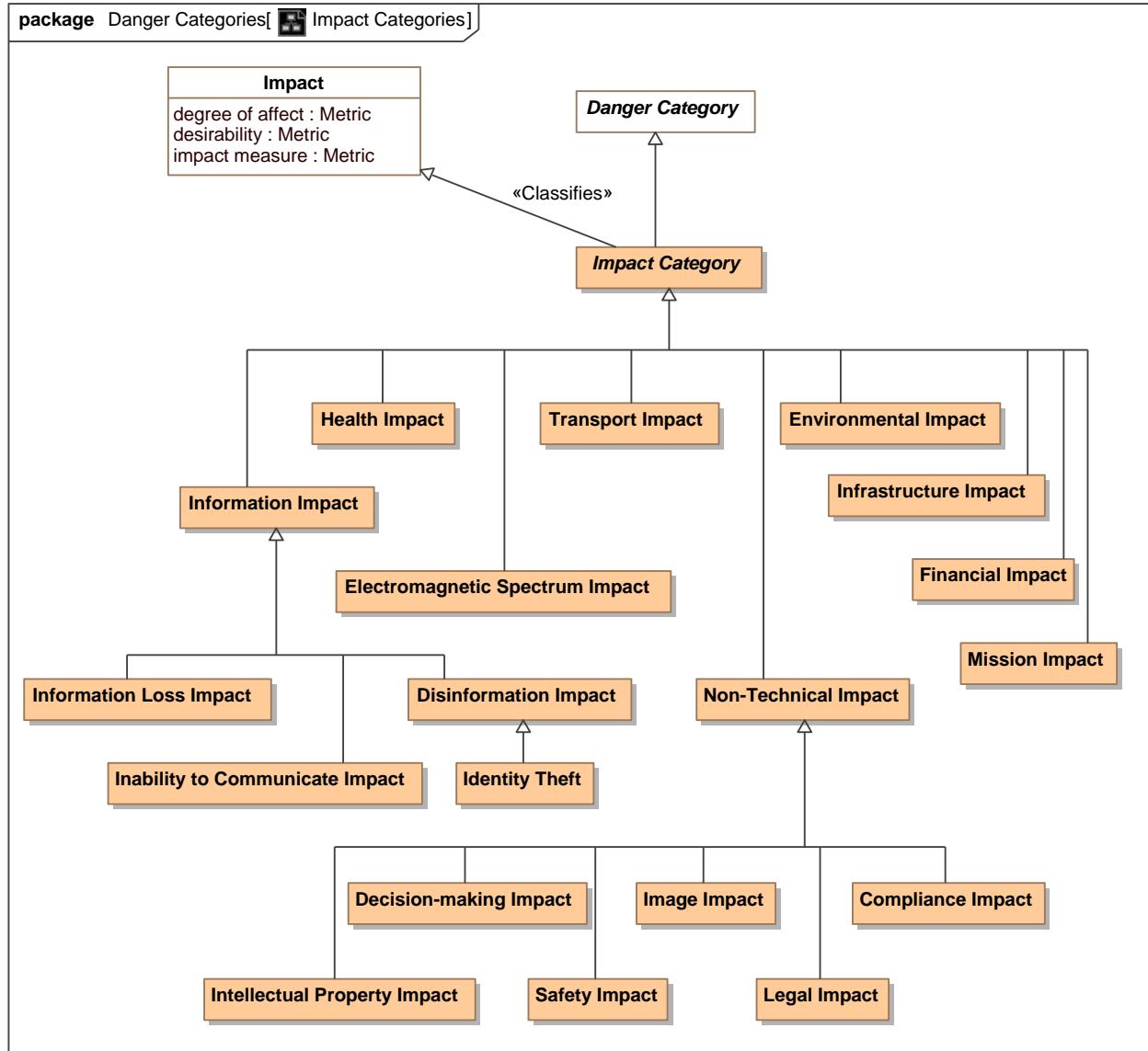


Figure 62. Impact Categories

#### 8.43.5 Class Access Control Failure

Failure of permission controls to prevent unintended access.

##### 8.43.51 Direct Supertypes

[Control Failure](#)

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

## **8.43.6 Class Biological Danger**

Any danger from a biological source.

### 8.43.61 Direct Supertypes

[CBRN Danger](#)

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

## **8.43.7 Class CBRN Danger**

A Chemical, biological, radiological or nuclear danger.

### 8.43.71 Direct Supertypes

[Source of Danger Category](#)

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

## **8.43.8 Class Chemical Danger**

A danger from a chemical.

### 8.43.81 Direct Supertypes

[CBRN Danger](#)

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

## **8.43.9 Class Civil Unrest Danger**

Civil disorder, also known as civil unrest or civil strife, is a broad term that is typically used by law enforcement to describe unrest caused by a group of people.[Wikipedia]

### 8.43.91 Direct Supertypes

[Security Danger](#)

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

## **8.43.10 Class Compliance Impact**

Impact on the ability to comply with policies.

### 8.43.101 Direct Supertypes

[Non-Technical Impact](#)

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

### **8.43.11 Class Control Failure**

Failure of a policy or control process.

#### 8.43.111 Direct Supertypes

[Failure Category](#)

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

### **8.43.12 Class Criminal Danger**

Danger from a criminal activity.

#### 8.43.121 Direct Supertypes

[Security Danger](#)

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

### **8.43.13 Class Cyber Danger**

Danger related to computer systems and networks.

#### 8.43.131 Direct Supertypes

[Security Danger](#)

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

### **8.43.14 Class Cyber System Failure**

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

#### 8.43.141 Direct Supertypes

[System Failure](#)

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

### **8.43.15 Class Danger Category**

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

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

### **8.43.16 Class Decision-making Impact**

Impact on the ability to make informed decisions.

#### 8.43.161 Direct Supertypes

[Non-Technical Impact](#)

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

### **8.43.17 Class Disinformation Impact**

Danger resulting from incorrect information as the result of intentional acts.

#### 8.43.171 Direct Supertypes

[Information Impact](#)

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

### **8.43.18 Class Electromagnetic Spectrum Impact**

Any disruption in spectrum.

#### 8.43.181 Direct Supertypes

[Impact Category](#)

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

### **8.43.19 Class Environmental Impact**

Any danger to the environment.

#### 8.43.191 Direct Supertypes

[Impact Category](#)

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

### **8.43.20 Class Failure Category**

Any category of failure of a resource.

#### 8.43.201 Direct Supertypes

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

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

### **8.43.21 Class Financial Impact**

Loss of capital or ability to obtain capital.

#### 8.43.211 Direct Supertypes

[Impact Category](#)

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

## **8.43.22 Class Fire Danger**

Fire suppression and rescue. [CAP]

### 8.43.221 Direct Supertypes

[Source of Danger Category](#)

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

## **8.43.23 Class Geophysical Danger**

Geophysical danger (e.g., landslide) [CAP]

### 8.43.231 Direct Supertypes

[Source of Danger Category](#)

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

## **8.43.24 Class Health Impact**

A danger to people's health.

### 8.43.241 Direct Supertypes

[Impact Category](#)

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

## **8.43.25 Class Identity Theft**

The assumption of another's identity .

### 8.43.251 Direct Supertypes

[Disinformation Impact](#)

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

## **8.43.26 Class Image Impact**

Impact to how an entity is viewed by others.

### 8.43.261 Direct Supertypes

[Non-Technical Impact](#)

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

### **8.43.27 Class Impact Category**

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

#### 8.43.271 Direct Supertypes

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

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

### **8.43.28 Class Inability to Communicate Impact**

Impact to the ability to communicate.

#### 8.43.281 Direct Supertypes

[Information Impact](#)

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

### **8.43.29 Class Industrial Control Failure**

Any danger to the control of industrial systems.

#### 8.43.291 Direct Supertypes

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

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

### **8.43.30 Class Information Impact**

Danger related to information.

#### 8.43.301 Direct Supertypes

[Impact Category](#)

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

### **8.43.31 Class Information Loss Impact**

Danger of any information being obtained by parties not intended to have that information by the information stewards and/or owner.

#### 8.43.311 Direct Supertypes

[Information Impact](#)

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

### **8.43.32 Class Infrastructure Impact**

Classification of impact to infrastructure such that it is not longer available to fulfill objectives.

#### 8.43.321 Direct Supertypes

[Impact Category](#)

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

### **8.43.33 Class Intellectual Property Impact**

Any loss or compromise to intellectual property.

#### 8.43.331 Direct Supertypes

[Non-Technical Impact](#)

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

### **8.43.34 Class Legal Impact**

Any impact to legal status or legal measures.

#### 8.43.341 Direct Supertypes

[Non-Technical Impact](#)

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

### **8.43.35 Class Loss of Control Danger**

Any danger resulting from the control of a system gained by parties not intended to have that control by those with authority over the system.

#### 8.43.351 Direct Supertypes

[Source of Danger Category](#)

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

### **8.43.36 Class Meteorological Danger**

Meteorological impact (e.g., flood).

#### 8.43.361 Direct Supertypes

[Geophysical Danger](#)

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

### **8.43.37 Class Mission Impact**

Impact on the ability to achieve a mission purpose.

#### 8.43.371 Direct Supertypes

[Impact Category](#)

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

### **8.43.38 Class Non-Technical Impact**

Impact to other than the ability to operate.

#### 8.43.381 Direct Supertypes

[Impact Category](#)

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

### **8.43.39 Class Nuclear Danger**

Danger from a nuclear blast.

#### 8.43.391 Direct Supertypes

[CBRN Danger](#)

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

### **8.43.40 Class Physical System Failure**

Danger of failure of any physical system.

#### 8.43.401 Direct Supertypes

[System Failure](#)

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

### **8.43.41 Class Process Failure**

Failure of a process to fulfill its objectives.

#### 8.43.411 Direct Supertypes

[Failure Category](#)

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

### **8.43.42 Class Radiological Danger**

Any danger from radiation.

#### 8.43.421 Direct Supertypes

[CBRN Danger](#)

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

#### 8.43.43 Class Safety Danger

General emergency and public safety danger. [CAP]

#### 8.43.431 Direct Supertypes

[Source of Danger Category](#)

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

#### 8.43.44 Class Safety Impact

Impact to safety of a resource.

#### 8.43.441 Direct Supertypes

[Non-Technical Impact](#)

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

#### 8.43.45 Class Security Danger

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

#### 8.43.451 Direct Supertypes

[Source of Danger Category](#)

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

#### 8.43.46 Class Source of Danger Category

A categorization of any source of danger.

#### 8.43.461 Direct Supertypes

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

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

#### 8.43.47 Class System Failure

Failure of any system - physical, financial, cyber, etc. such that the system is no longer available to serve objectives.

#### 8.43.471 Direct Supertypes

[Failure Category](#)

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

#### **8.43.48 Class Terrorism Danger**

Danger from terrorism.

##### 8.43.481 Direct Supertypes

[Security Danger](#)

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

#### **8.43.49 Class Transport Impact**

Public and private transportation.[CAP]

##### 8.43.491 Direct Supertypes

[Impact Category](#)

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

#### **8.43.50 Class War Danger**

Danger from acts of war.

##### 8.43.501 Direct Supertypes

[Security Danger](#)

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

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

The source of any danger - natural, systematic, or intentional

### 8.44.1 Diagram: Danger Sources

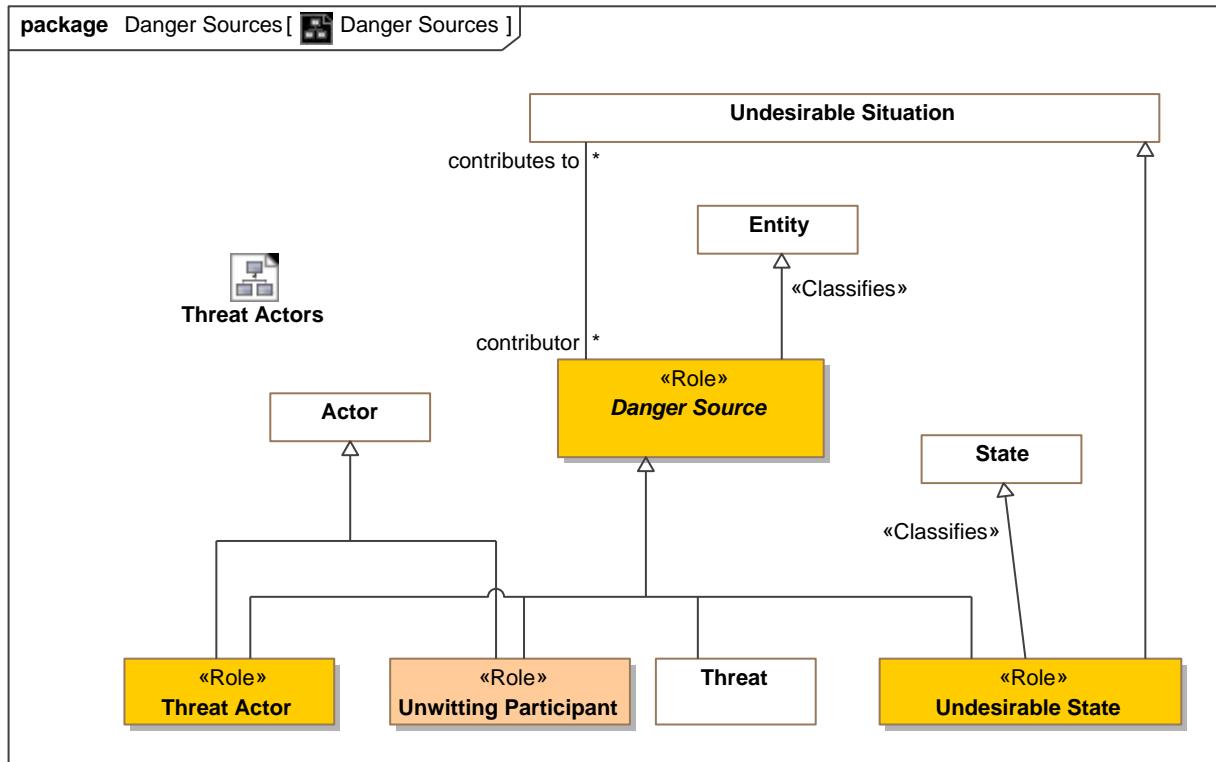


Figure 63. Danger Sources

## 8.44.2 Diagram: Threat Actors

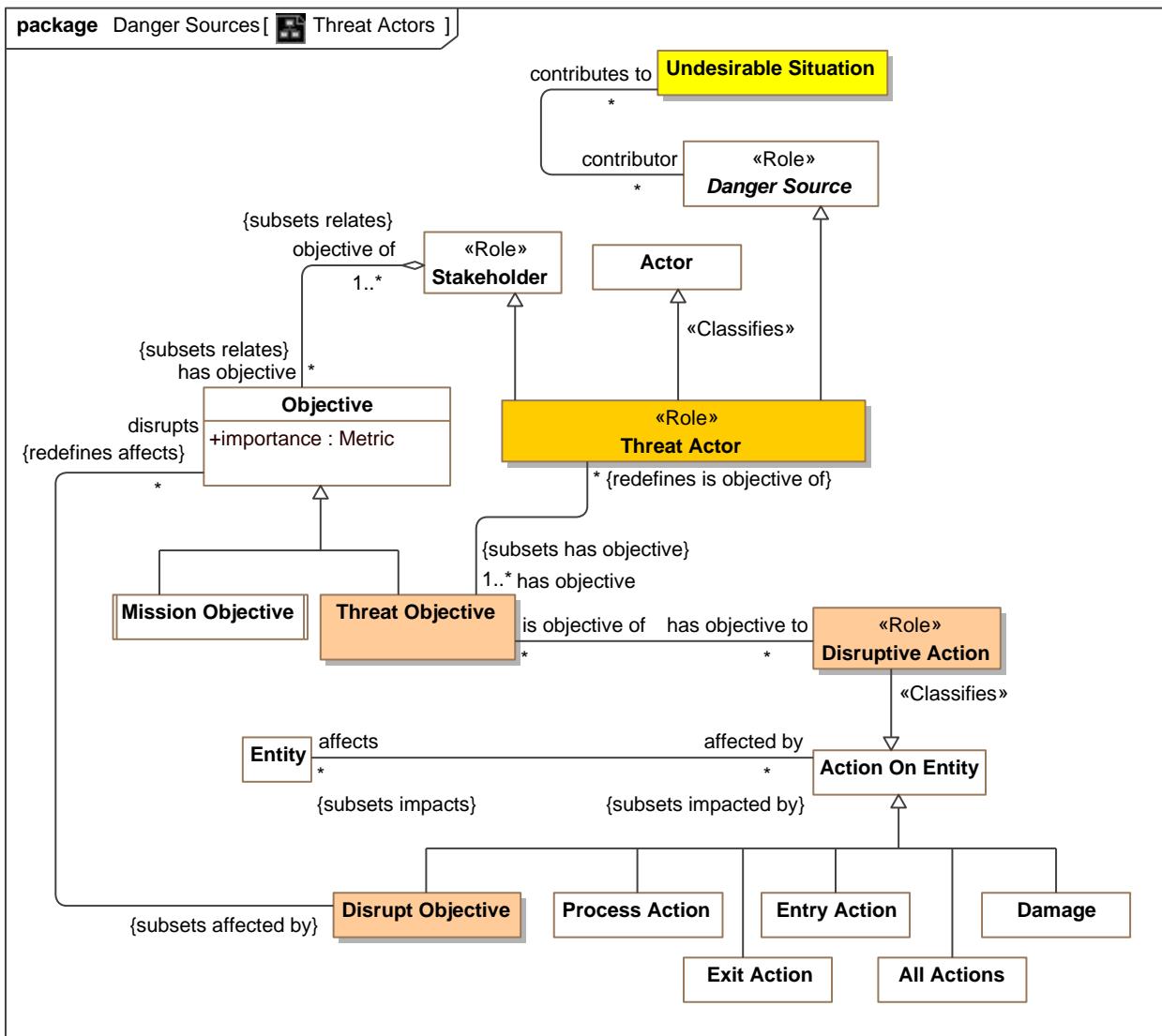


Figure 64. Threat Actors

## 8.44.3 Class Danger Source

The source of any danger - natural, systematic, or intentional

### 8.44.31 Direct Supertypes

[Entity](#)

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

### 8.44.32 Associations

/ contributes to : [Probability Metric](#)

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

### 8.44.4 Class Disrupt Objective

Action to disrupt the objective of another.

#### 8.44.41 Direct Supertypes

[Action On Entity](#)

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

#### 8.44.42 Associations

/ disrupts : [Objective](#) [\*] *Redefines:* affects:[Entity](#)

An objective that is disrupted.

### 8.44.5 Class Disruptive Action

Any action that serves the objectives of a threat actor.

#### 8.44.51 Direct Supertypes

[Action On Entity](#)

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

#### 8.44.52 Associations

/ is objective of : [Threat Objective](#) [\*]

objective of an action.

### 8.44.6 Class Threat Actor

An actor; all or partially responsible for some undesired situation - threat, risk, or attack. Threat actors may or may not have intent to do harm.

#### 8.44.61 Direct Supertypes

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

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

#### 8.44.62 Associations

/ perpetrates : [Attack](#) [\*] *Subsets:* performs:[Occurrence](#) contributes to:[Undesirable Situation](#)

The activity performed by a threat actor to cause or contribute to a dangerous situation in a real or possible world.

/ has objective : [Threat Objective](#) [1..\*] *Subsets:* has objective:[Objective](#)

Objective of a threat actor.

### **8.44.7 Class Threat Objective**

Something that one's efforts or actions are intended to attain such that it damages another in some way or obtains resources not intended for the actor.

#### **8.44.71 Direct Supertypes**

[Objective](#)

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

#### **8.44.72 Associations**

 has objective to : [Disruptive Action](#) [\*]

Objective of a threat actor to disrupt something.

 : [Threat Actor](#) [\*] *Redefines:* is objective of:[Threat Objective](#)

## **8.45 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects**

Actions that impact various kinds of entities in specific ways. Such actions can be the subject of permissions, capabilities, or objectives.

### 8.45.1 Diagram: Threat Effects

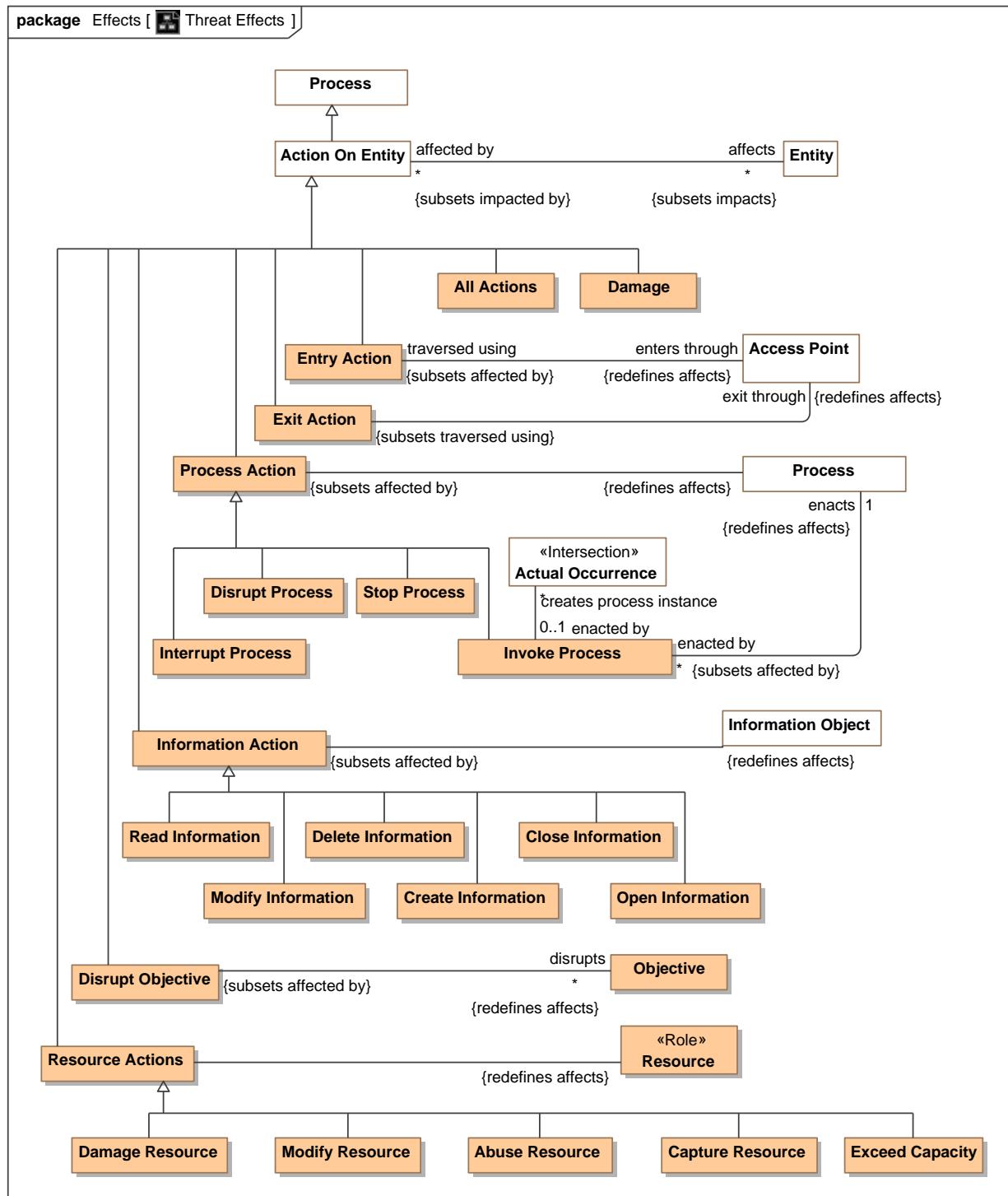


Figure 65. Threat Effects

## **8.45.2 Class Abuse Resource**

Action to abuse a resource.

### 8.45.21 Direct Supertypes

[Resource Actions](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

## **8.45.3 Class All Actions**

All possible effects to an entity.

### 8.45.31 Direct Supertypes

[Action On Entity](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

## **8.45.4 Class Capture Resource**

Action to capture or gain control of some resource.

### 8.45.41 Direct Supertypes

[Resource Actions](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

## **8.45.5 Class Close Information**

An action that removes information from visibility.

### 8.45.51 Direct Supertypes

[Information Action](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

## **8.45.6 Class Create Information**

An action that creates information.

### 8.45.61 Direct Supertypes

[Information Action](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

## **8.45.7 Class Damage**

Action to cause damage to an entity.

### 8.45.71 Direct Supertypes

[Action On Entity](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

### 8.45.8 Class Damage Resource

Action to damage some resource.

### 8.45.81 Direct Supertypes

[Damage, Resource Actions](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

### 8.45.9 Class Delete Information

An action to delete information.

### 8.45.91 Direct Supertypes

[Information Action](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

### 8.45.10 Class Disrupt Process

An action to cause a process to not achieve its desired affect.

### 8.45.101 Direct Supertypes

[Damage, Process Action](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

### 8.45.11 Class Entry Action

An action of entering through a boundary.

### 8.45.111 Direct Supertypes

[Action On Entity](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

### 8.45.112 Associations

/ enters through : [Access Point](#) Redefines: affects:[Entity](#)

An action of entering into something through an opening in a boundary.

## **8.45.12 Class Exceed Capacity**

Action to exceed the capacity of some resource.

### 8.45.121 Direct Supertypes

[Resource Actions](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

## **8.45.13 Class Exit Action**

An action of exiting through a boundary.

### 8.45.131 Direct Supertypes

[Action On Entity](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

### 8.45.132 Associations

/ exit through : [Access Point](#) *Redefines:* affects:[Entity](#)

The action of exiting through a boundary via an access point.

## **8.45.14 Class Interrupt Process**

An action that pauses or stops a process.

### 8.45.141 Direct Supertypes

[Process Action](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

## **8.45.15 Class Modify Information**

Action to change information (for good or bad reasons).

### 8.45.151 Direct Supertypes

[Information Action](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

## **8.45.16 Class Modify Resource**

Action to modify some resource.

### 8.45.161 Direct Supertypes

[Resource Actions](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

### **8.45.17 Class Open Information**

Action to gain visibility to some information, e.g., Open a file or an envelope.

#### 8.45.171 Direct Supertypes

[Information Action](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

### **8.45.18 Class Read Information**

An action to read, access, or understand some information.

#### 8.45.181 Direct Supertypes

[Information Action](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

### **8.45.19 Class Resource Actions**

An action impacting a potential or realized resource/asset.

#### 8.45.191 Direct Supertypes

[Action On Entity](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

#### 8.45.192 Associations

 : [Resource](#) Redefines: affects:[Entity](#)

### **8.45.20 Class Stop Process**

An action to terminate a process.

#### 8.45.201 Direct Supertypes

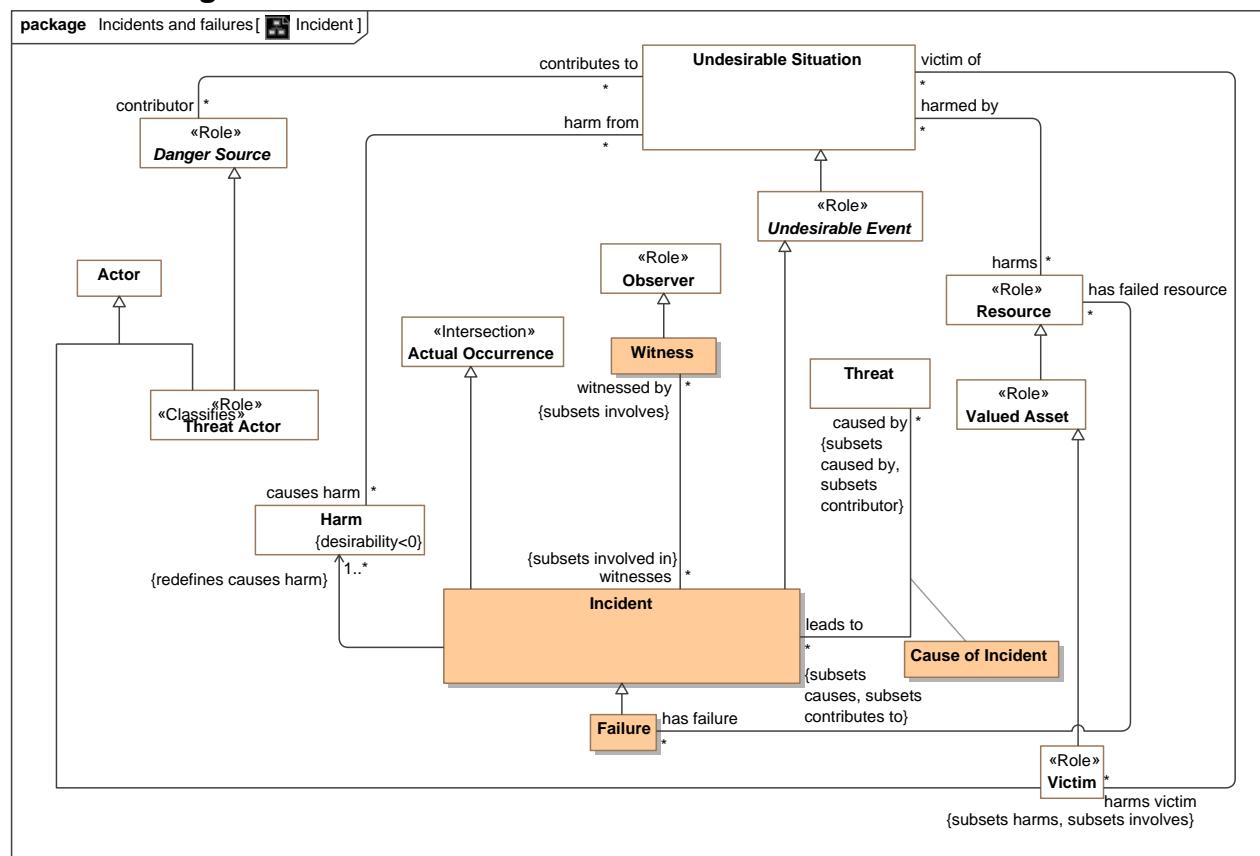
[Process Action](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Effects

## **8.46 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents and failures**

Concepts relating to incidents - undesired events that actually happen.

### **8.46.1 Diagram: Incident**



**Figure 66.** Incident

#### **8.46.2 Association Class Cause of Incident**

The cause of an incident

### 8.46.21 Direct Supertypes

### **Cause and Effect**

## **package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents and failures

### **8.46.21 Association Ends**

 leads to : [Incident](#) [\*] *Redefines*: affects: [Entity](#)

Incident that is the result of a threat.

 caused by : [Threat](#) [\*] *Redefines*: affects: [Entity](#)

Cause of an incident.

### **8.46.22 Associations**

 has condition : [Vulnerability](#) [\*]

A condition for a causation of an incident or failure.

### **8.46.3 Class Failure**

Failure is an incident where a resource does not achieve its objectives.

#### **8.46.31 Direct Supertypes**

[Incident](#)

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

#### **8.46.32 Associations**

 has failed resource : [Resource](#) [\*]

Resource that fails.

### **8.46.4 Class Incident**

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.

#### **8.46.41 Direct Supertypes**

[Actual Occurrence](#), [Undesirable Event](#)

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

#### **8.46.42 Associations**

 caused by : [Threat](#) [\*] *Subsets*: contributor:[Danger Source](#) caused by:[Situation](#)

Cause of an incident.

 : [Harm](#) [1..\*] *Redefines*: causes harm:[Harm](#)

 witnessed by : [Witness](#) [\*] *Subsets*: involves:[Actor](#)

Witnesses of an incident

## **8.46.5 Class Witness**

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

### 8.46.51 Direct Supertypes

Observer

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

### 8.46.52 Associations

 witnesses : Incident [\*] Subsets: involved in:Situation

Incident witnessed.

## **8.47 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.

### 8.47.1 Diagram: Indicator

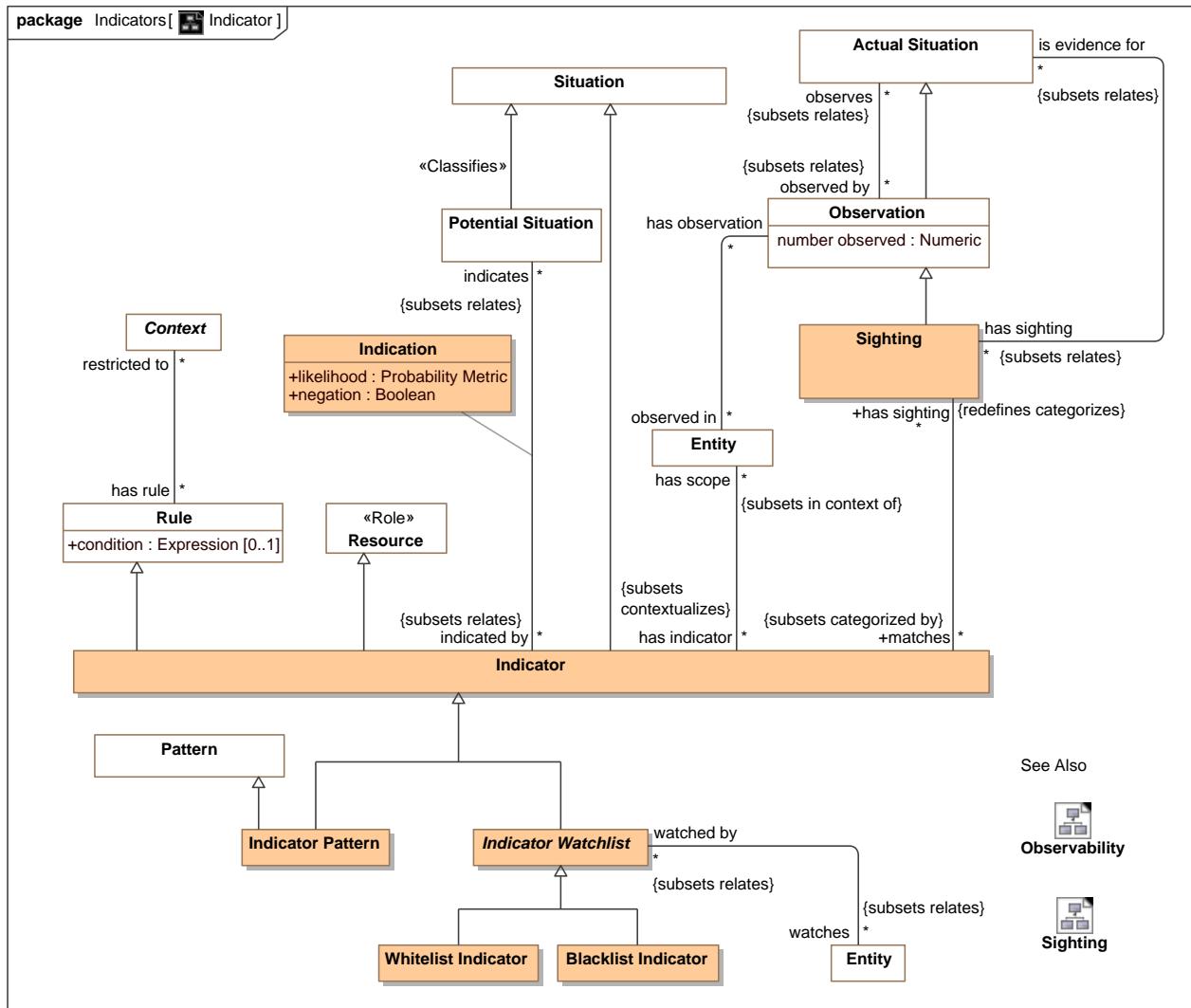


Figure 67. Indicator

## 8.47.2 Diagram: Sighting

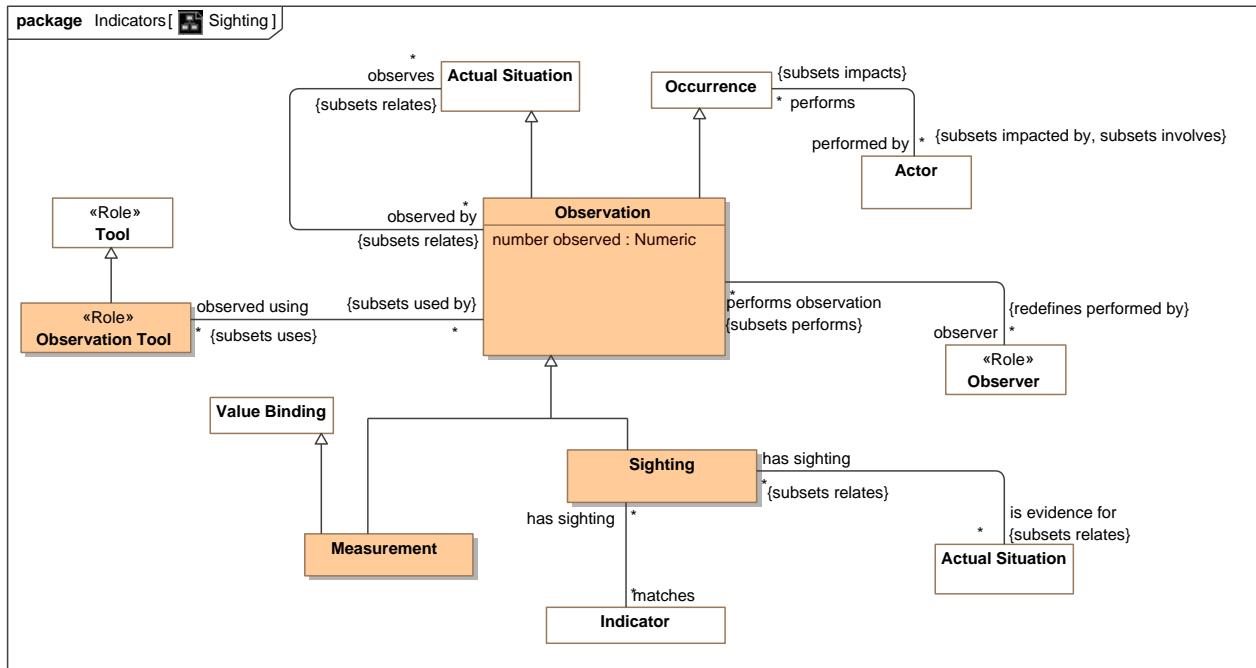


Figure 68. Sighting

## 8.47.3 Class Blacklist Indicator

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

### 8.47.3.1 Direct Supertypes

[Indicator Watchlist](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators

## 8.47.4 Association Class Indication

An indication relation - that a particular indicator indicates a situation.

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators

### 8.47.4.1 Association Ends

indicates : [Potential Situation](#) [\*] Subsets: involved in: [Situation](#)

The situation or situation or situation pattern indicated by an indicator.

indicated by : [Indicator](#) [\*] Subsets: involved in: [Situation](#)

Indicator of a possible situation.

#### 8.47.42 Attributes

 likelihood : [Probability Metric](#)

The probability that the indication actually indicates the situation.

 negation : [Boolean](#)

The negate field specifies the absence of the pattern [STIX]indicates the specified situation.

#### 8.47.5 Class Indicator

An **indicator** is a type of a *sighting* which defines conditions <*selected by*> under which sightings are relevant to the situations it *indicates*. Sightings suggests further study or action based on a **course of action rule**. Indicators may be used to identify situations or entities that should be watched for.

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) specific context.

#### 8.47.51 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators

#### 8.47.52 Associations

 has sighting : [Sighting](#) [\*] *Redefines*: categorizes:[Anything](#)

Sightings of an indicator.

 indicates : [Potential Situation](#) [\*] *Subsets*: relates:[Anything](#)

The situation or situation or situation pattern indicated by an indicator.

 : [Observer](#) [\*] *Redefines*: influenced by:[Actor](#)

 monitored by : [Monitoring Safeguard](#) [\*] *Subsets*: relates:[Anything](#)

Activities monitoring an indicator.

 has scope : [Entity](#) [\*] *Subsets*: in context of:[Context](#)

The scope of an indicator, where it is valid.

#### 8.47.6 Class Indicator Pattern

An indicator defined by a pattern

#### 8.47.61 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators

## **8.47.7 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".

### **8.47.71 Direct Supertypes**

[Indicator](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators

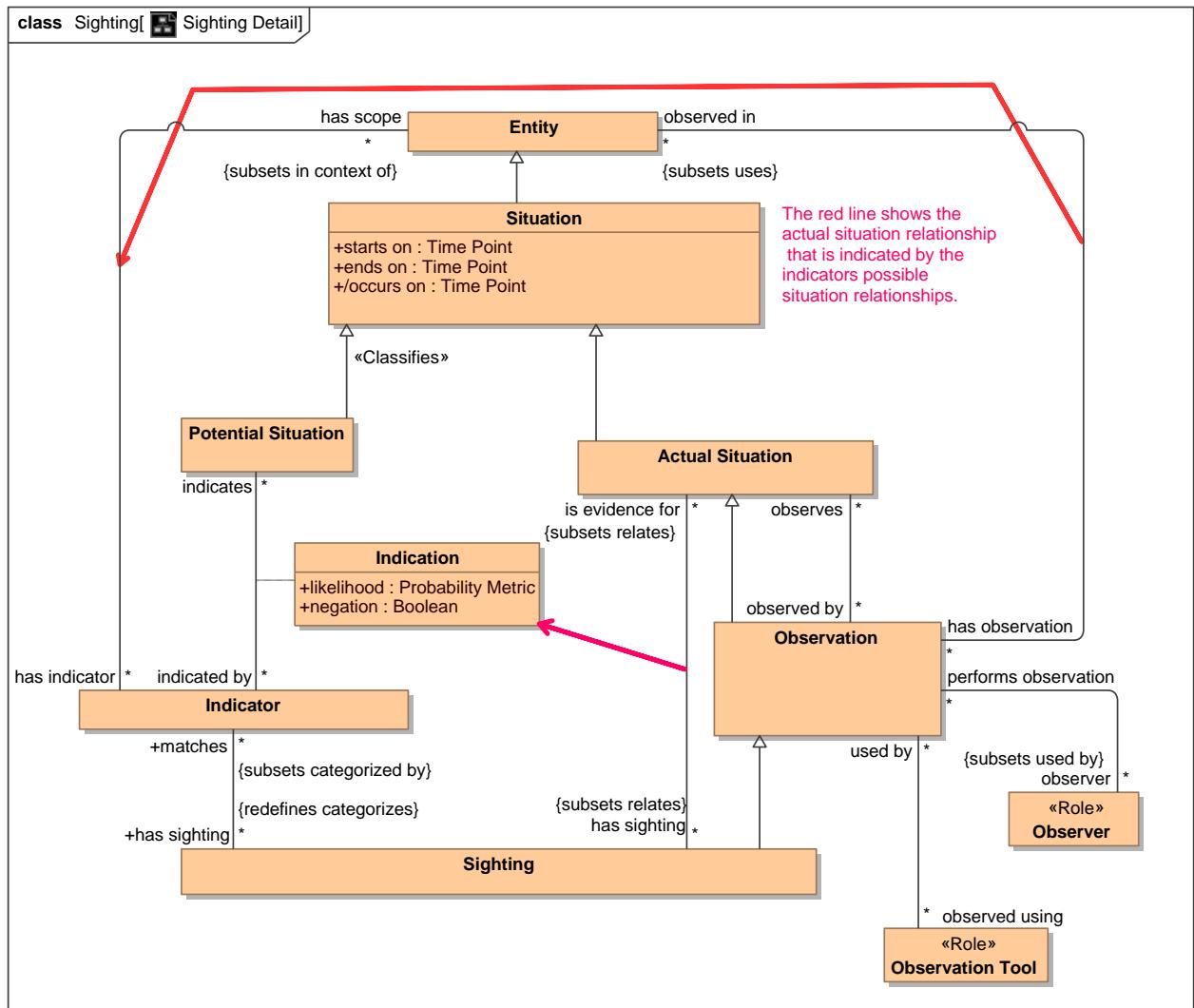
### **8.47.72 Associations**

 [watches](#) : [Entity](#) [\*] [Subsets](#): [relates](#):[Anything](#)

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

## **8.47.8 Class Sighting**

An actual sighting that may match an indicator - a sighting is evidence for some situation. The sighting observes the entity or situation of interest. It is observed in an actual situation that matches the "selected by" situation. The sighting is evidence for an actual situation that the indicator indicates.



**Figure 69. Sighting Detail**

#### 8.47.81 Direct Supertypes

[Observation](#)

**package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators**

#### 8.47.82 Associations

/ matches : [Indicator](#) [\*] Subsets: categorized by:[Category](#)

Indicators a sighting matches.

/ is evidence for : [Actual Situation](#) [\*] Subsets: relates:[Anything](#)

Situation that is indicated by a sighting.

## **8.47.9 Class Whitelist Indicator**

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

### 8.47.9.1 Direct Supertypes

[Indicator Watchlist](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators

## 8.48 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Kill Chains

A kill chain is a high level process definition for causing harm.

### 8.48.1 Diagram: Kill Chain

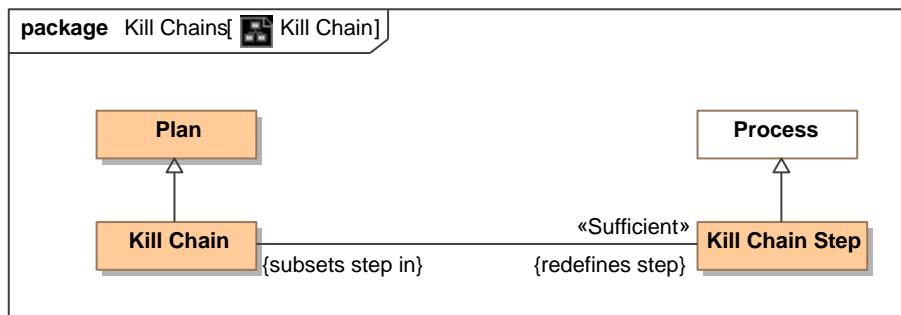


Figure 70. Kill Chain

### 8.48.2 Class Kill Chain

A kill chain is a high level process definition **for causing harm**. Kill chain generalizes specific processes that implement the kill chain.

#### 8.48.21 Direct Supertypes

[Plan](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Kill Chains

#### 8.48.22 Associations

: [Kill Chain Step](#) *Redefines:* step:[Occurrence](#)

### 8.48.3 Class Kill Chain Step

A step or phase in a kill chain. Kill chain steps generalizes specific processes that implement the kill chain.

#### 8.48.31 Direct Supertypes

[Process](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Kill Chains

### 8.48.32 Associations

 : [Kill Chain](#) Subsets: step in:[Occurrence](#)

## 8.49 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments

Mitigations lessen the likelihood or impact of undesirable situations.

### 8.49.1 Diagram: Risk Treatment

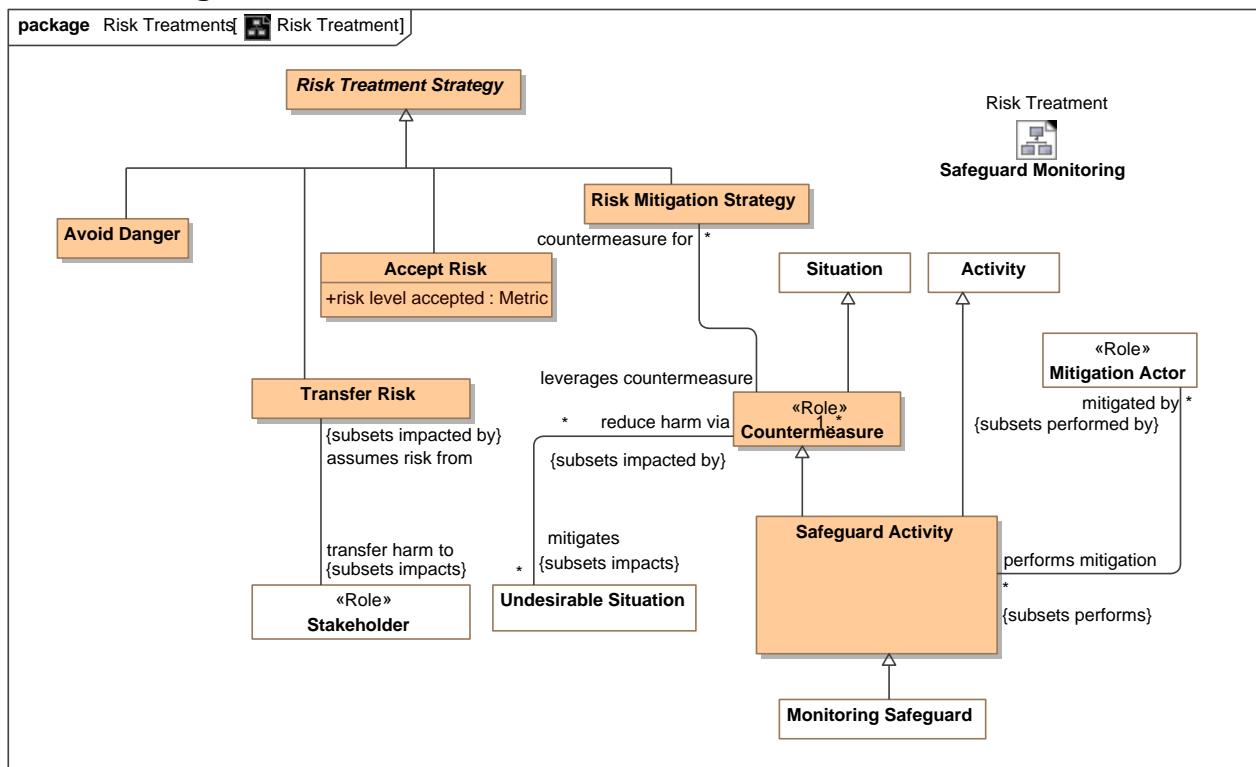


Figure 71. Risk Treatment

## 8.49.2 Diagram: Safeguard Monitoring

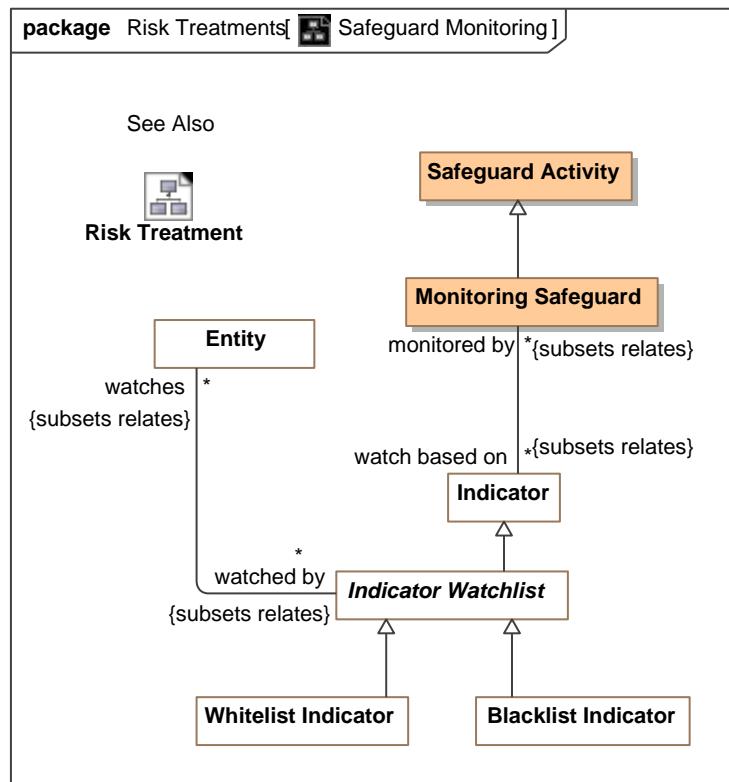


Figure 72. Safeguard Monitoring

## 8.49.3 Class Avoid Danger

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

### 8.49.31 Direct Supertypes

[Risk Treatment Strategy](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments

## 8.49.4 Class Countermeasure

Anything that protects a resource.

### 8.49.41 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments

#### 8.49.42 Associations

/ protects : [Resource](#) [\*] Subsets: supports:[Resource](#)

Resource protected by a safeguard.

/ mitigates : [Undesirable Situation](#) [\*] Subsets: impacts:[Entity](#)

Danger that a mitigation responds to.

/ countermeasure for : [Risk Mitigation Strategy](#) [\*] Subsets: required to perform:[Process](#)

Strategy a countermeasure serves.

#### 8.49.5 Class Mitigation Actor

One who performs a mitigation.

#### 8.49.51 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments

#### 8.49.52 Associations

/ performs mitigation : [Safeguard Activity](#) [\*] Subsets: performs:[Occurrence](#)

The mitigation an actor performs.

#### 8.49.6 Class Monitoring Safeguard

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

#### 8.49.61 Direct Supertypes

[Safeguard Activity](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments

#### 8.49.62 Associations

/ watch based on : [Indicator](#) [\*] Subsets: relates:[Anything](#)

Indicators watched for

#### 8.49.7 Class Risk Treatment Strategy

A strategy for dealing with risk.

#### 8.49.71 Direct Supertypes

[Policy](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments

### 8.49.72 Attributes

 degree of modification : [Metric](#)

A metric for how much a mitigation mitigates a dangerous situation.

### 8.49.73 Associations

 modifies risk : [Risk](#) [\*]

Risk that a mitigation reduces.

 imposed by : [Risk Owner](#) [\*] Subsets: asserted by:[Authority](#)

Authority that imposes a risk strategy.

## 8.49.8 Class Safeguard Activity

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

### 8.49.81 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments

### 8.49.82 Associations

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

The actor(s) that may perform a mitigation.

## 8.49.9 Class Transfer Risk

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

### 8.49.91 Direct Supertypes

[Risk Treatment Strategy](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments

### 8.49.92 Associations

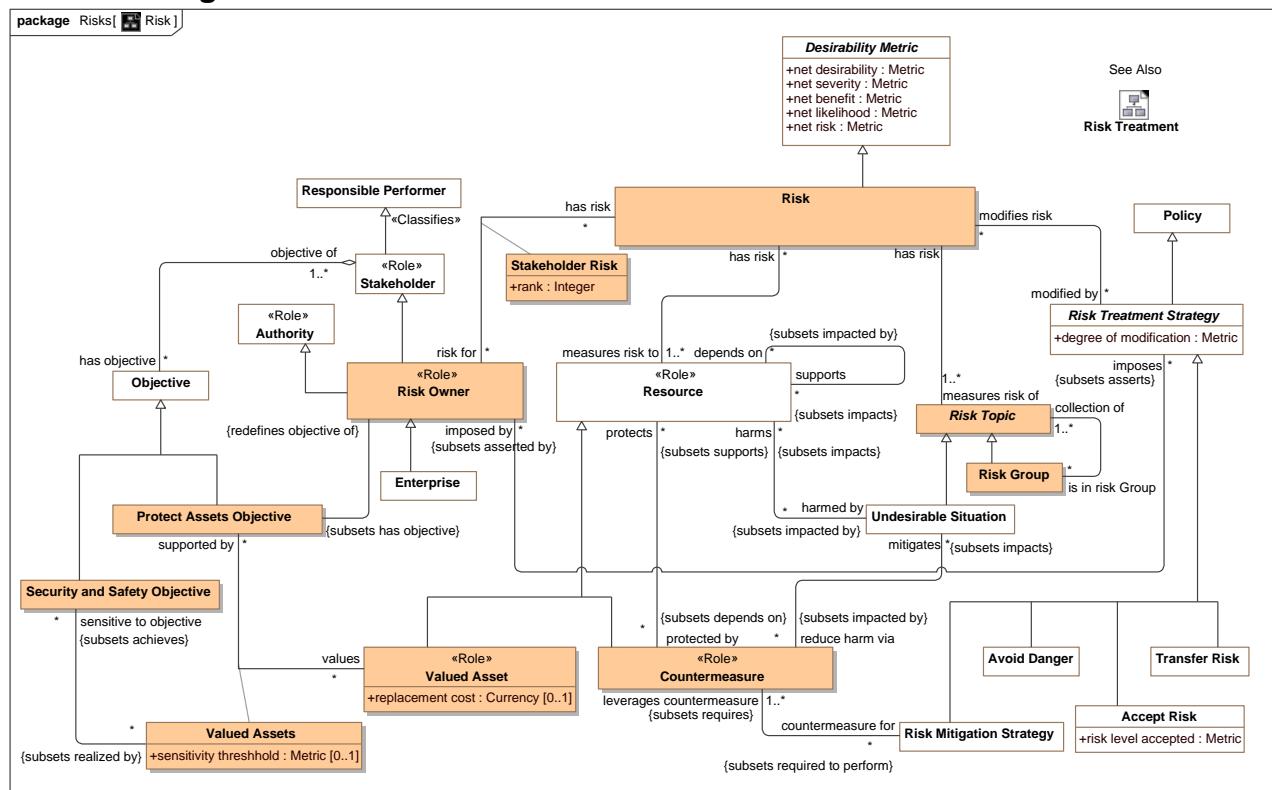
 transfer harm to : [Stakeholder](#) Subsets: impacts:[Entity](#)

Stakeholder that assumes a risk.

## **8.50 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks**

## Concepts relative to risk and risk analytics.

## 8.50.1 Diagram: Risk



**Figure 73.** Risk

## 8.50.2 Diagram: Risk Metrics

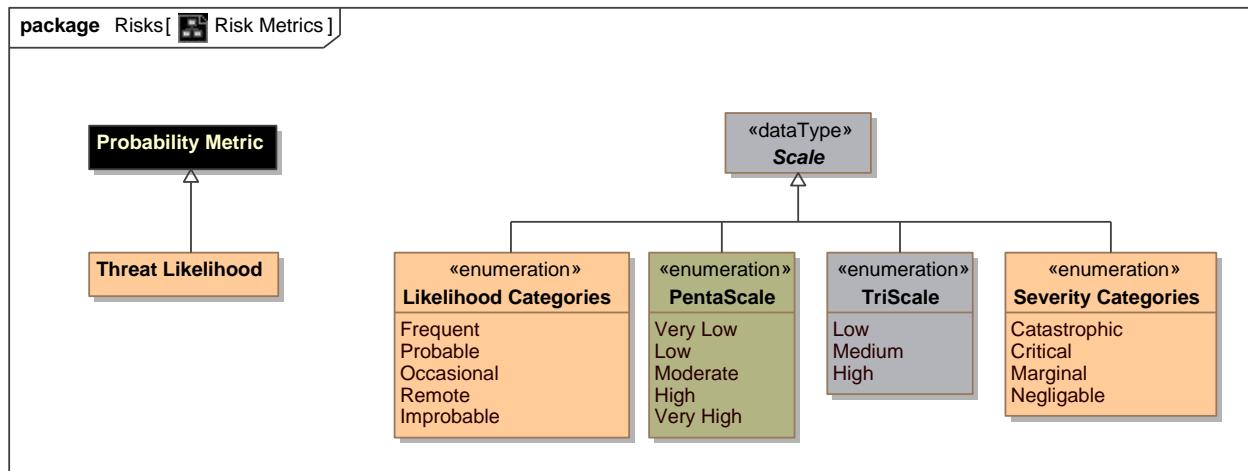


Figure 74. Risk Metrics

## 8.50.3 Class Accept Risk

A strategy to accept risk.

### 8.50.31 Direct Supertypes

[Risk Treatment Strategy](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

### 8.50.32 Attributes

risk level accepted : [Metric](#)

As a way to treat risk, the level of acceptable risk.

## 8.50.4 Class Protect Assets Objective

Objective to protect an asset.

### 8.50.41 Direct Supertypes

[Objective](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

### 8.50.42 Associations

values : [Valued Asset](#) [\*] Subsets: relates:[Anything](#)

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

: [Risk Owner](#) Redefines: objective of:[Stakeholder](#)

## **8.50.5 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 occurrence.

[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.]

### **8.50.51 Direct Supertypes**

[Desirability Metric](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

### **8.50.52 Associations**

 modified by : [Risk Treatment Strategy](#) [\*]

Mitigations that reduce a risk.

 measures risk of : [Risk Topic](#) [1..\*]

Undesirable situations measured by a risk.

 measures risk to : [Resource](#) [1..\*]

Resources (aka assets) at risk.

 risk for : [Risk Owner](#) [\*]

Owner of a risk.

## **8.50.6 Class Risk Group**

Multiple undesirable situations that are assessed together in terms of their risk.

### **8.50.61 Direct Supertypes**

[Risk Topic](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

### **8.50.62 Associations**

 collection of : [Risk Topic](#) [1..\*]

A component of a risk group.

## **8.50.7 Class Risk Mitigation Strategy**

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

### 8.50.71 Direct Supertypes

[Risk Treatment Strategy](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

### 8.50.72 Associations

 leverages countermeasure : [Countermeasure](#) [1..\*] Subsets: requires:[Resource](#)

Countermeasure which serves a risk mitigation strategy.

## 8.50.8 Class Risk Owner

A stakeholder with an objective to manage risk.

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

### 8.50.81 Direct Supertypes

[Authority](#), [Stakeholder](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

### 8.50.82 Associations

 : [Protect Assets Objective](#) Subsets: has objective:[Objective](#)

 has risk : [Risk](#) [\*]

Risk owned by a risk owner.

 imposes : [Risk Treatment Strategy](#) [\*] Subsets: asserts:[Policy](#)

Risk strategy imposed by a risk owner

## 8.50.9 Class Risk Topic

One or more undesirable situations that are assessed together in terms of their risk.

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

### 8.50.91 Associations

 has risk : [Risk](#)

Risk of a situation happening.

 is in risk Group : [Risk Group](#) [\*]

Group containing a risk topic.

## 8.50.10 Class Security and Safety Objective

Objective related to the safety and security of a stakeholder.

## 8.50.101 Direct Supertypes

[Objective](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

## 8.50.102 Associations

 : [Valued Assets](#) [\*] Subsets: realized by:[Means](#)

## 8.50.11 Association Class Stakeholder Risk

Risk owned by a risk owner.

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

## 8.50.111 Association Ends

 risk for : [Risk Owner](#) [\*] Subsets: realized by:[Means](#)

Owner of a risk.

 has risk : [Risk](#) [\*] Subsets: realized by:[Means](#)

Risk owned by a risk owner.

## 8.50.112 Attributes

 rank : [Integer](#)

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.

## 8.50.12 Class Threat Likelihood

### 8.50.121 Direct Supertypes

[Probability Metric](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

## 8.50.13 Class Valued Asset

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

### 8.50.131 Direct Supertypes

[Resource](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

### 8.50.132 Attributes

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

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

#### 8.50.133 Associations

 supported by : [Protect Assets Objective](#) [\*] Subsets: relates:[Anything](#)

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

### 8.50.14 Association Class Valued Assets

The set of assets directly important to stakeholders objectives.

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

#### 8.50.141 Association Ends

 values : [Valued Asset](#) [\*] Subsets: relates:[Anything](#)

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

 supported by : [Protect Assets Objective](#) [\*] Subsets: relates:[Anything](#)

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

#### 8.50.142 Attributes

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

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

#### 8.50.143 Associations

 sensitive to objective : [Security and Safety Objective](#) [\*] Subsets: achieves:[Objective](#)

Objectives that directly justify the valuing of specific assets.

#### 8.50.144 Enumeration Likelihood Categories

A high-level scale of likelihood.

#### 8.50.144 Direct Known Superclasses

[Scale](#)

package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks

public enum Likelihood Categories

{Frequent, Probable, Occasional, Remote, Improbable}

#### 8.50.144 Literals

 Frequent

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

 Probable

Will occur several times in the life of an item, with a probability of occurrence 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 occurrence 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 occurrence less than 10:3 but greater than 10:6 in that life.

 Improbable

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

### 8.50.145 Enumeration Severity Categories

A high-level scale of severity.

#### 8.50.145 Direct Known Superclasses

Scale

```
package Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risks
```

```
public enum Severity Categories
```

```
{Catastrophic, Critical, Marginal, Negligible}
```

#### 8.50.145 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 mitigatable 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.

#### 8.50.146 Known other enumerations

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

## 8.51 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Threats

Threat is a real situation that increases the likelihood of one or more related incidents.

### 8.51.1 Diagram: Threat

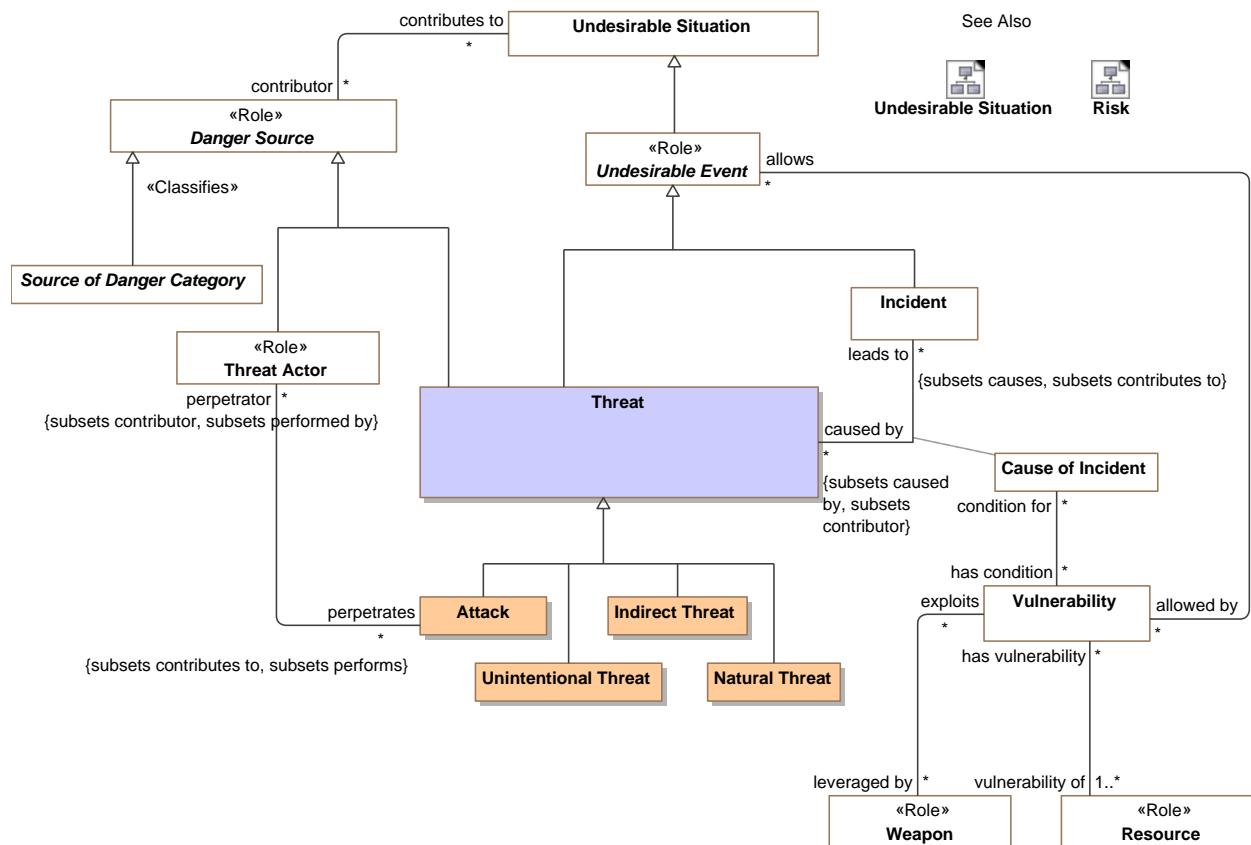


Figure 75. Threat

### 8.51.2 Class Threat

A threat is 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].

### 8.51.21 Direct Supertypes

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

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Threats

### 8.51.22 Associations

 leads to : [Incident](#) [\*] Subsets: contributes to:[Undesirable Situation](#) causes:[Situation](#)

Incident that is the result of a threat.

## **8.52 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.

## 8.52.1 Diagram: Undesirable Situation

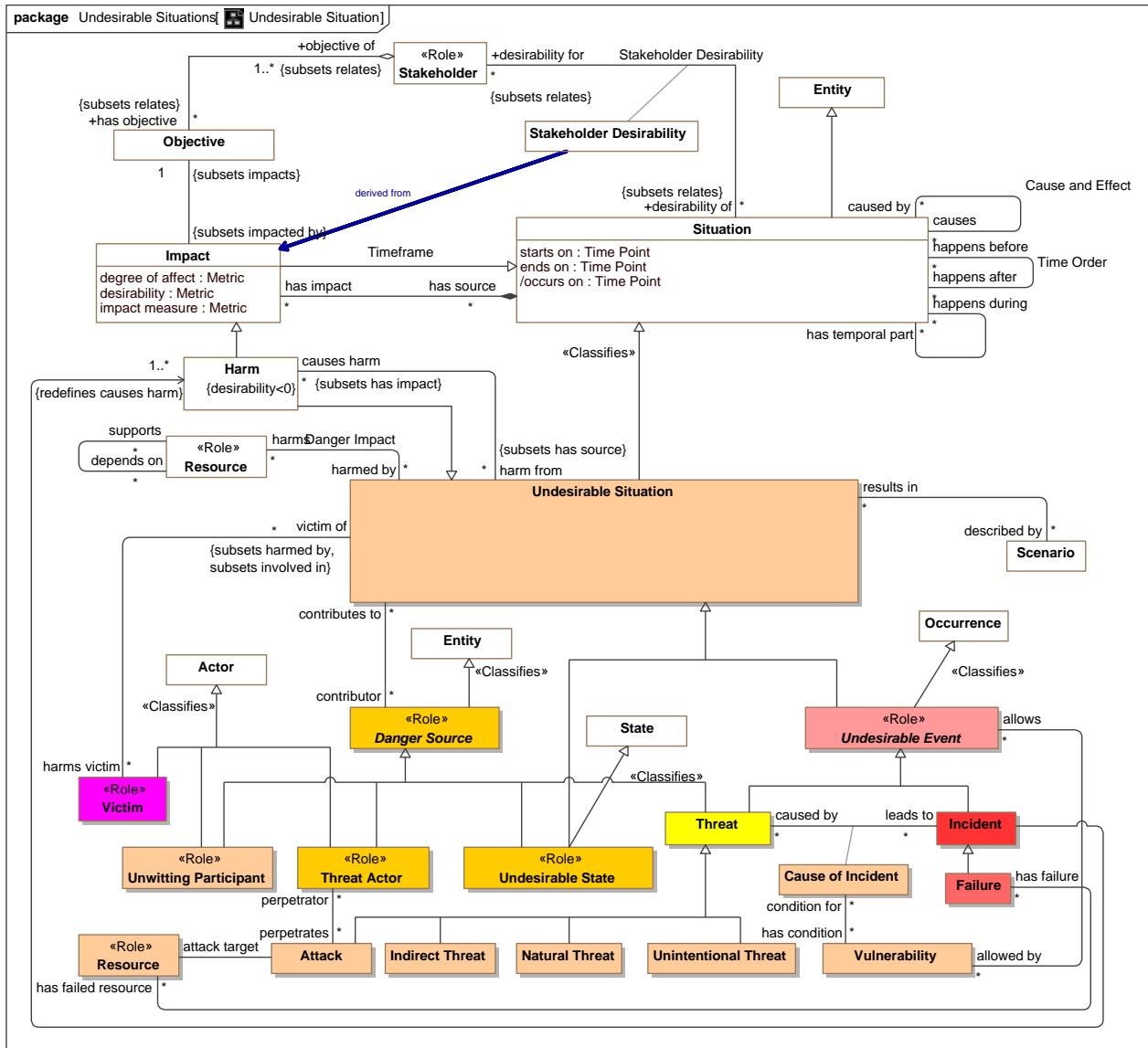


Figure 76. Undesirable Situation

## 8.52.2 Class Attack

A dangerous activity to make use of and derive benefit from a vulnerability.

### 8.52.21 Direct Supertypes

[Threat](#)

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

## 8.52.22 Associations

/ attack target : [Resource](#)

A resource intended to be harmed by an attack.

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

The threat actor performing an activity to cause or contribute to a dangerous situation in a real or possible world.

## 8.52.3 Association Danger Impact

An impact of a danger on a resource.

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

### 8.52.31 Association Ends

/ harms : [Resource](#) [\*] Subsets: performed by:[Actor](#) contributor:[Danger Source](#)

Anything damaged by a undesirable situation.

/ harmed by : [Undesirable Situation](#) [\*] Subsets: performed by:[Actor](#) contributor:[Danger Source](#)

Danger that damages anything.

/ likelihood : [Probability Metric](#) Subsets: performed by:[Actor](#) contributor:[Danger Source](#)

Possibility of the impact occurring.

## 8.52.4 Class Indirect Threat

A threat that does directly lead to an incident.

### 8.52.41 Direct Supertypes

[Threat](#)

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

## 8.52.5 Class Natural Threat

A threat from natural means.

### 8.52.51 Direct Supertypes

[Threat](#)

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

## 8.52.6 Class Undesirable Event

Anything that happens that does or may directly or indirectly cause harm.

## 8.52.61 Direct Supertypes

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

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

## 8.52.62 Associations

 allowed by : [Vulnerability](#) [\*]

Vulnerabilities that an event depends on or exploits.

## 8.52.7 Class Undesirable Situation

An undesirable situation is any condition or event that has, is, or may cause harm (directly or indirectly). Undesirable situations negatively impact the objectives of stakeholders. An undesirable situation is classified in the context of the impacted stakeholders.

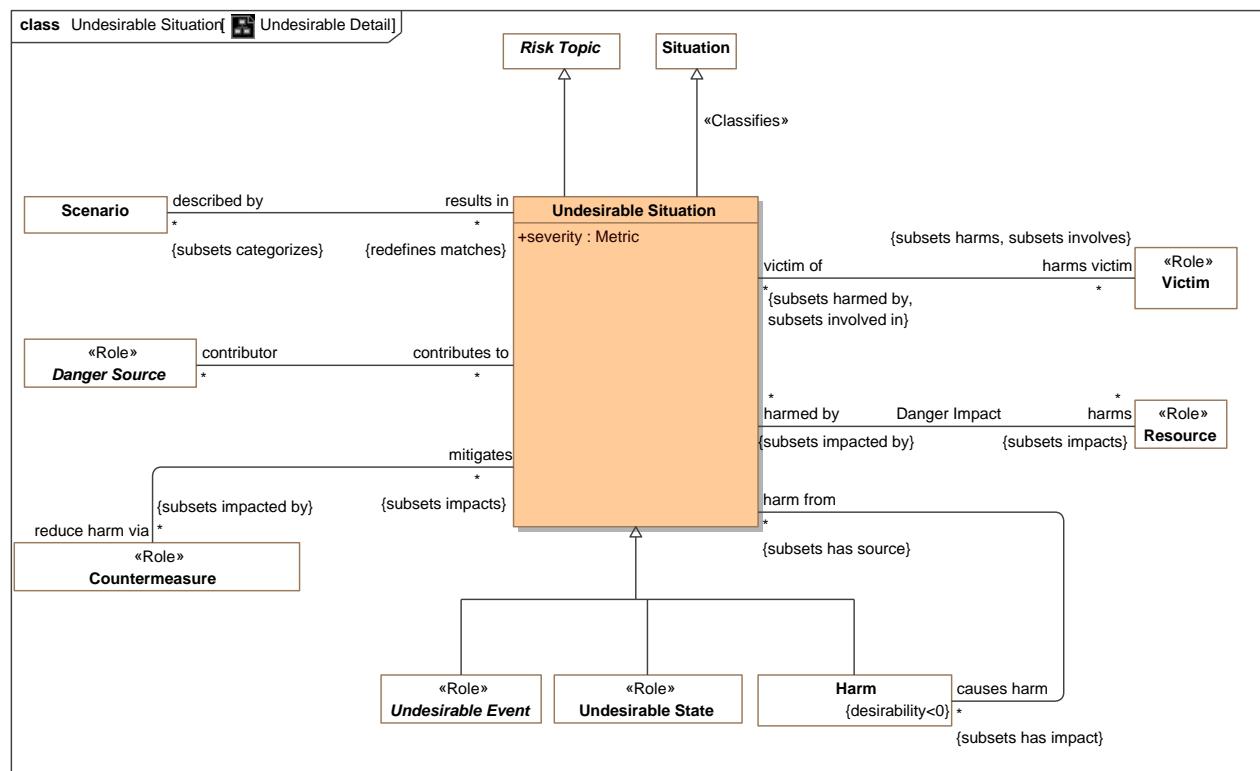


Figure 77. Undesirable Detail

## 8.52.71 Direct Supertypes

[Risk Topic](#), [Situation](#)

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

## 8.52.72 Attributes

 severity : [Metric](#)

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

### 8.52.73 Associations

/ reduce harm via : [Countermeasure](#) [\*] Subsets: impacted by:[Entity](#)

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

/ described by : [Scenario](#) [\*] Subsets: categorizes:[Situation](#)

A scenario that typifies a danger.

/ contributor : [Probability Metric](#)

Anything that can contribute to an undesired condition.

/ harms : [Probability Metric](#)

Anything damaged by a undesirable situation.

/ harms victim : [Victim](#) [\*] Subsets: harms:[Resource](#) involves:[Actor](#)

Victim harmed by a situation.

/ causes harm : [Harm](#) [\*] Subsets: has impact:[Impact](#)

The harm to a resource caused by a undesirable situation.

### 8.52.8 Class Undesirable State

A dangerous condition is a static situation (not something happening) that directly or indirectly does or may have detrimental consequences impacting the objectives of stakeholders.

#### 8.52.81 Direct Supertypes

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

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

### 8.52.9 Class Unintentional Threat

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

#### 8.52.91 Direct Supertypes

[Threat](#)

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

### 8.52.10 Class Unwitting Participant

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

#### 8.52.101 Direct Supertypes

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

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

### **8.52.11 Class Victim**

The role of any actor harmed by an incident.

#### 8.52.111 Direct Supertypes

[Actor](#), [Valued Asset](#)

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

#### 8.52.112 Associations

 victim of : [Undesirable Situation](#) [\*] Subsets: harmed by:[Undesirable Situation](#) involved in:[Situation](#)

Situations of which an actor is a victim.

## 8.53 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.

### 8.53.1 Diagram: Cyber Vulnerability

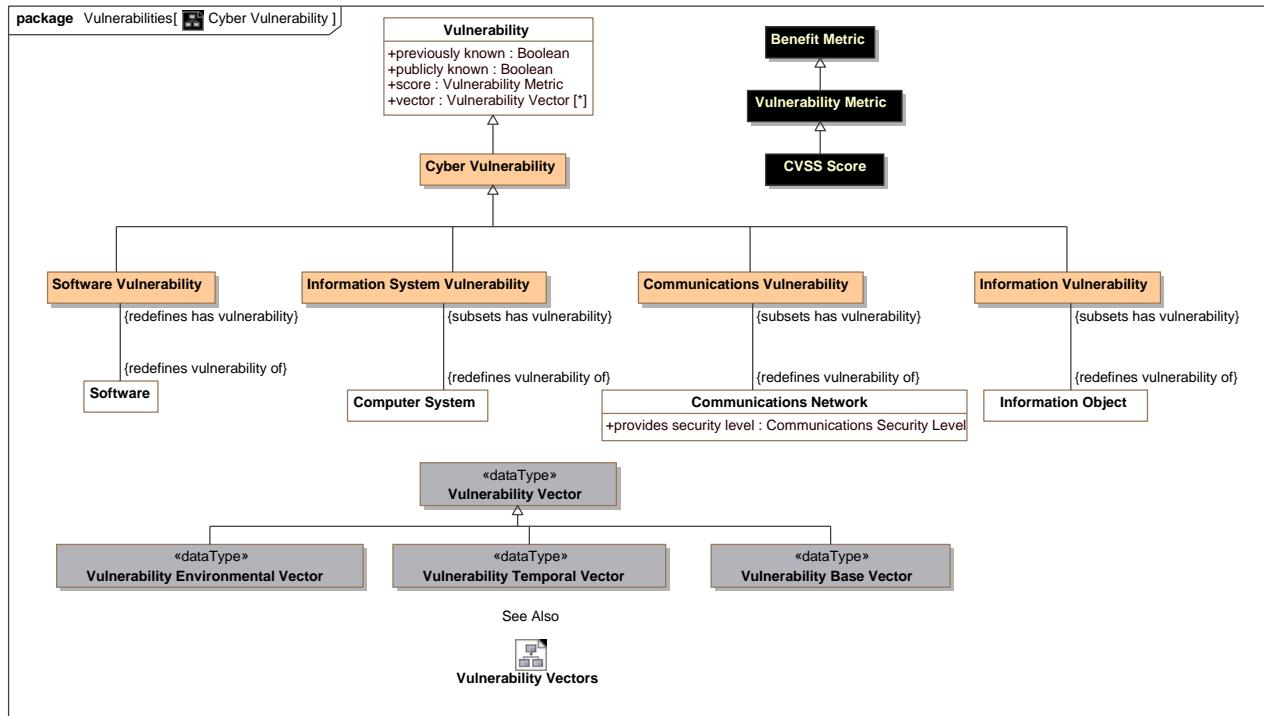


Figure 78. Cyber Vulnerability

## 8.53.2 Diagram: Vulnerability

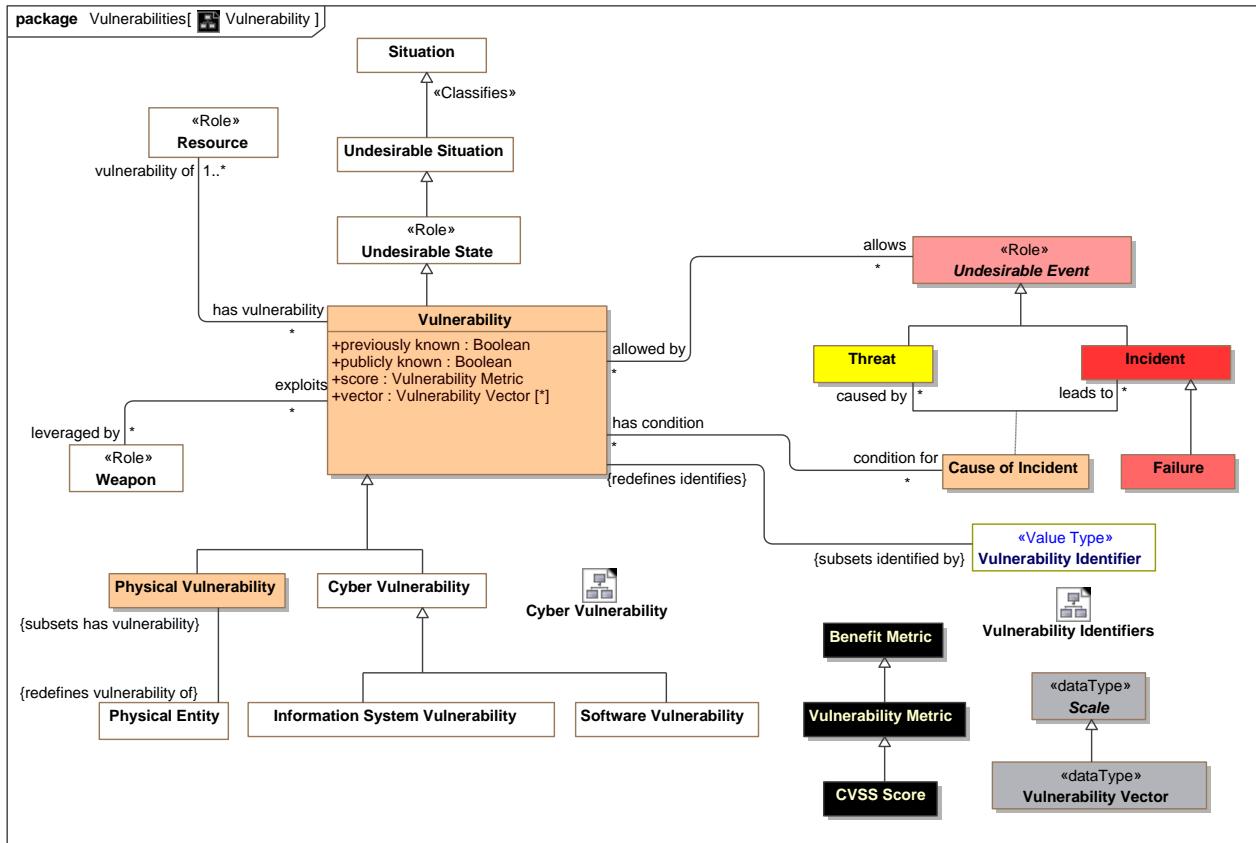


Figure 79. Vulnerability

### 8.53.3 Diagram: Vulnerability Identifiers

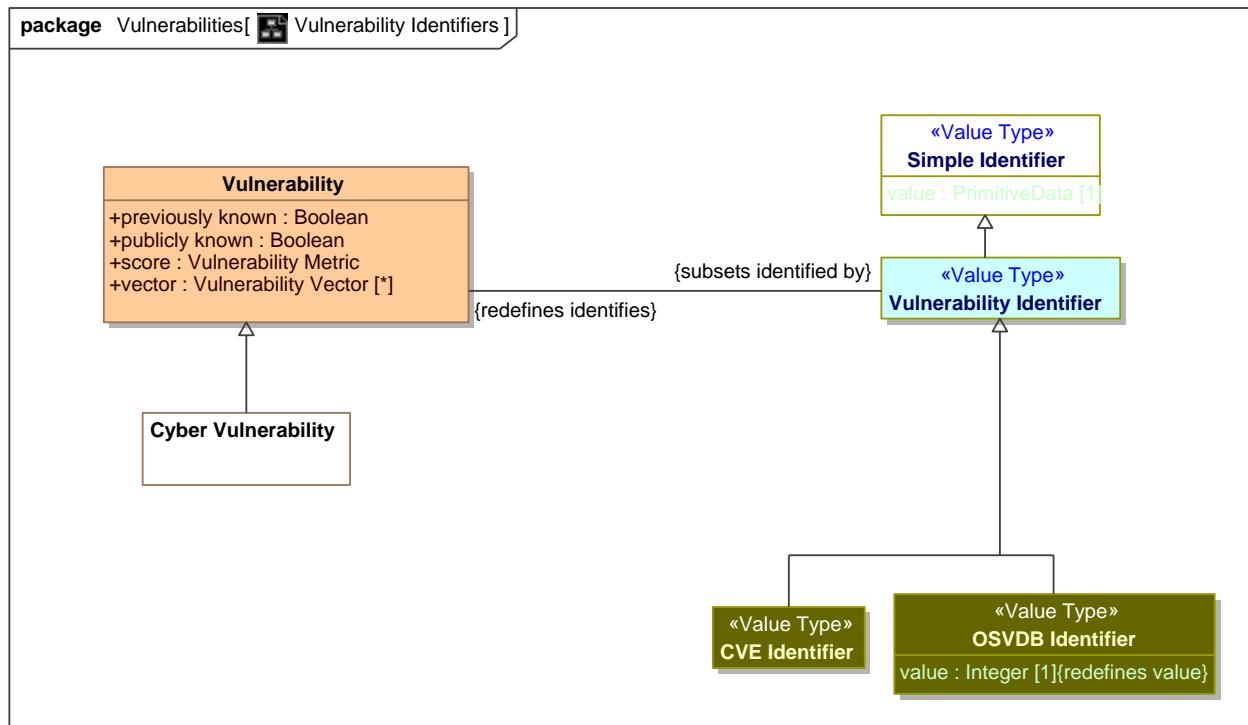


Figure 80. Vulnerability Identifiers

### 8.53.4 Class Communications Vulnerability

#### 8.53.4.1 Direct Supertypes

[Cyber Vulnerability](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

#### 8.53.4.2 Associations

/ : [Communications Network](#) Redefines: vulnerability of:[Resource](#)

### 8.53.5 Class CVE Identifier

An identifier for Common Vulnerabilities and Exposures.

#### 8.53.5.1 Direct Supertypes

[Vulnerability Identifier](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

## **8.53.6 Class Cyber Vulnerability**

A vulnerability of any cyber related resource.

### 8.53.6.1 Direct Supertypes

Vulnerability

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

## **8.53.7 Class Information System Vulnerability**

Vulnerability of a computer system and/or its network.

### 8.53.7.1 Direct Supertypes

Cyber Vulnerability

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

### 8.53.7.2 Associations

 : Computer System Redefines: vulnerability of:Resource

## **8.53.8 Class Information Vulnerability**

Vulnerability of information loss, misuse or corruption.

### 8.53.8.1 Direct Supertypes

Cyber Vulnerability

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

### 8.53.8.2 Associations

 : Information Object Redefines: vulnerability of:Resource

## **8.53.9 Class OSVDB Identifier**

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

### 8.53.9.1 Direct Supertypes

Vulnerability Identifier

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

### 8.53.9.2 Attributes

 value : Integer [1]

Index into the OSVDB database.

## **8.53.10 Class Physical Vulnerability**

Vulnerability of something to physical danger or attack.

### 8.53.101 Direct Supertypes

[Vulnerability](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

### 8.53.102 Associations

 : [Physical Entity](#) *Redefines:* vulnerability of: [Resource](#)

## **8.53.11 Class Software Vulnerability**

A vulnerability of software.

### 8.53.111 Direct Supertypes

[Cyber Vulnerability](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

### 8.53.112 Associations

 : [Software](#) *Redefines:* vulnerability of: [Resource](#)

## **8.53.12 Class Vulnerability**

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.

### 8.53.121 Direct Supertypes

[Undesirable State](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

### 8.53.122 Attributes

 previously known : [Boolean](#)

**At the time of** the vulnerability characterization, true if the vulnerability had been previously reported, false if newly discovered or "zero day".

 publicly known : [Boolean](#)

An indication that a vulnerability is **public** knowledge.

 score : [Vulnerability Metric](#)

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

vector : [Vulnerability Vector](#) [\*]

Factors influencing the vulnerability score.

### 8.53.123 Associations

vulnerability of : [Resource](#) [1..\*]

Resources a vulnerability may affect.

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

allows : [Undesirable Event](#) [\*]

Situations that a vulnerability allows to happen including attacks that may exploit the vulnerability.

condition for : [Cause of Incident](#) [\*]

Incident or failure for which a vulnerability is **a required** condition.

leveraged by : [Weapon](#) [\*]

**Weapon that a vulnerability is vulnerable to.**

### 8.53.13 Class Vulnerability Identifier

Any identifier for a vulnerability.

#### 8.53.131 Direct Supertypes

[Simple Identifier](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

#### 8.53.132 Associations

: [Vulnerability](#) Redefines: identifies:[Entity](#)

### 8.53.14 Class Vulnerability Metric

An overall score for a vulnerability.

#### 8.53.141 Direct Supertypes

[Benefit Metric](#)

**package** Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities

# 9 STIX Mapping Specification (Normative)

## 9.1 How STIX is represented

STIX 1.2 is represented as a **UML model imported from the STIX XML schema**. This model is in the machine readable artifacts as “Stix12.” Mappings are then made between UML models.

## 9.2 Generic NIEM Mapping Rules and Conventions

The mapping specification below specifies the semantic relationships between **NIEM** and the corresponding conceptual 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 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 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 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.

## 9.3 STIX Mapping to the threat/risk conceptual model

### 9.3.1 Diagram: High Level STIX Mapping

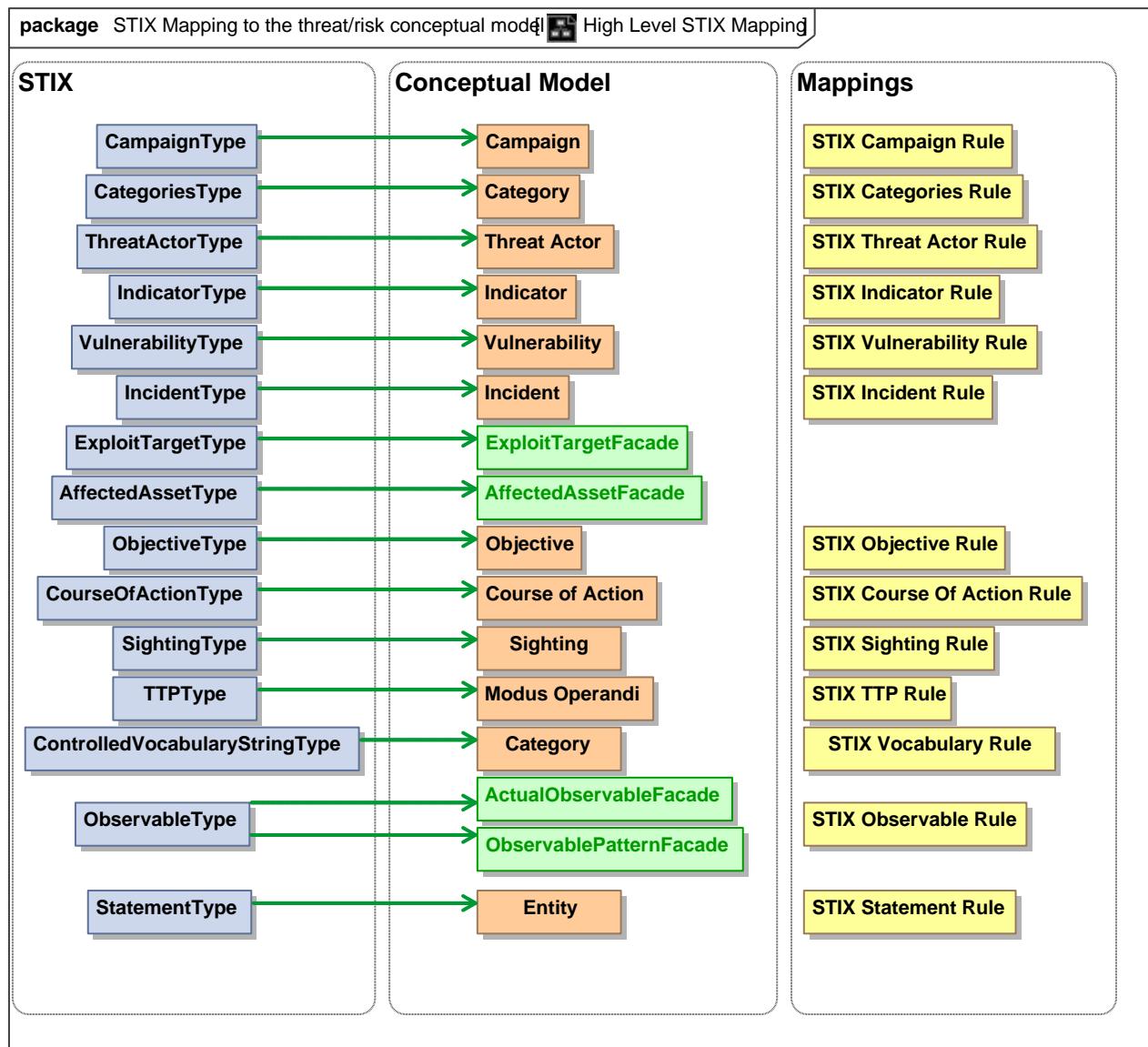


Figure 81. High Level STIX Mapping

## 9.4 STIX Mapping to the threat/risk conceptual model::Facades

### 9.4.1 Diagram: Facade Summary

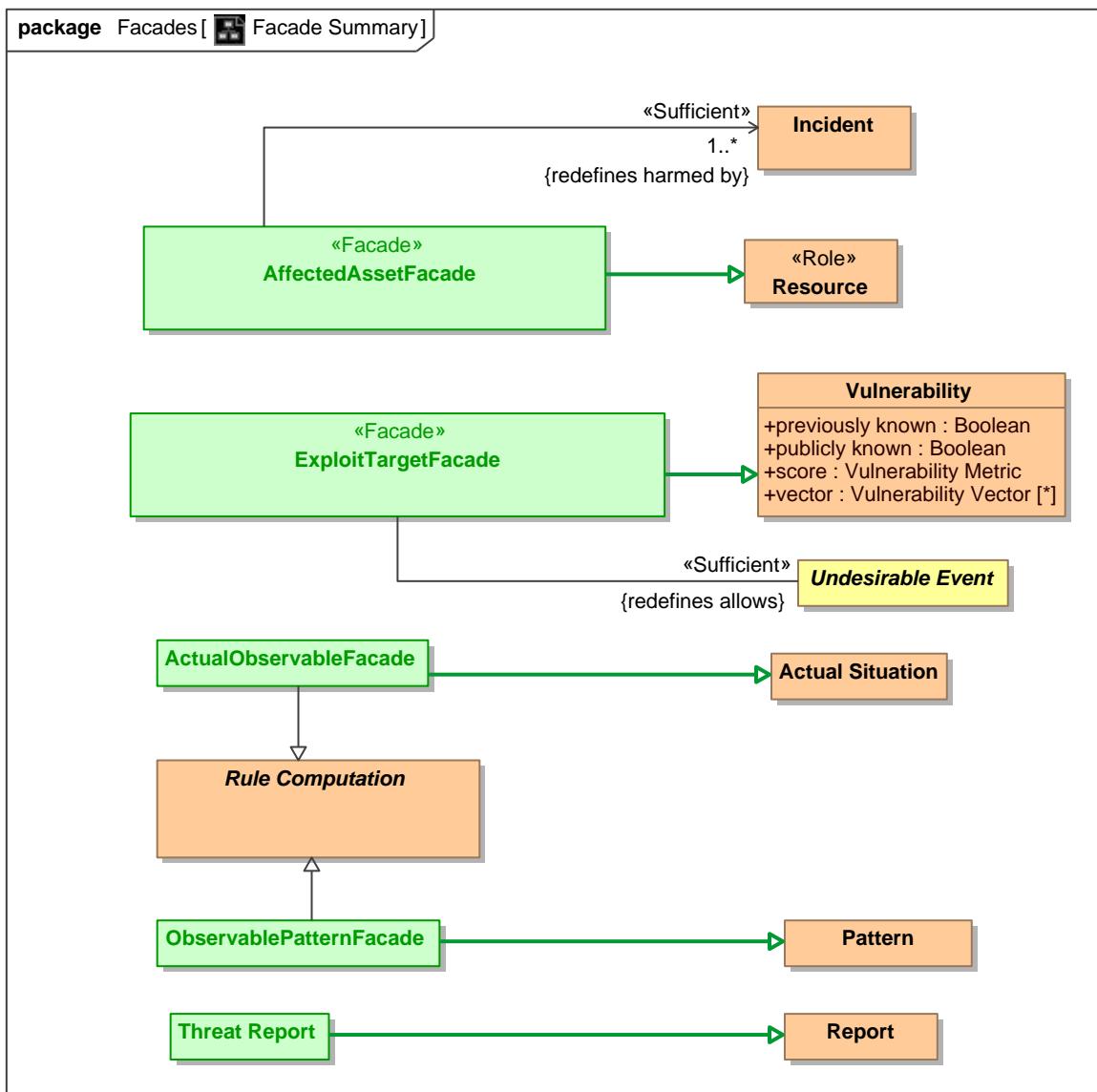


Figure 82. Facade Summary

### 9.4.2 Class ActualObservableFacade

Computation of an observable from an actual situation. This computation is done by the mapping implementation.

#### 9.4.21 Direct Supertypes

[Actual Situation](#), [Rule Computation](#)

**package** STIX Mapping to the threat/risk conceptual model::Facades

#### 9.4.3 Class AffectedAssetFacade

##### 9.4.31 Direct Supertypes

[Resource](#)

**package** STIX Mapping to the threat/risk conceptual model::Facades

##### 9.4.32 Associations

 : [Incident](#) [1..\*] *Redefines:* harmed by: [Undesirable Situation](#)

#### 9.4.4 Class ExploitTargetFacade

##### 9.4.41 Direct Supertypes

[Vulnerability](#)

**package** STIX Mapping to the threat/risk conceptual model::Facades

##### 9.4.42 Associations

 : [Undesirable Event](#) *Redefines:* allows: [Undesirable Event](#)

#### 9.4.5 Class ObservablePatternFacade

Computation of an observable from a situation pattern. This computation is done by the mapping implementation.

##### 9.4.51 Direct Supertypes

[Pattern](#), [Rule Computation](#)

**package** STIX Mapping to the threat/risk conceptual model::Facades

#### 9.4.6 Class Threat Report

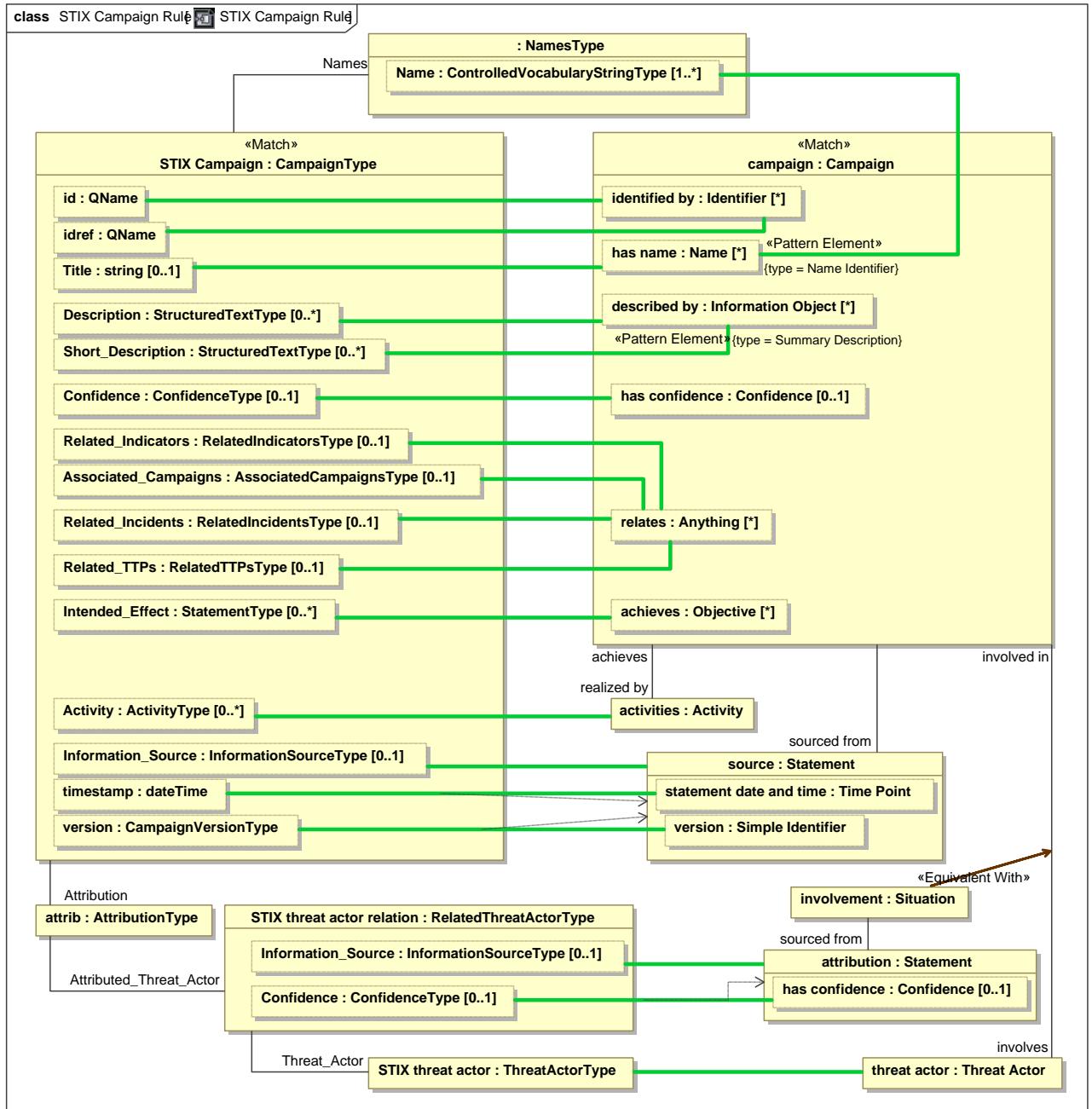
##### 9.4.61 Direct Supertypes

[Report](#)

**package** STIX Mapping to the threat/risk conceptual model::Facades

## 9.5 STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

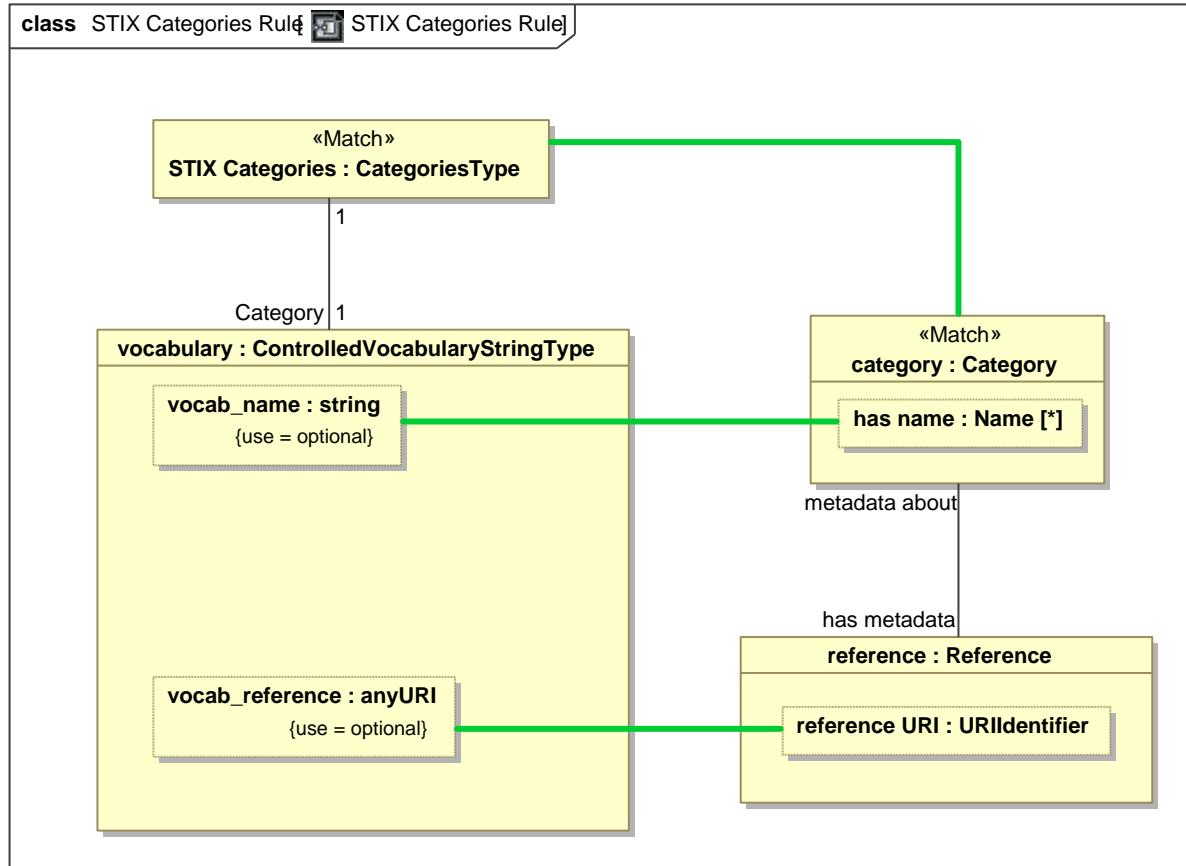
### 9.6 Class STIX Campaign Rule



**Figure 83. STIX Campaign Rule**

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.7 Class STIX Categories Rule



**Figure 84. STIX Categories Rule**

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.8 Class STIX Course Of Action Rule

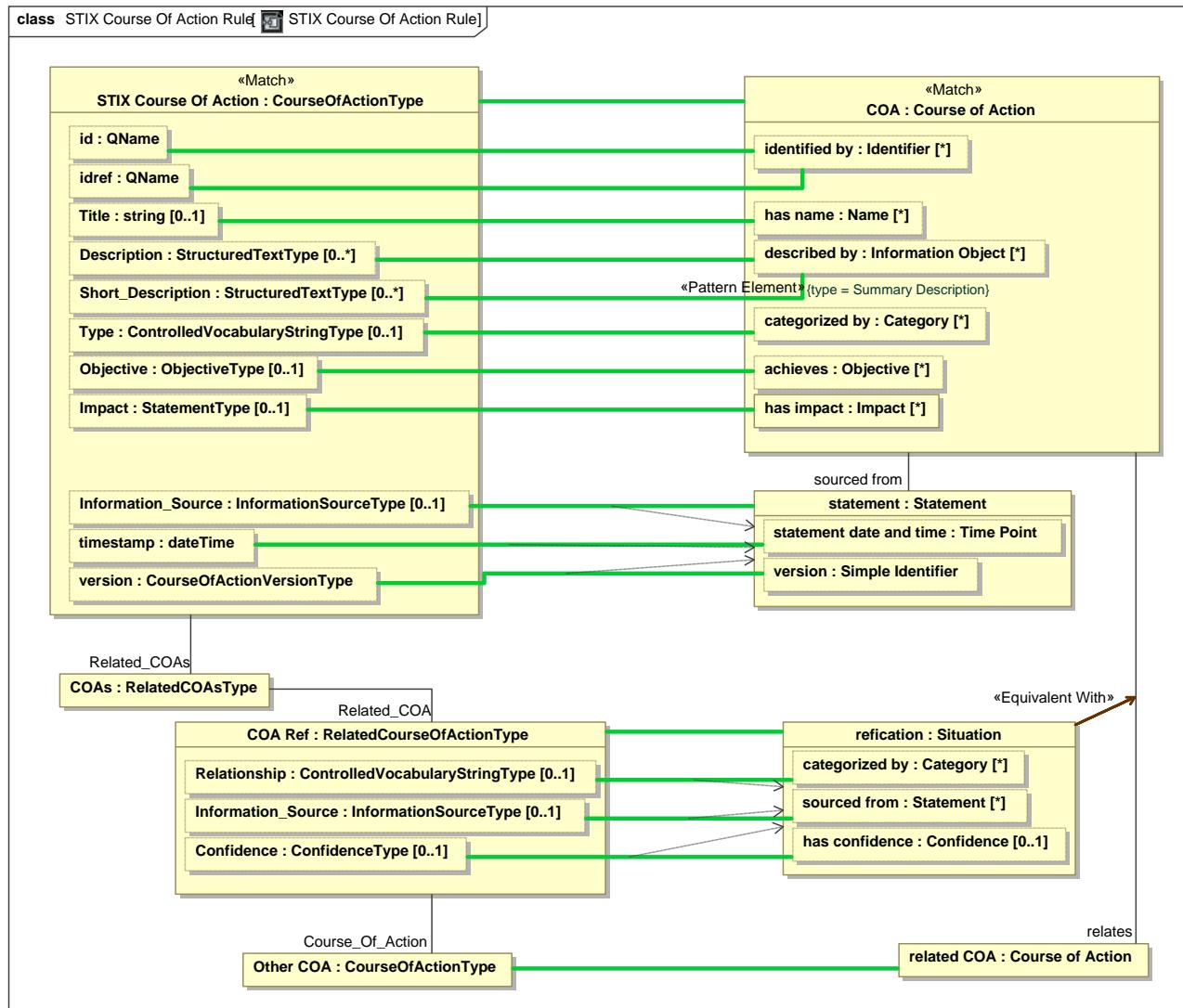


Figure 85. STIX Course Of Action Rule

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.9 Class STIX Incident Rule

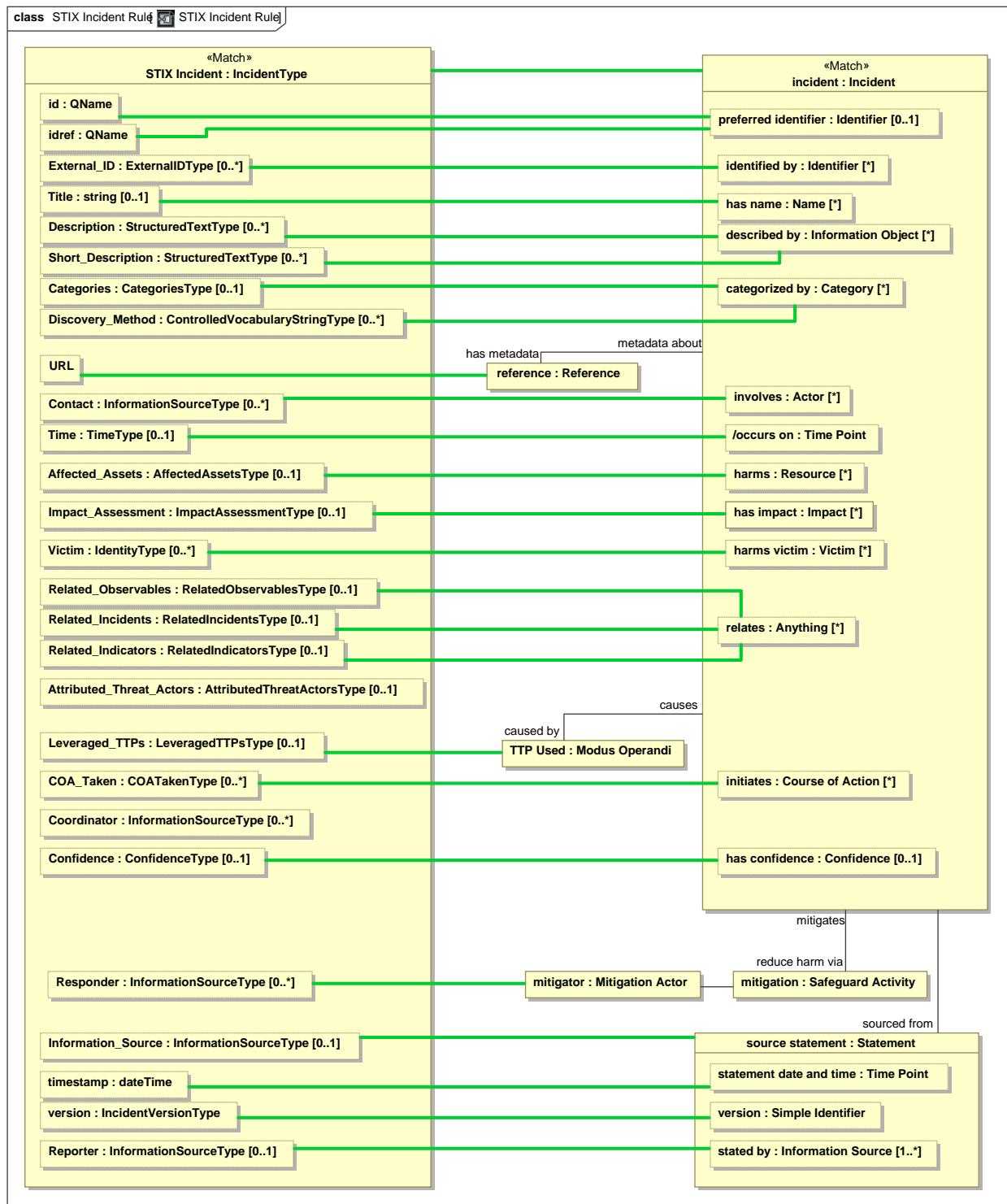


Figure 86. STIX Incident Rule

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.10 Class STIX Indicator Rule

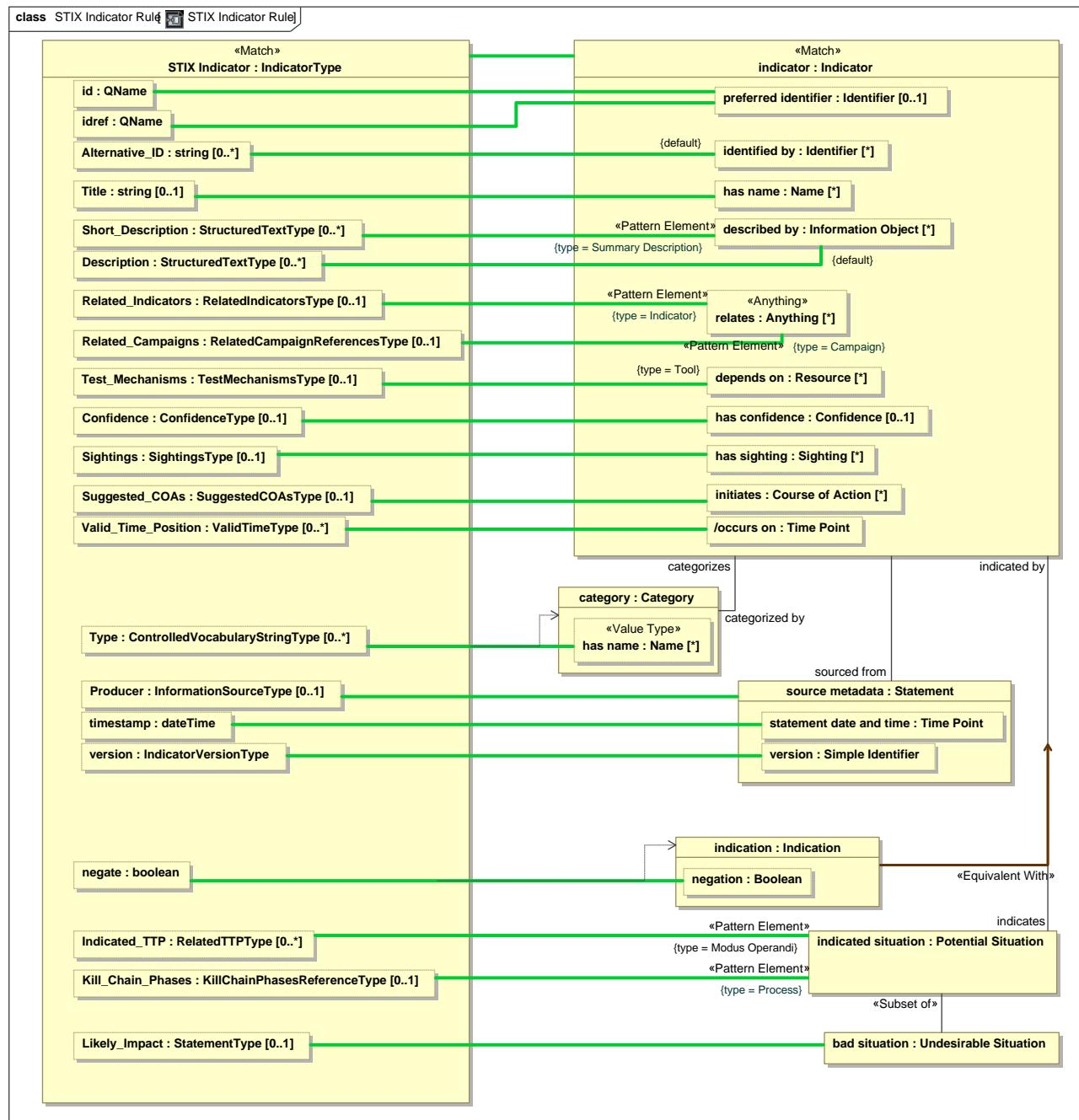
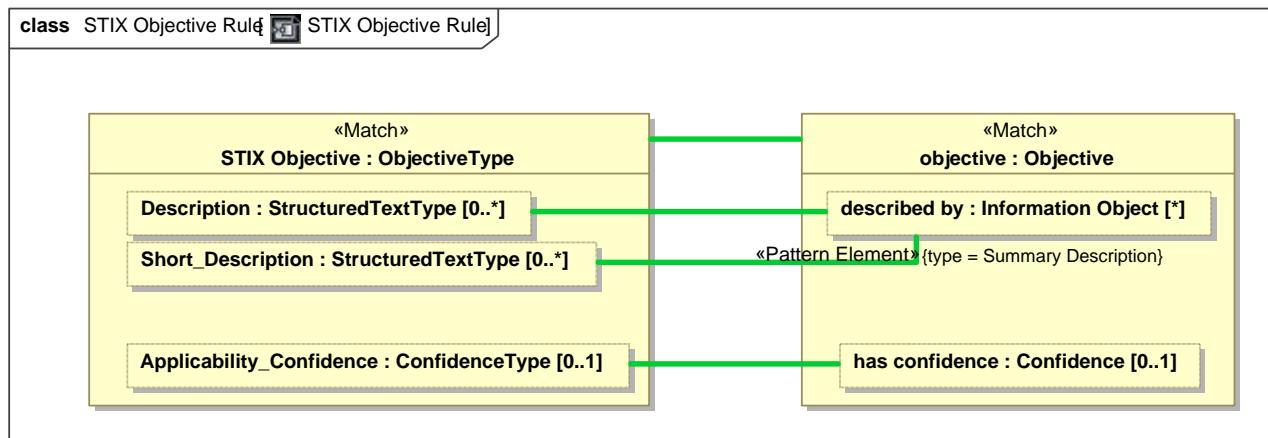


Figure 87. STIX Indicator Rule

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.11 Class STIX Objective Rule



**Figure 88. STIX Objective Rule**

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.12 Class STIX Observable Rule

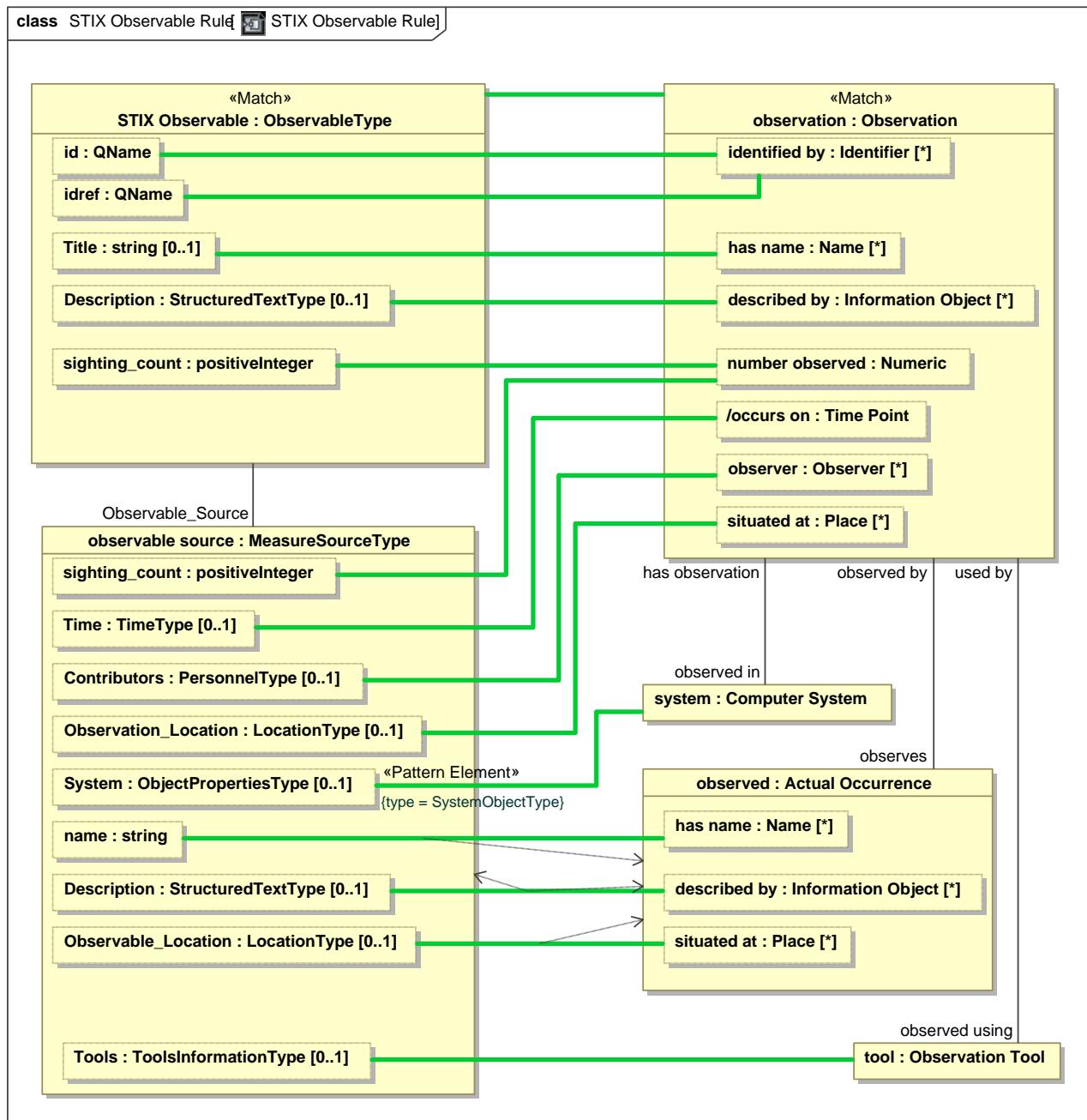


Figure 89. STIX Observable Rule

package STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.13 Class STIX Sighting Rule

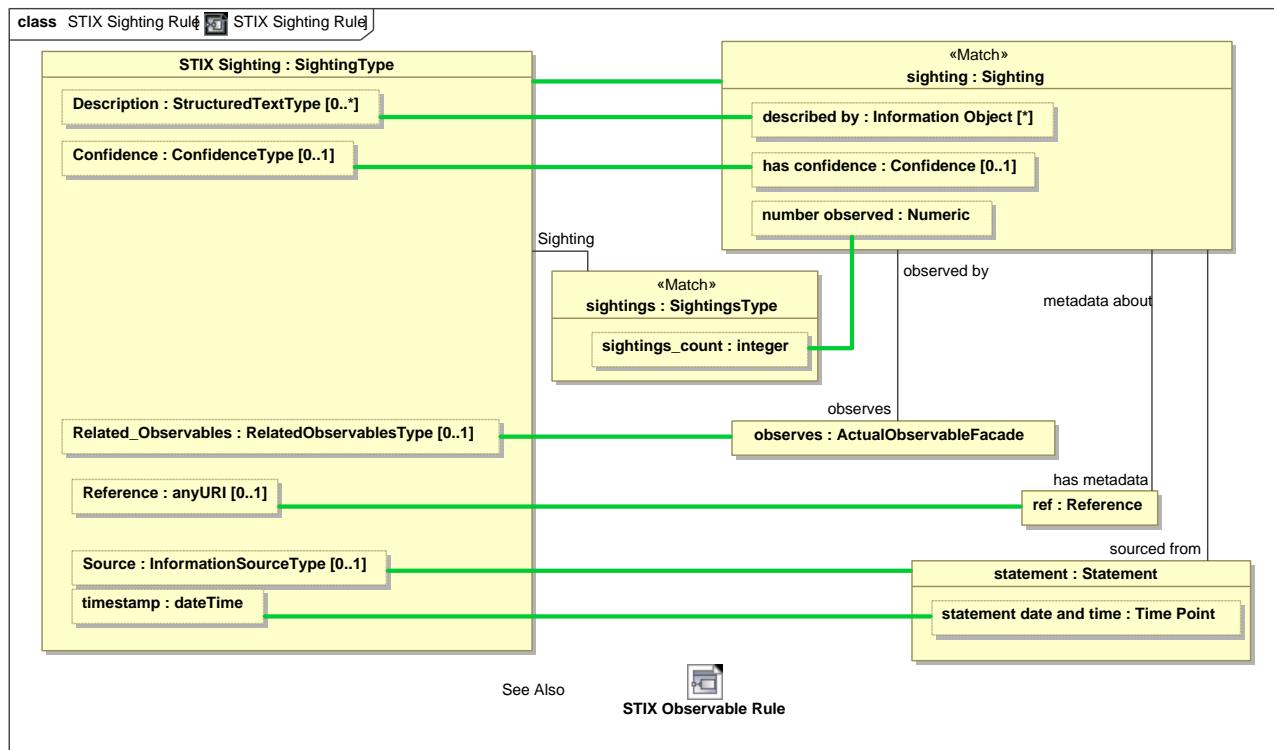


Figure 90. STIX Sighting Rule

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.14 Class STIX Statement Rule

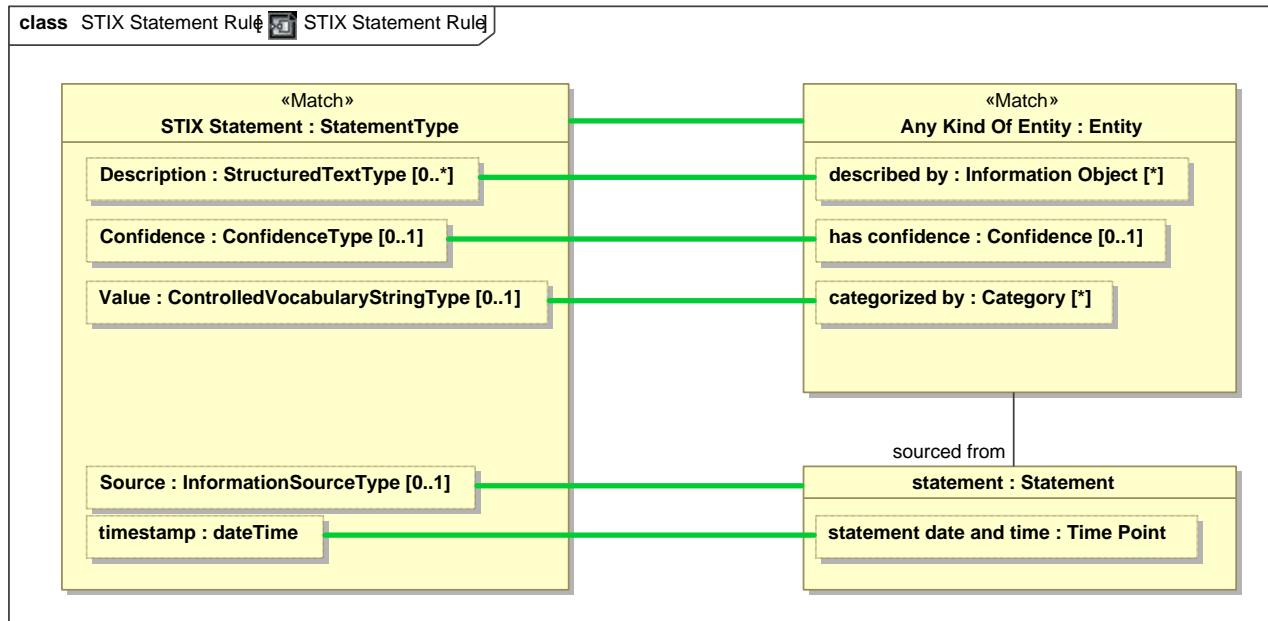


Figure 91. STIX Statement Rule

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.15 Class STIX Threat Actor Rule

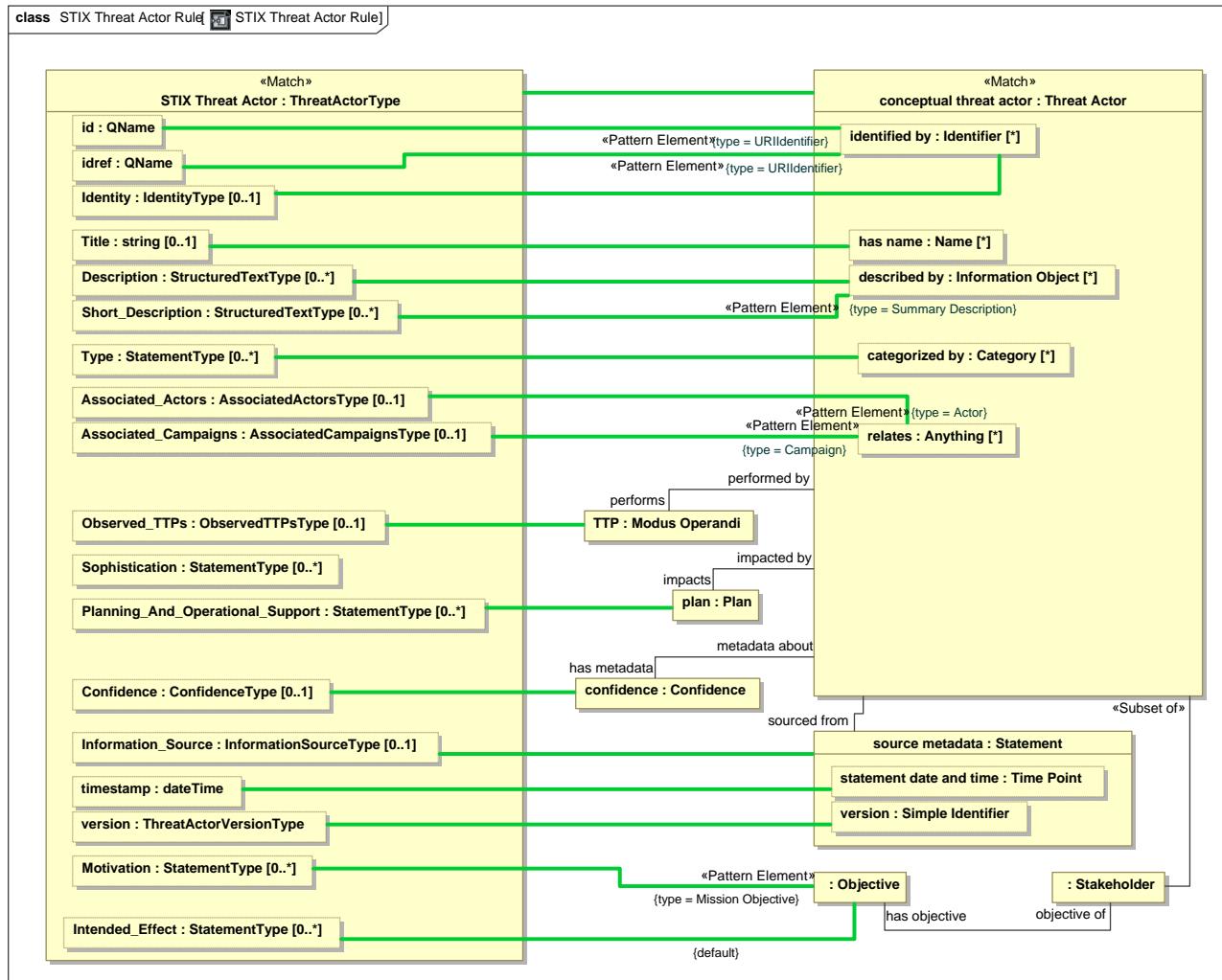


Figure 92. STIX Threat Actor Rule

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.16 Class STIX TTP Rule

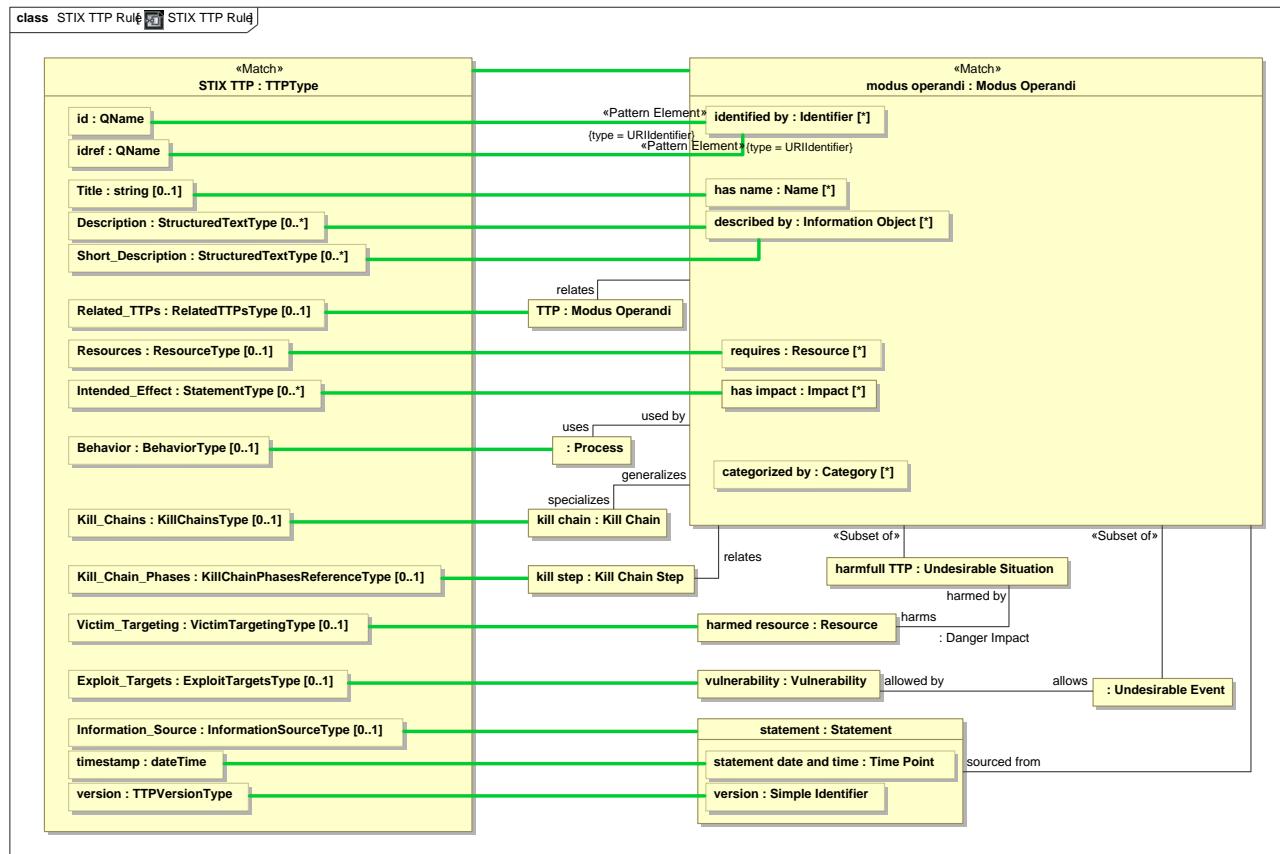


Figure 93. STIX TTP Rule

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.17 Class STIX Vocabulary Rule

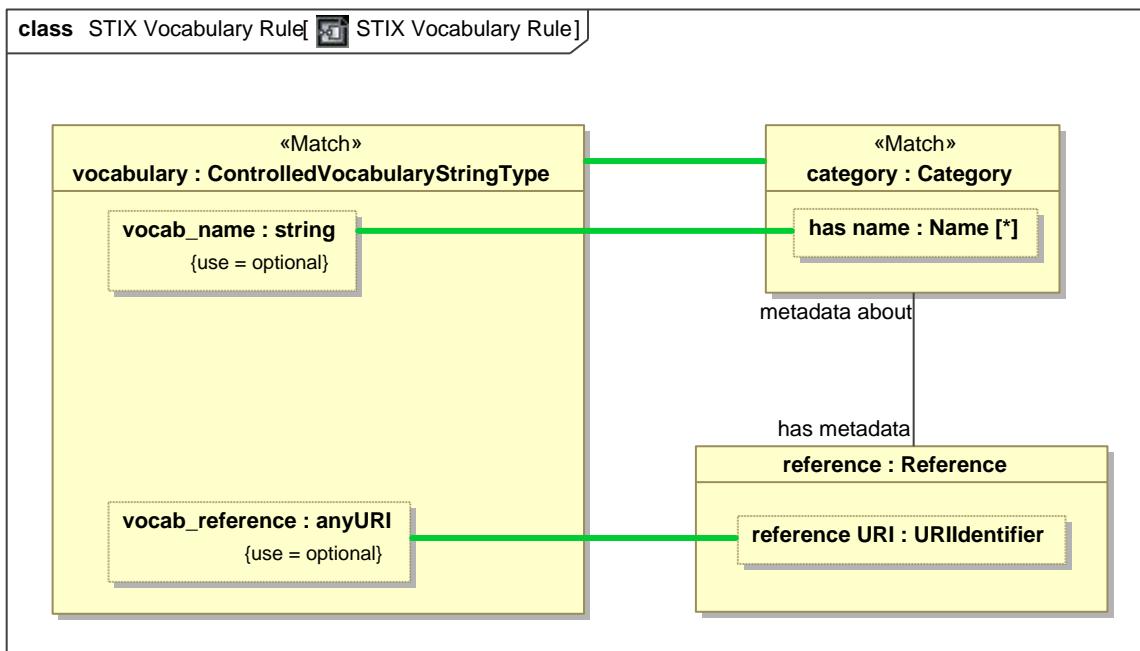


Figure 94. STIX Vocabulary Rule

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

## 9.18 Class STIX Vulnerability Rule

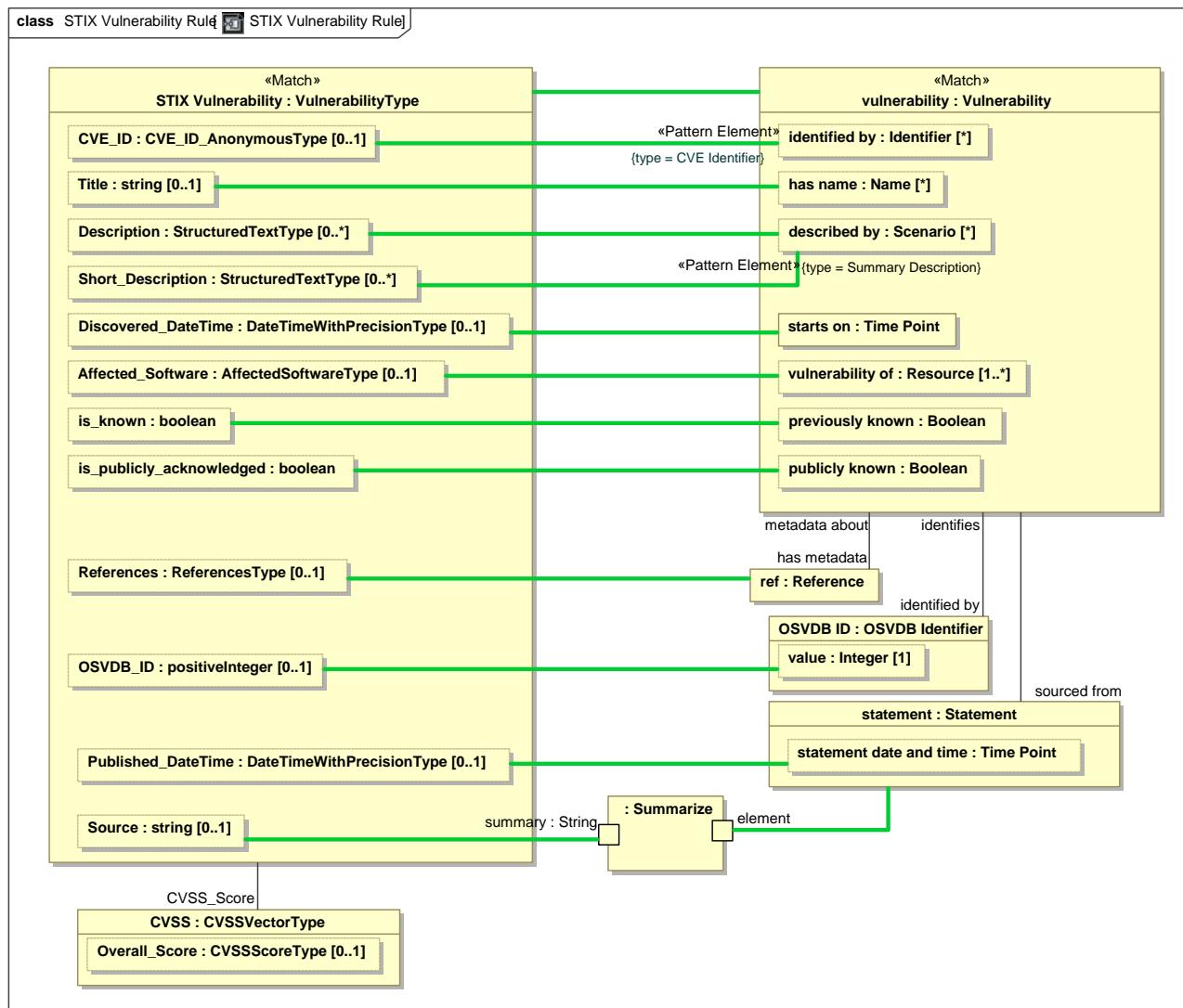


Figure 95. STIX Vulnerability Rule

**package** STIX Mapping to the threat/risk conceptual model::STIX Mapping Rules

# **10 NIEM Mapping Specification (Normative)**

This clause specifies the mapping between NIEM-Core and the threat/risk conceptual model using the mapping profile specified defined in section 12.

## **10.1 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 & risk.

## **10.2 Generic NIEM mapping rules and conventions**

The mapping specification below specifies the semantic relationships between NIEM and the corresponding conceptual 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 conceptual 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 conceptual 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 utilizes multiple inheritance (and multiple classification) directly. Implementations shall convert augmentations to a multiple inheritance interpretation when mapping to the conceptual model.

## NIEM substitution groups

NIEM substitution groups correspond roughly to “subsets” and “redefines” relations in the conceptual 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 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 a relationship is made directly to contact means whch 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 subsititue for that property corresponds to a subclass in the conceptual model, which will also have a mapping. In this way the implementation shall correctly map between the substitution groups and conceptual class hierarchies.

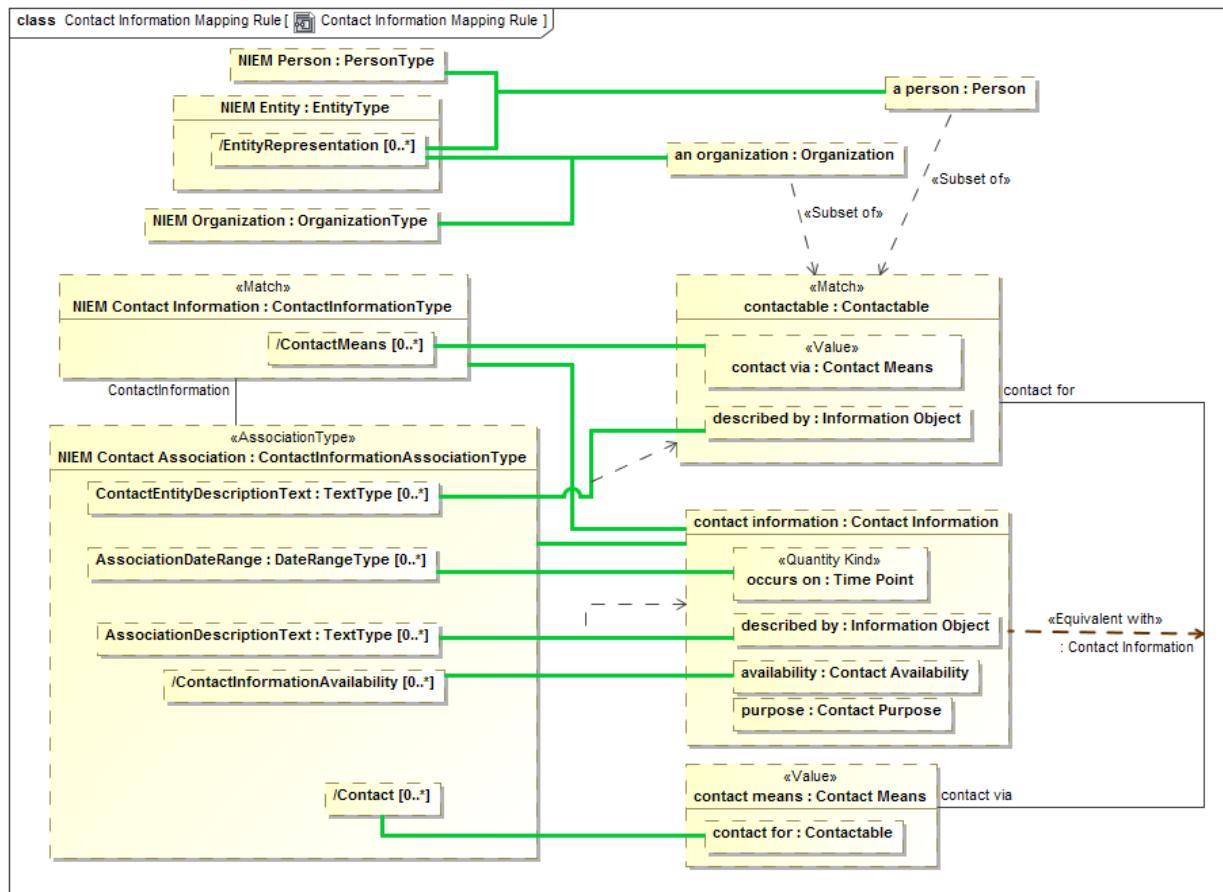


Figure 11 Example mapping involving substitution groups.

## 10.3 NIEM Mapping to the threat / risk model::Facades::Contact Information

### 10.3.1 Diagram: Contact Information Facades

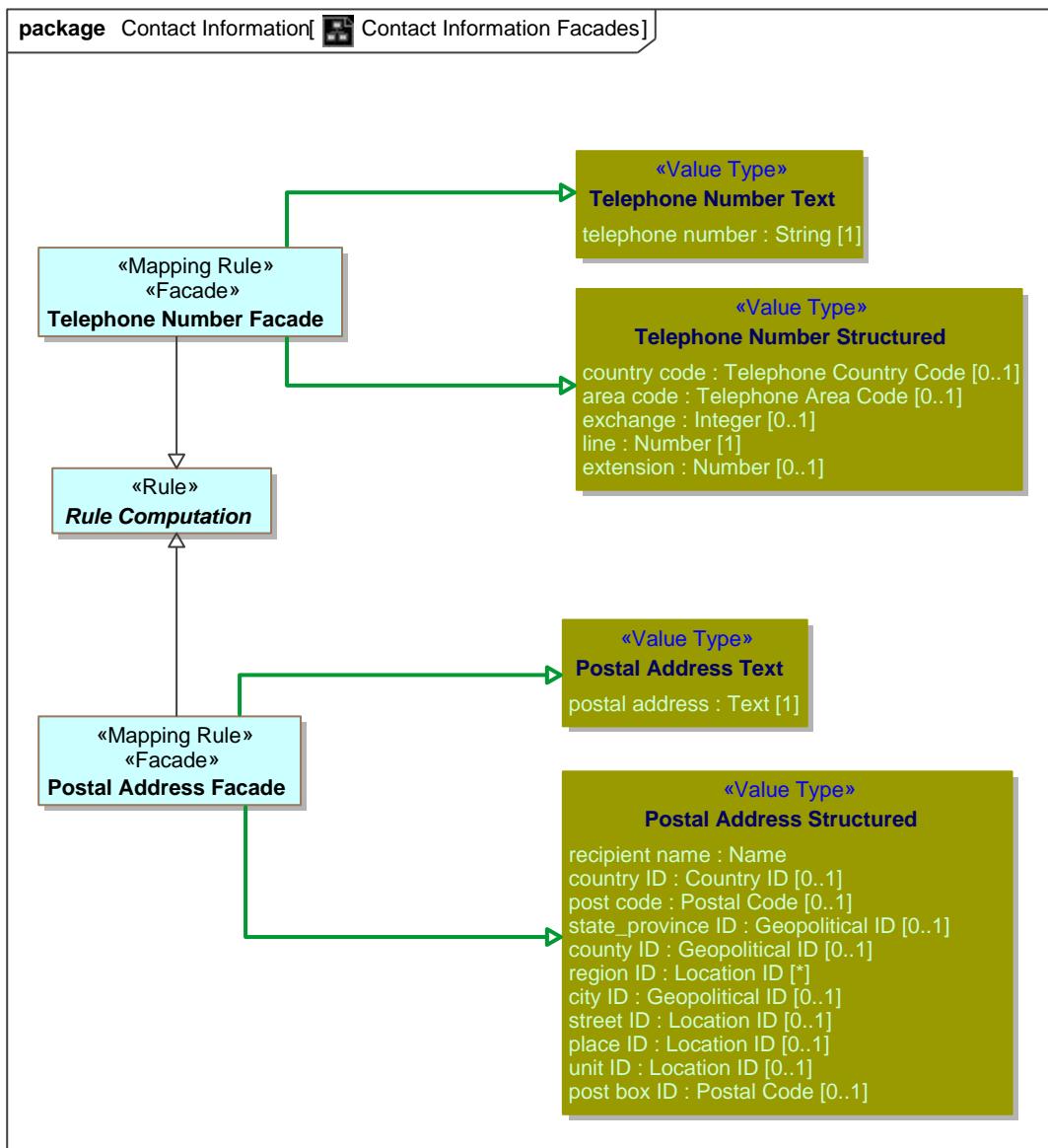


Figure 96. Contact Information Facades

### 10.3.2 Class Postal Address Facade

The union of textual and structured address. Mapping logic will parse and distribute the fields.

### 10.3.21 Direct Supertypes

[Postal Address Structured](#), [Postal Address Text](#), [Rule Computation](#)

**package** NIEM Mapping to the threat / risk model::Facades::Contact Information

### 10.3.22 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.

## 10.3.3 Class Telephone Number Facade

The union of textual and structured phone number. Mapping logic will parse and distribute the fields.

### 10.3.31 Direct Supertypes

[Rule Computation](#), [Telephone Number Structured](#), [Telephone Number Text](#)

**package** NIEM Mapping to the threat / risk model::Facades::Contact Information

## 10.4 NIEM Mapping to the threat / risk model::Facades::Injury

### 10.4.1 Diagram: Person Injury Facade

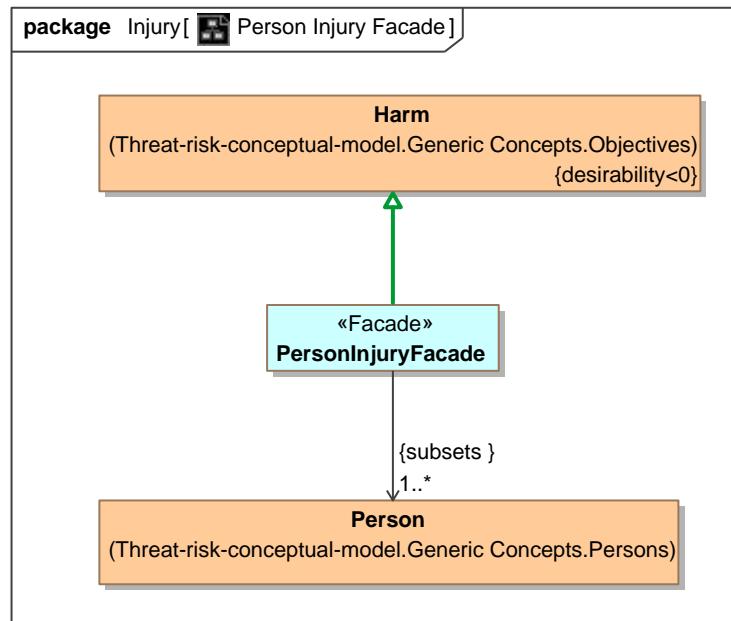


Figure 97. Person Injury Facade

### 10.4.2 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.

#### 10.4.21 Direct Supertypes

[Harm](#)

**package** NIEM Mapping to the threat / risk model::Facades::Injury

#### 10.4.22 Associations

: [Person](#) [1..\*] Subsets: :[Resource](#)

## 10.5 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships

Mapping specification of NIEM Core to the threat/risk model

### 10.5.1 Diagram: NIEM Mapping Rules

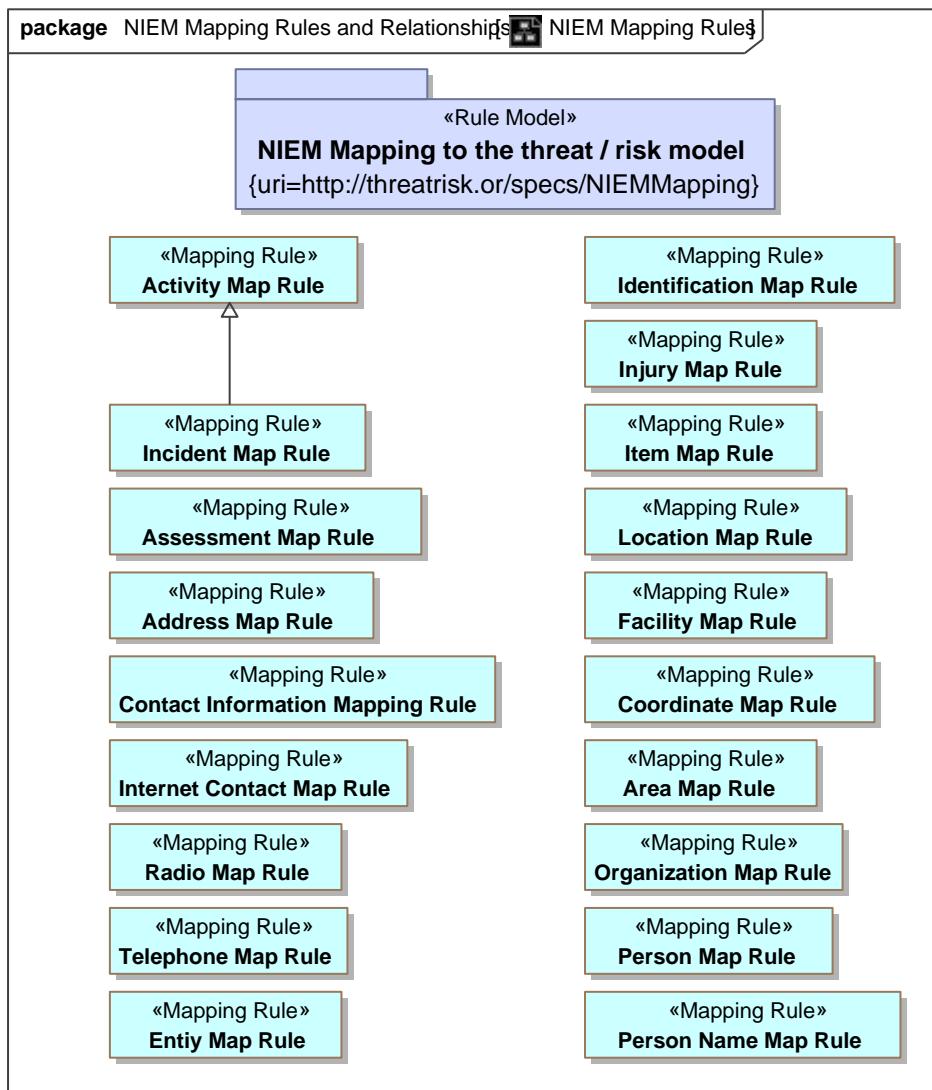


Figure 98. NIEM Mapping Rules

## 10.5.2 Diagram: NIEM Mapping Summary 1

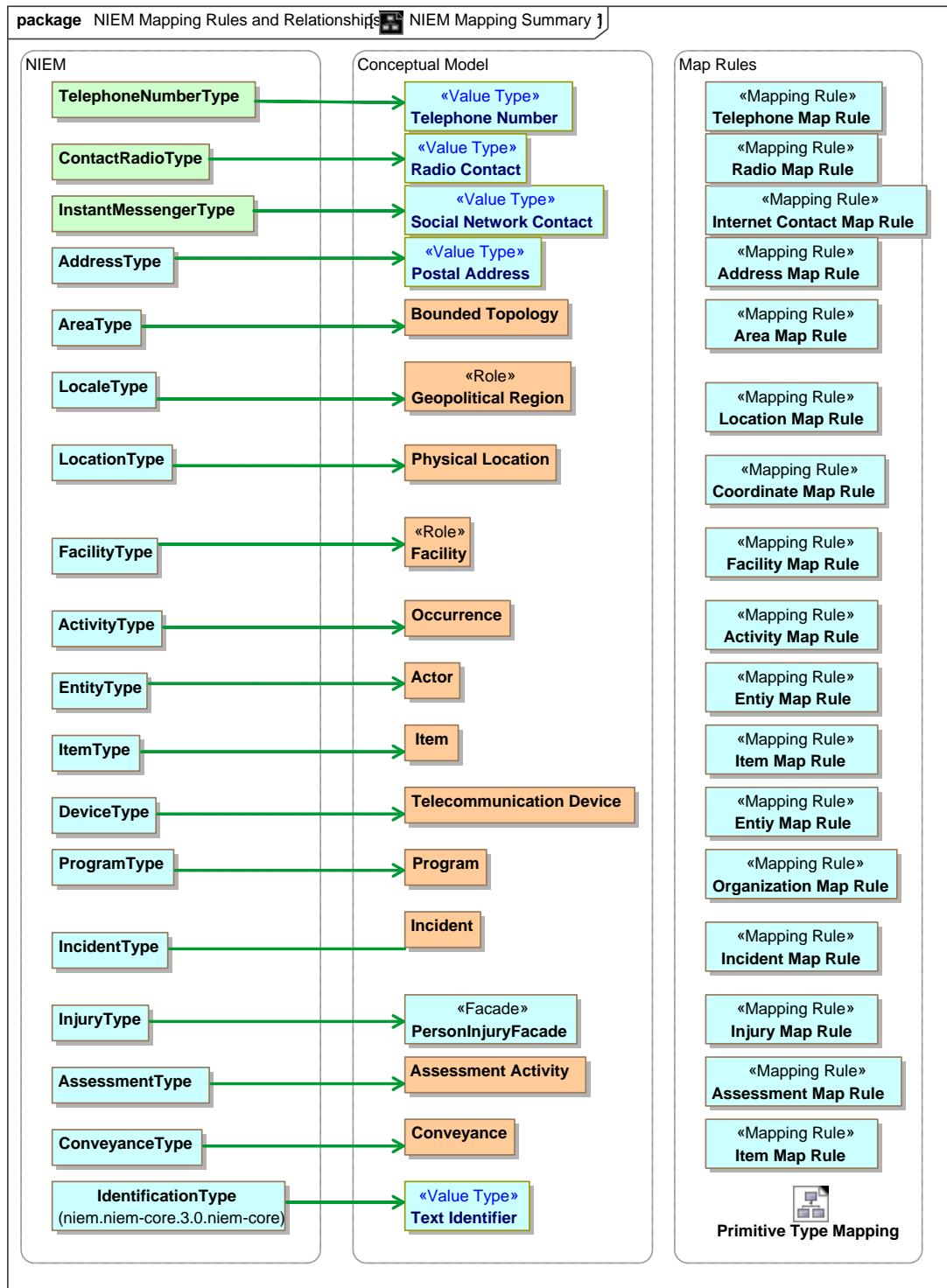


Figure 99. NIEM Mapping Summary 1

### 10.5.3 Diagram: NIEM Mapping Summary 2

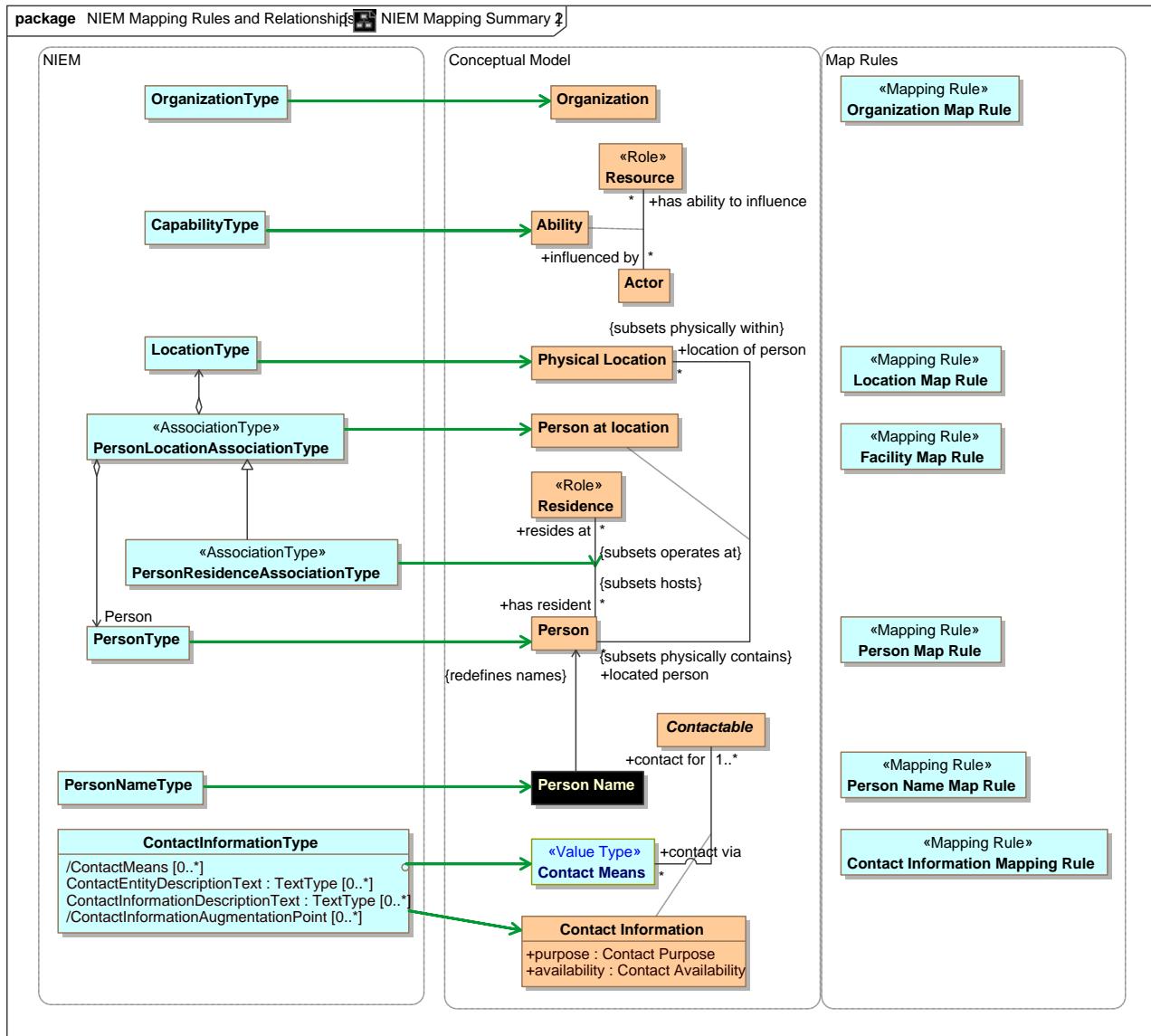


Figure 100. NIEM Mapping Summary 2

## 10.6 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Activity

Mapping specification of NIEM Activity to the threat/risk model

### 10.6.1 Diagram: Activity Mapping Summary

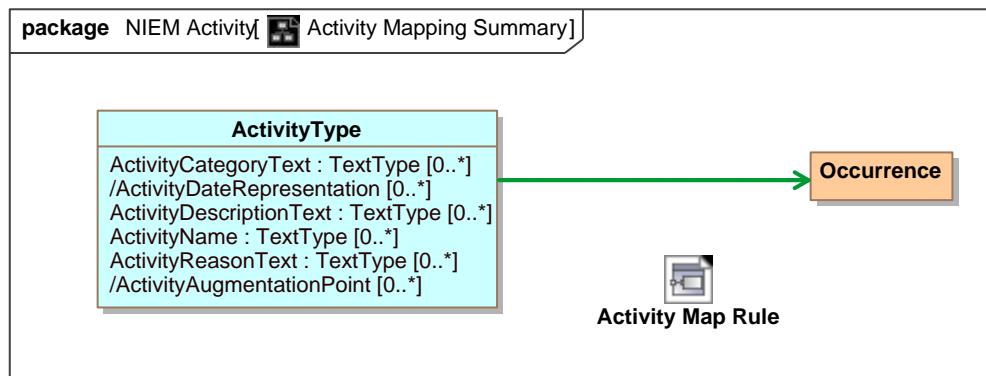


Figure 101. Activity Mapping Summary

### 10.6.2 Class Activity Map Rule

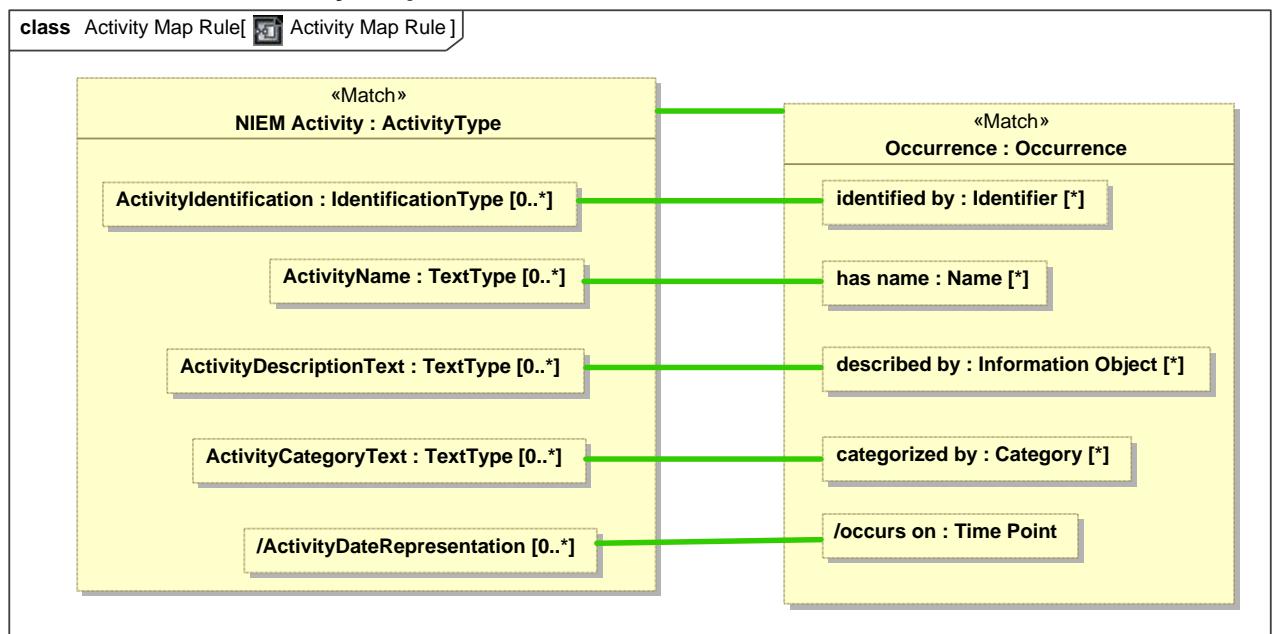


Figure 102. Activity Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Activity

## 10.7 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Assessment

Mapping specification of NIEM Assessment to the threat/risk model

### 10.7.1 Diagram: Assessment Mapping Summary

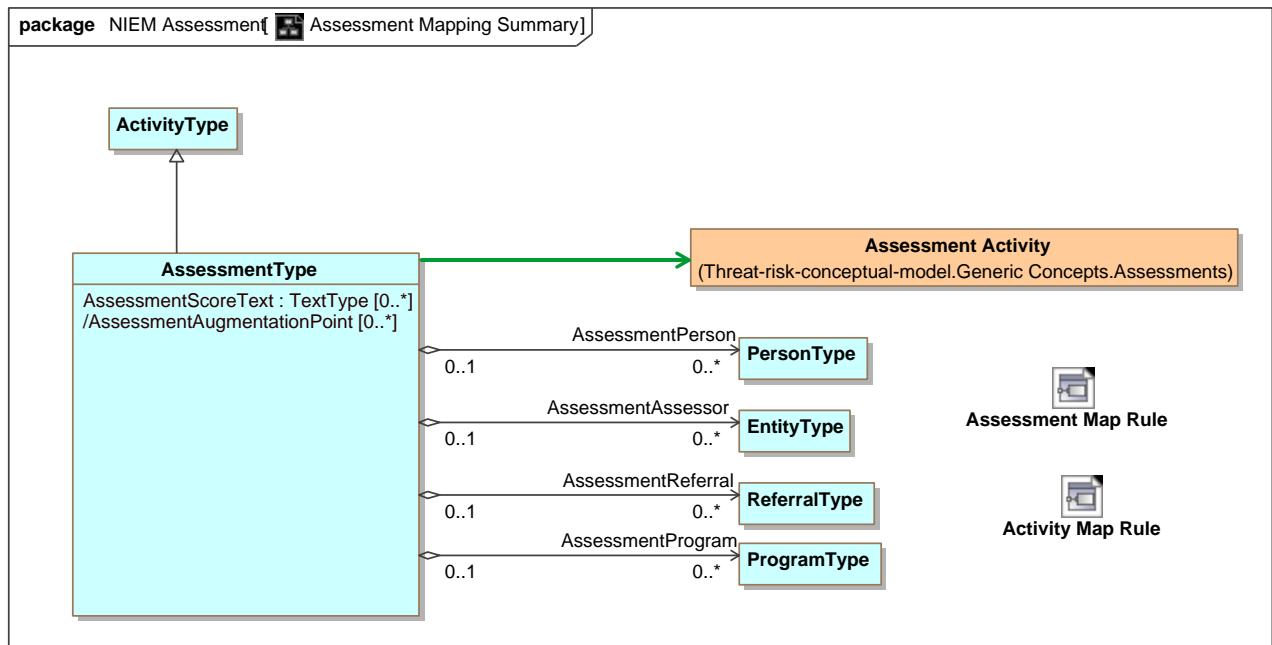


Figure 103. Assessment Mapping Summary

## 10.7.2 Class Assessment Map Rule

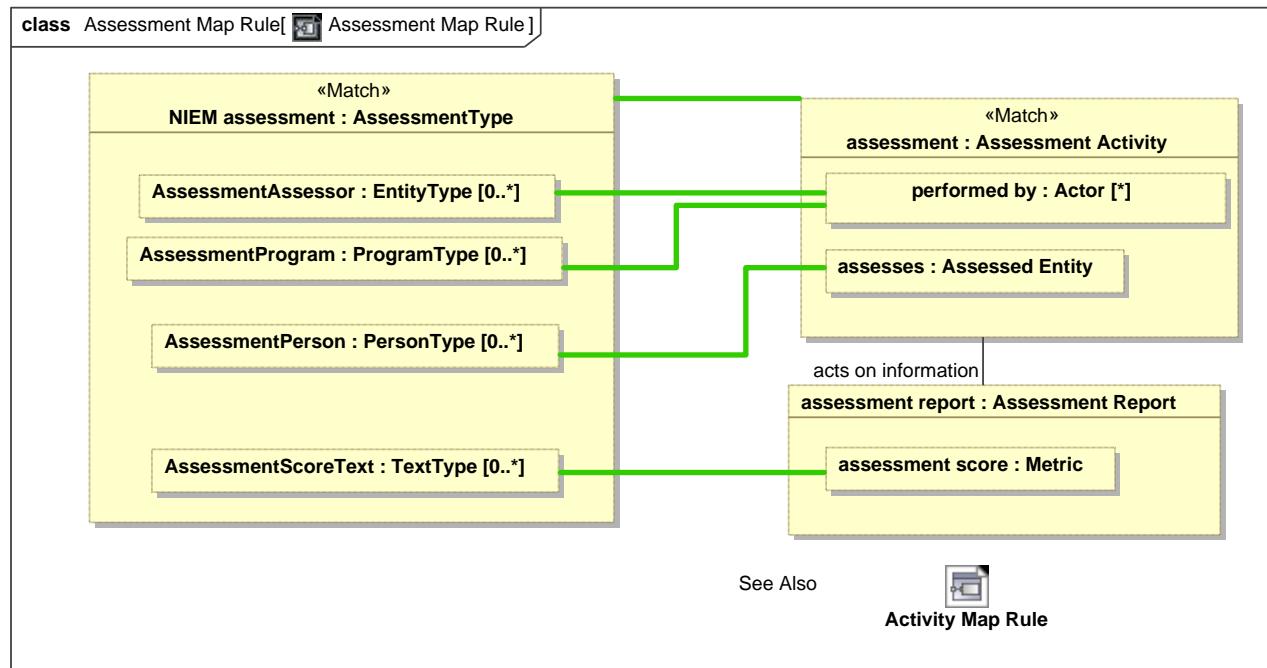


Figure 104. Assessment Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Assessment

## 10.8 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

### 10.8.1 Diagram: Contact Information Mapping Summary

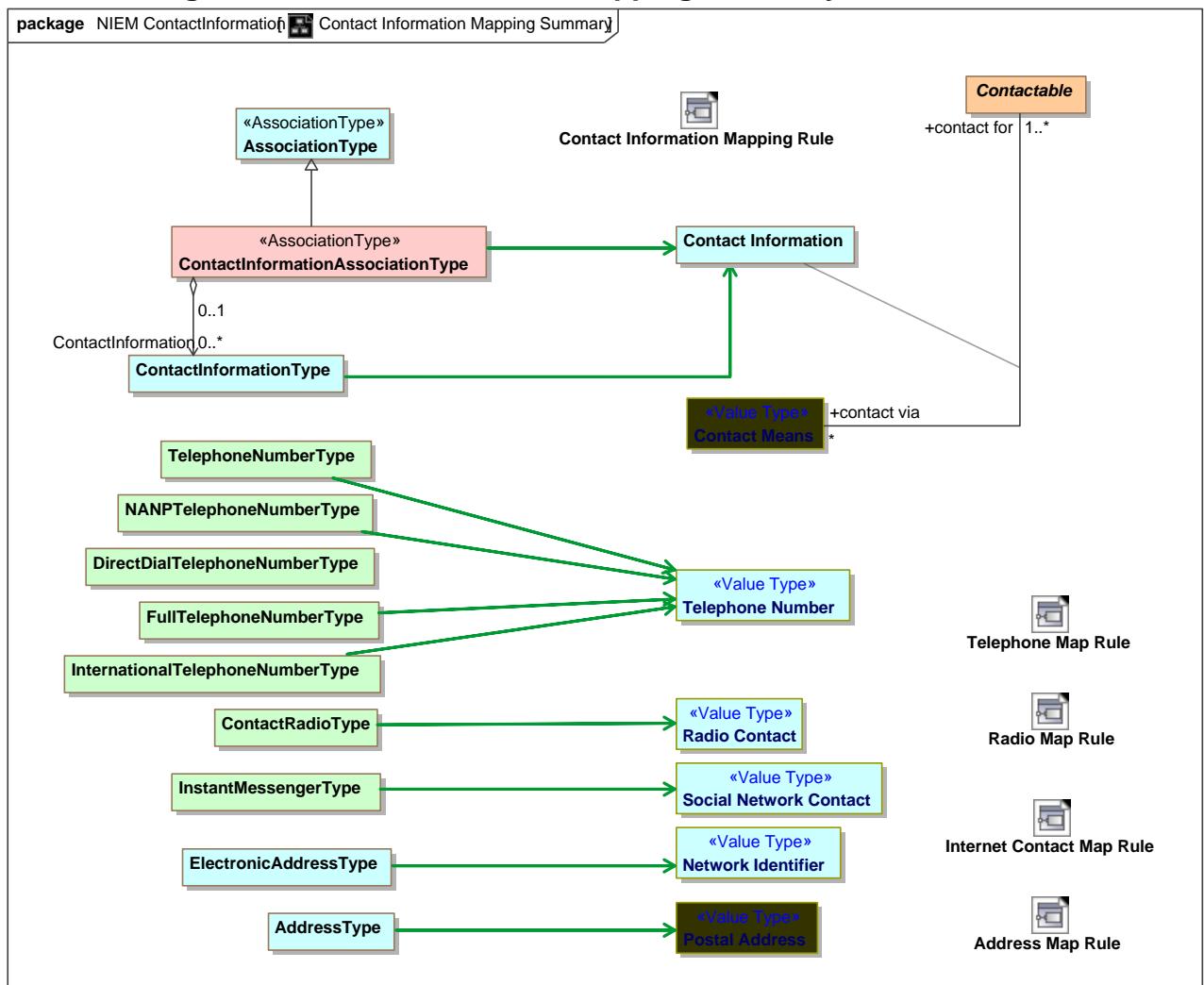


Figure 105. Contact Information Mapping Summary

## 10.8.2 Class Address Map Rule

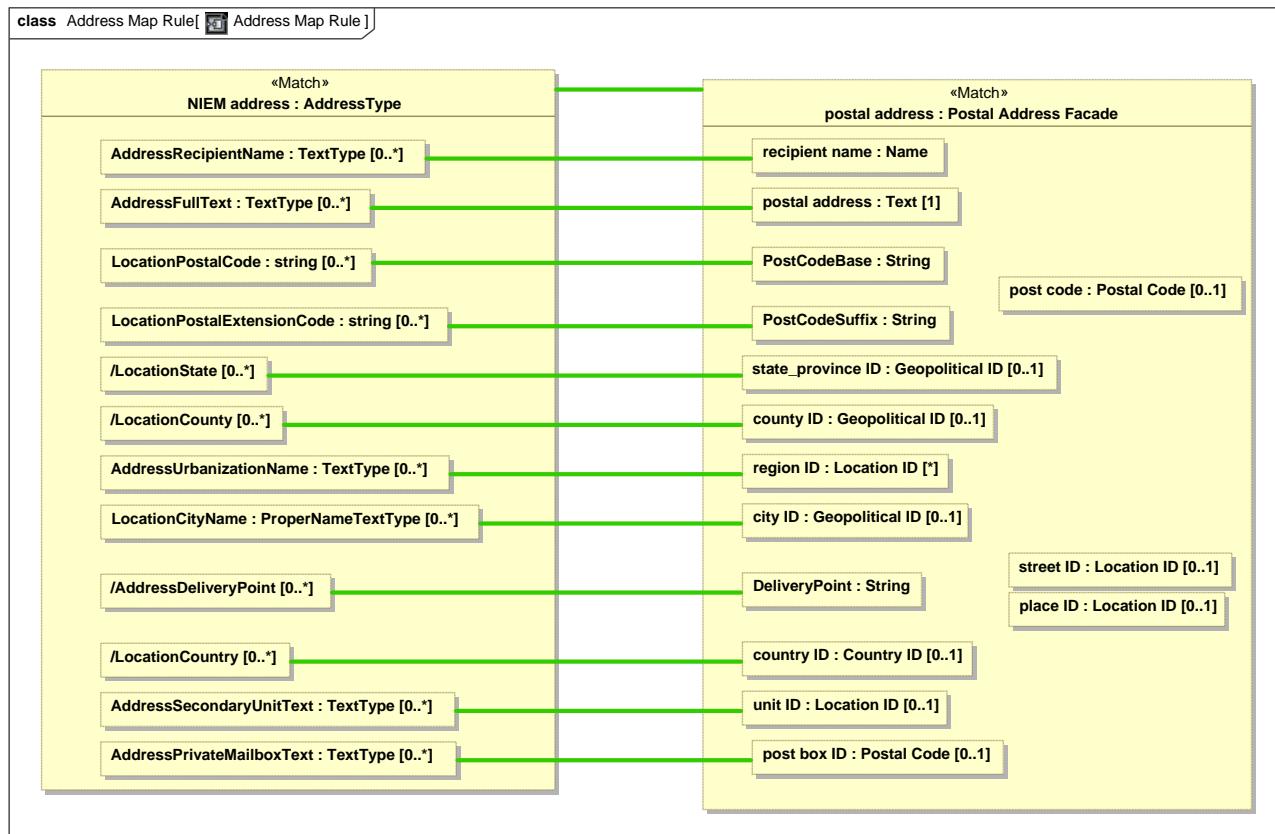


Figure 106. Address Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

### 10.8.3 Class Contact Information Mapping Rule

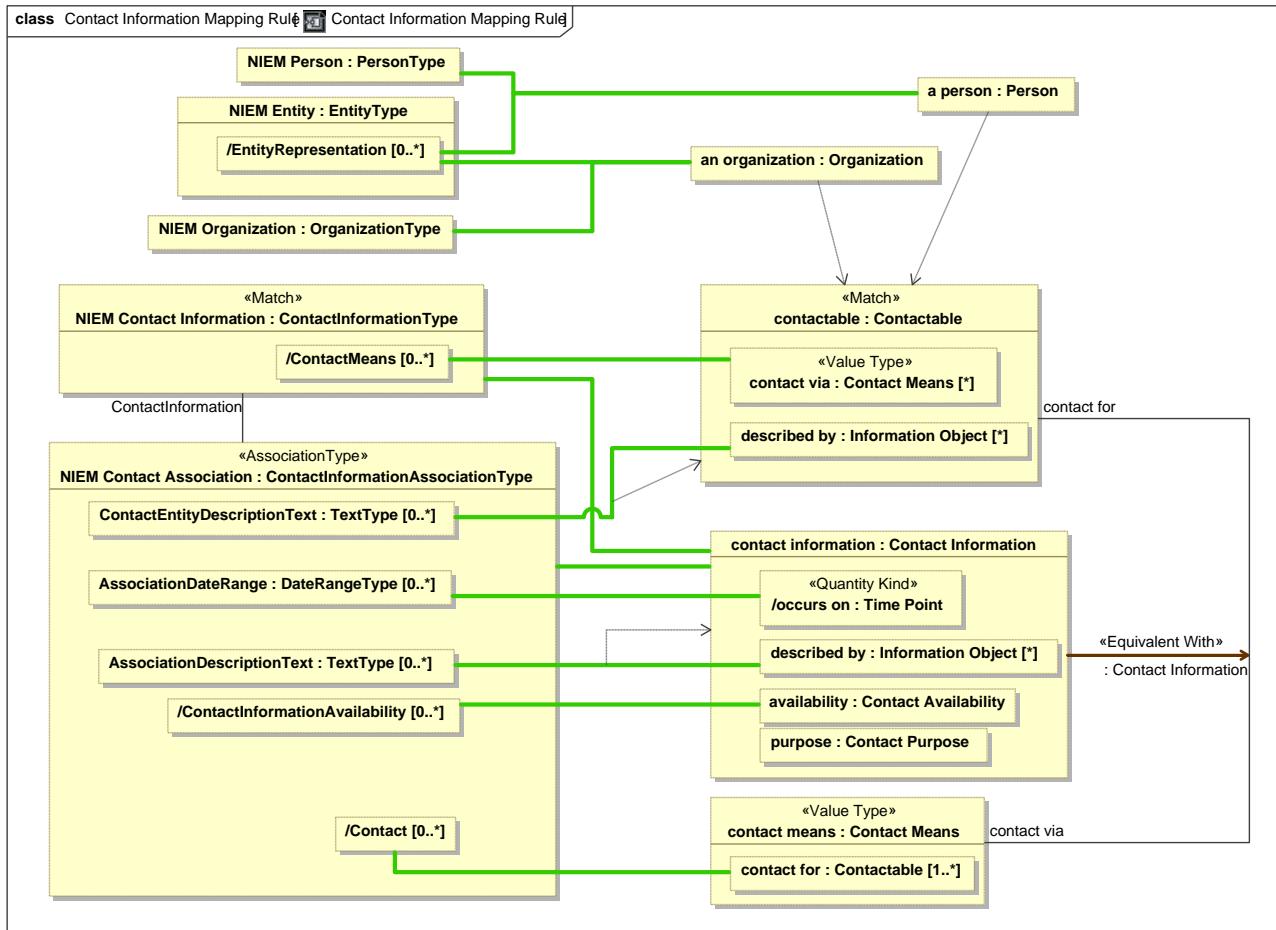


Figure 107. Contact Information Mapping Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

#### 10.8.4 Class Internet Contact Map Rule

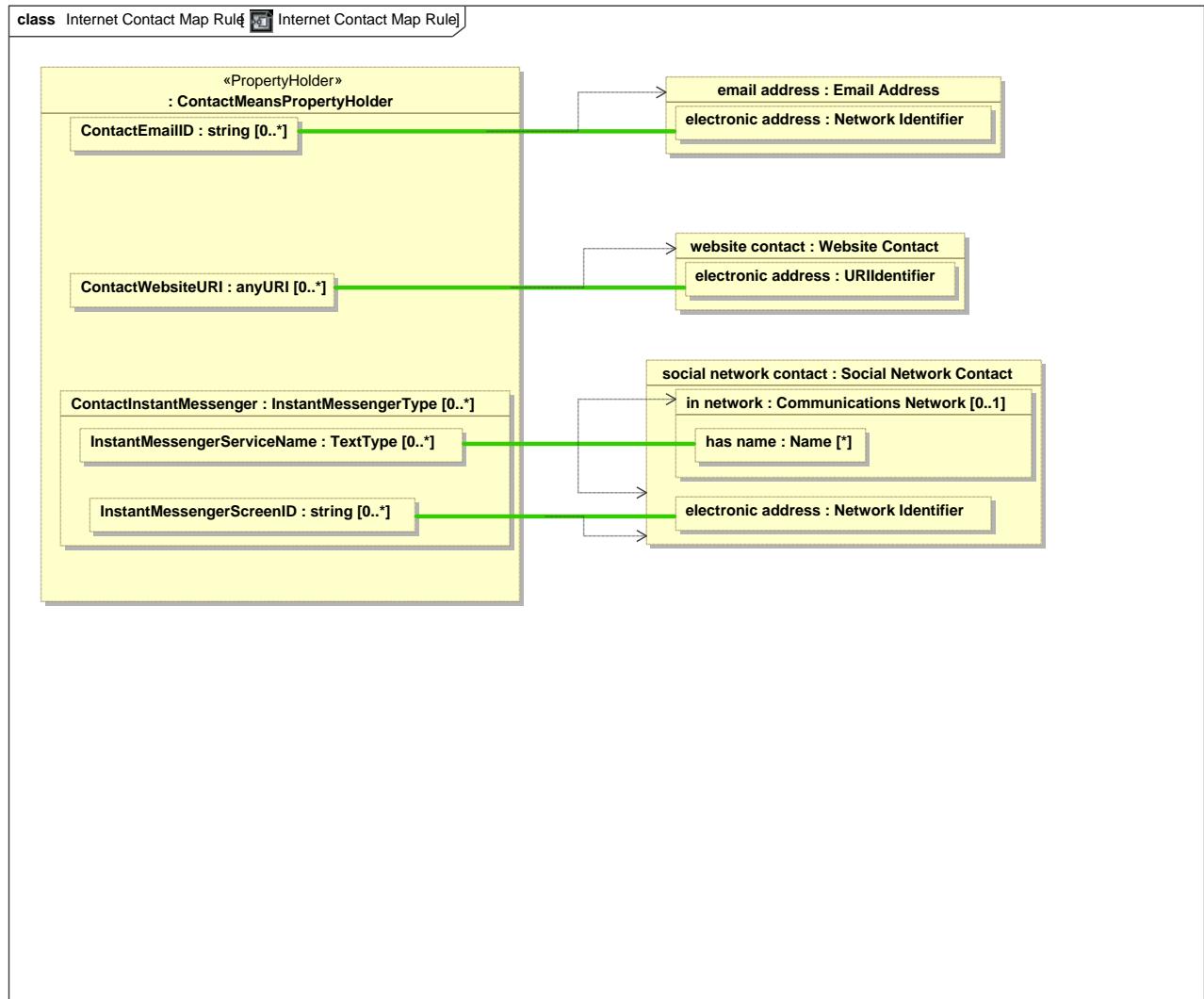


Figure 108. Internet Contact Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

### 10.8.5 Class Radio Map Rule

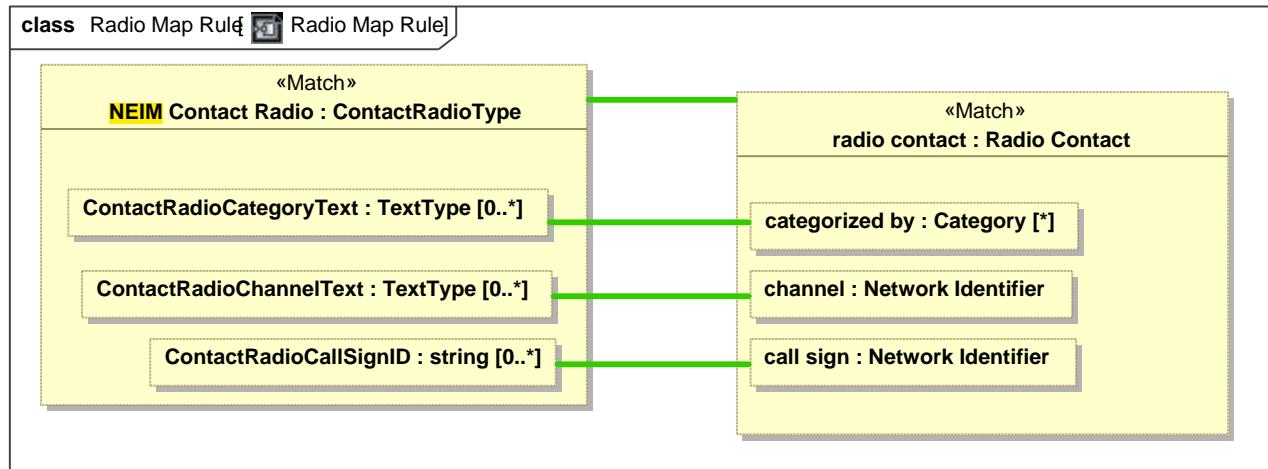


Figure 109. Radio Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

## 10.8.6 Class Telephone Map Rule

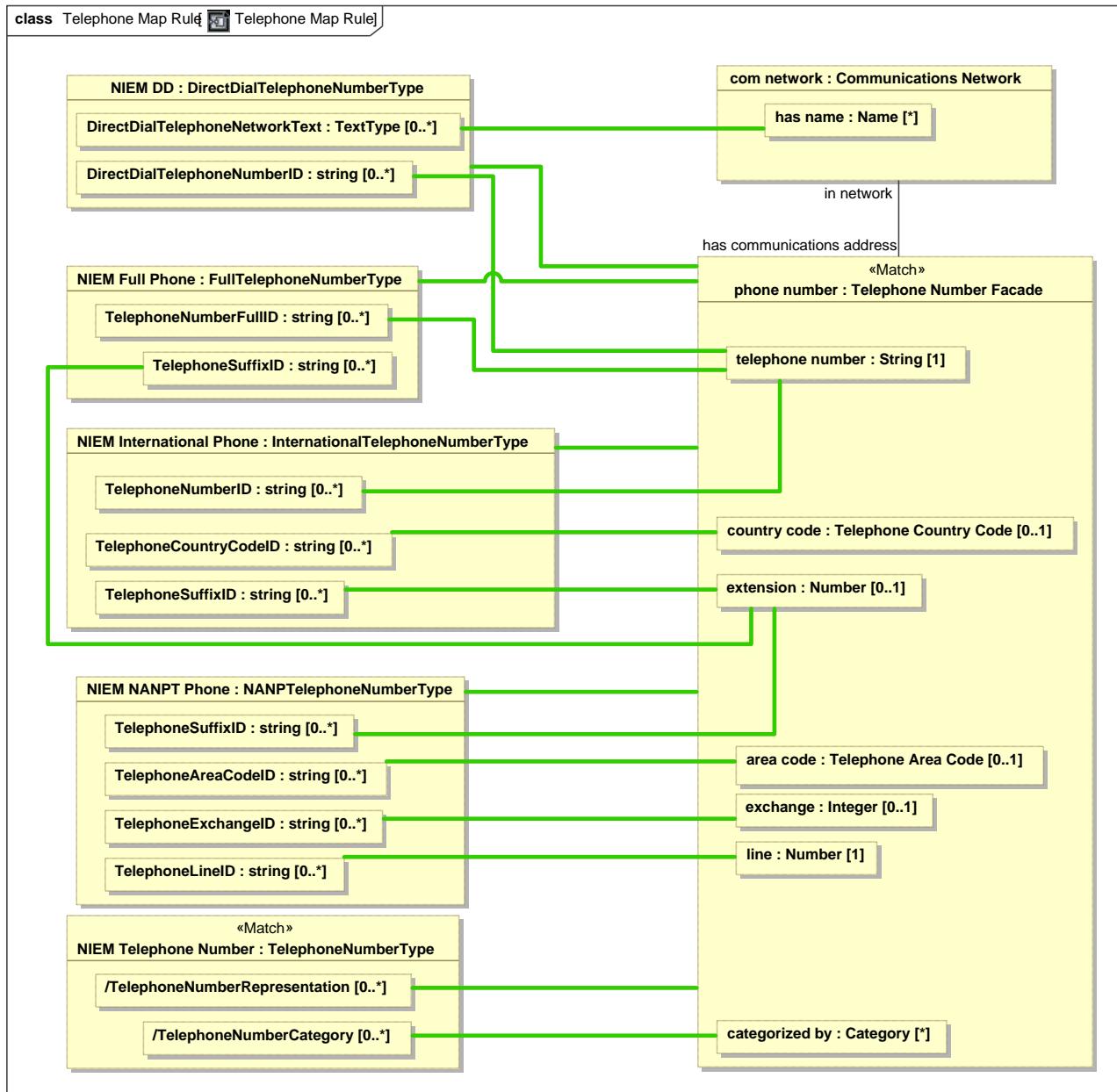


Figure 110. Telephone Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM ContactInformation

## 10.9 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Entity

Mapping specification of NIEM Entity to the threat/risk model.

### 10.9.1 Diagram: Entity Mapping Summary

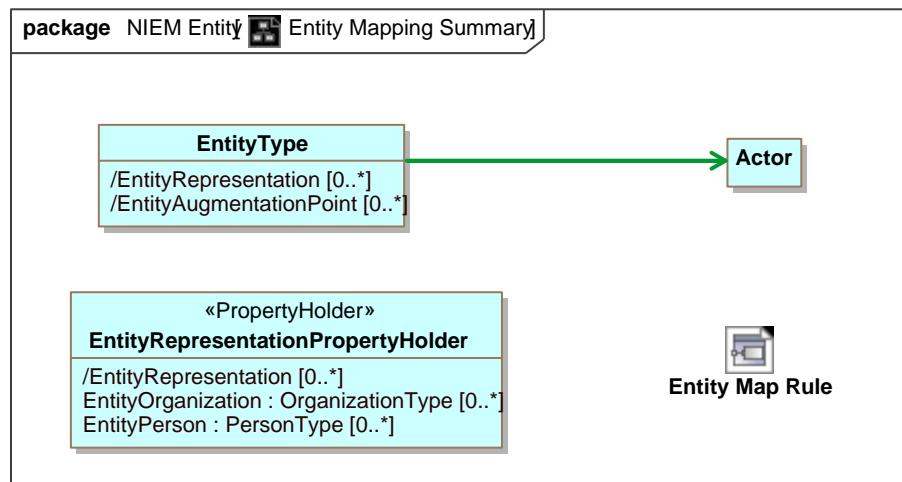
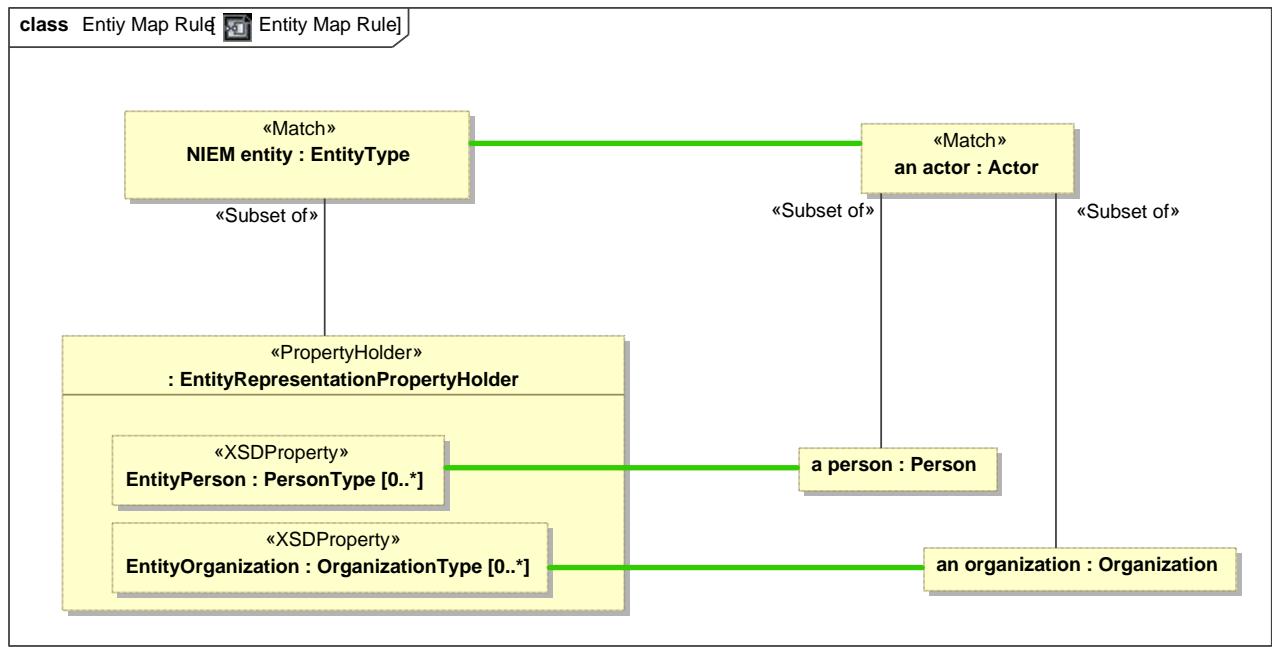


Figure 111. Entity Mapping Summary

### 10.9.2 Class Entiy Map Rule

Detail is provide in the mappings to person and organization.



**Figure 112. Entity Map Rule**

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Entity

## 10.10 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.

### 10.10.1 Diagram: Identification Mapping Summary

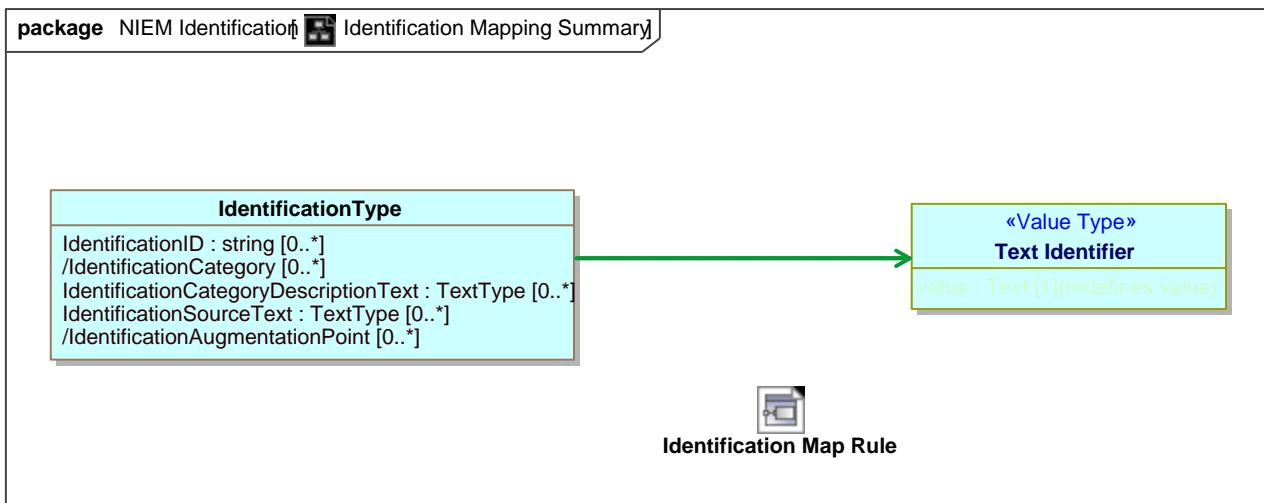


Figure 113. Identification Mapping Summary

## 10.10.2 Class Identification Map Rule

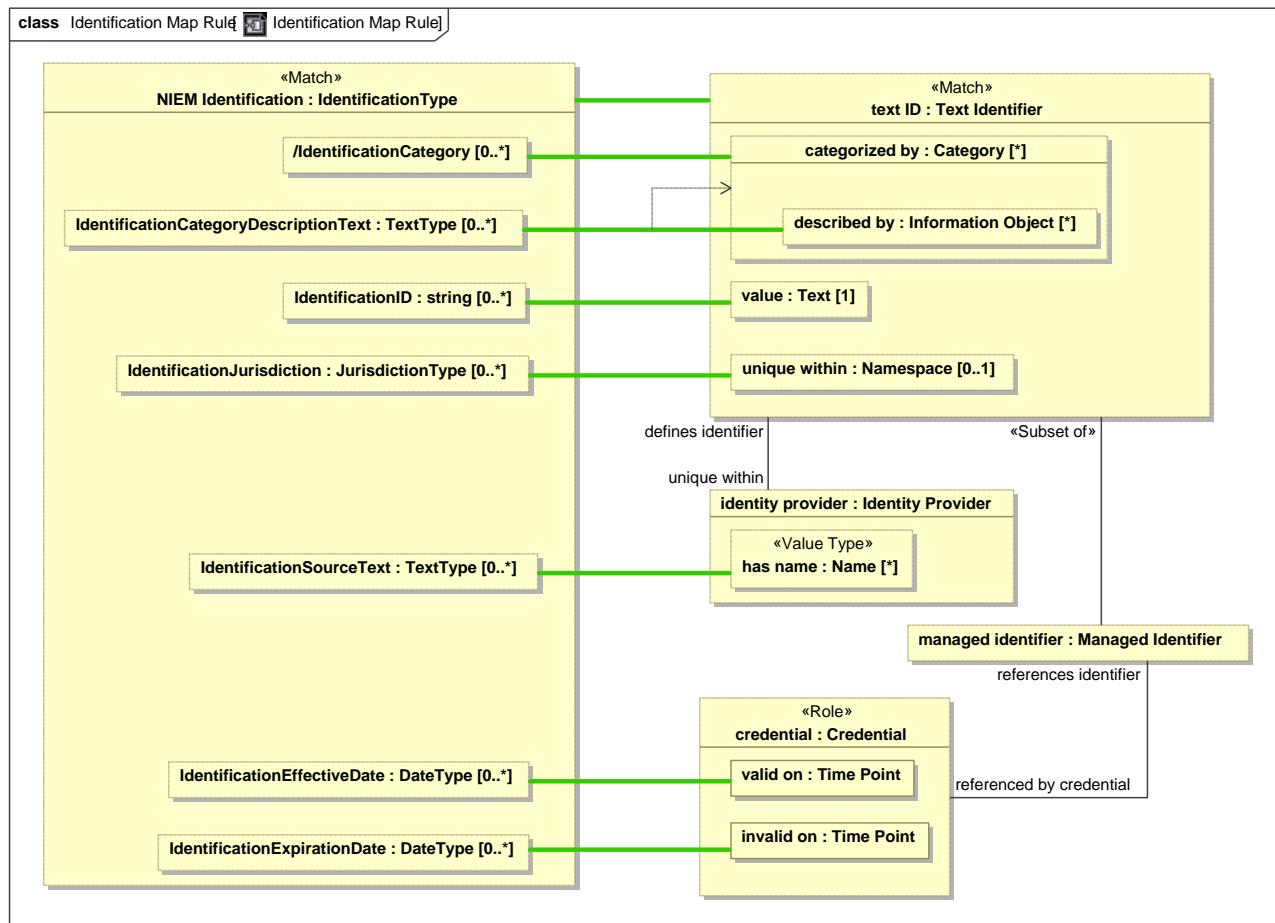


Figure 114. Identification Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Identification

## 10.11 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Incident

Mapping specification of NIEM Incident to the threat/risk model.

### 10.11.1 Diagram: Incident mapping summary

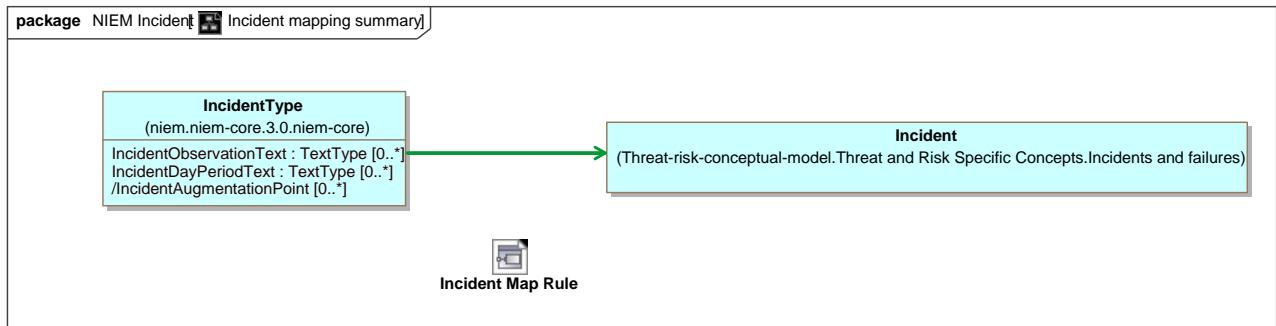


Figure 115. Incident mapping summary

### 10.11.2 Class Incident Map Rule

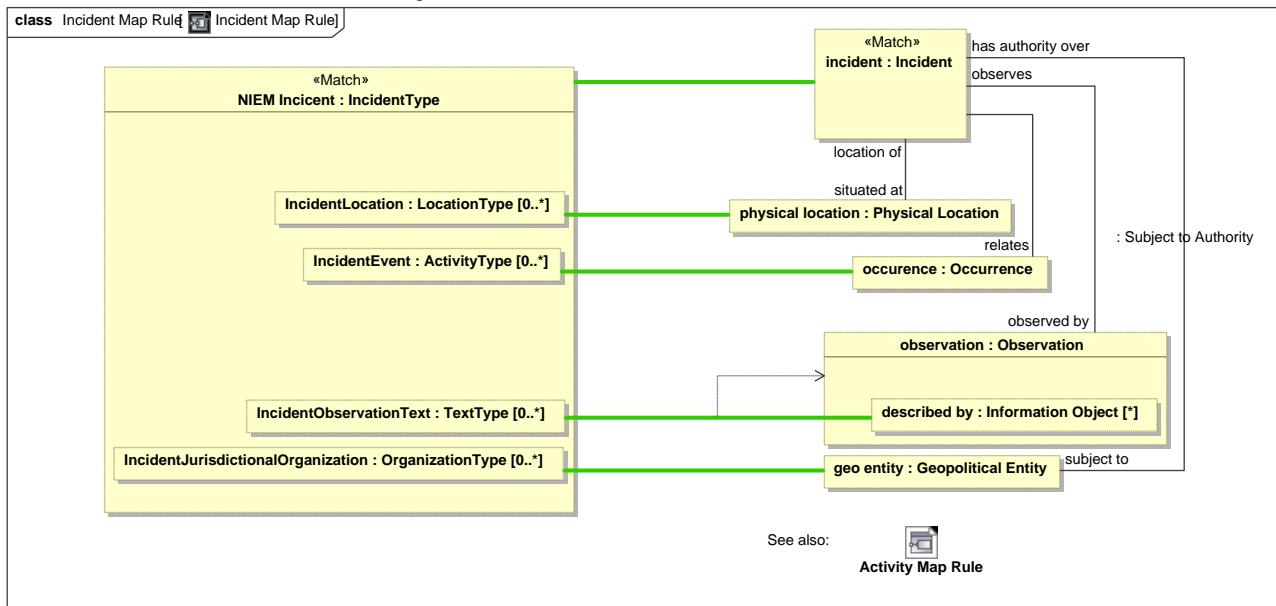


Figure 116. Incident Map Rule

### 10.11.21 Direct Supertypes

[Activity Map Rule](#)

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Incident

## 10.12 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Injury

Mapping specification of NIEM Injury to the threat/risk model.

### 10.12.1 Diagram: Injury Mapping Summary

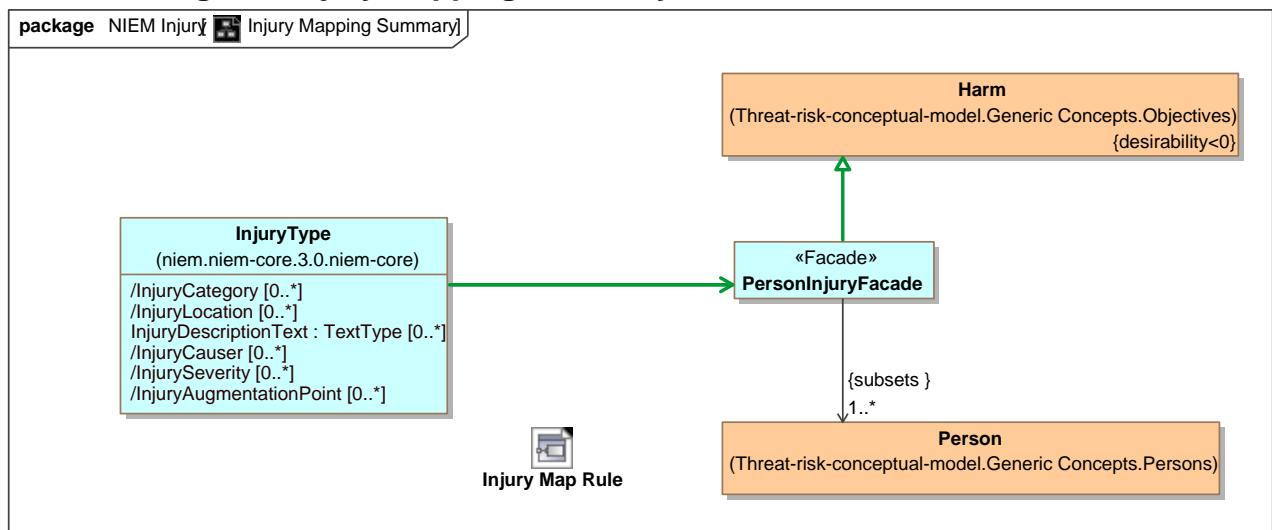


Figure 117. Injury Mapping Summary

## 10.12.2 Class Injury Map Rule

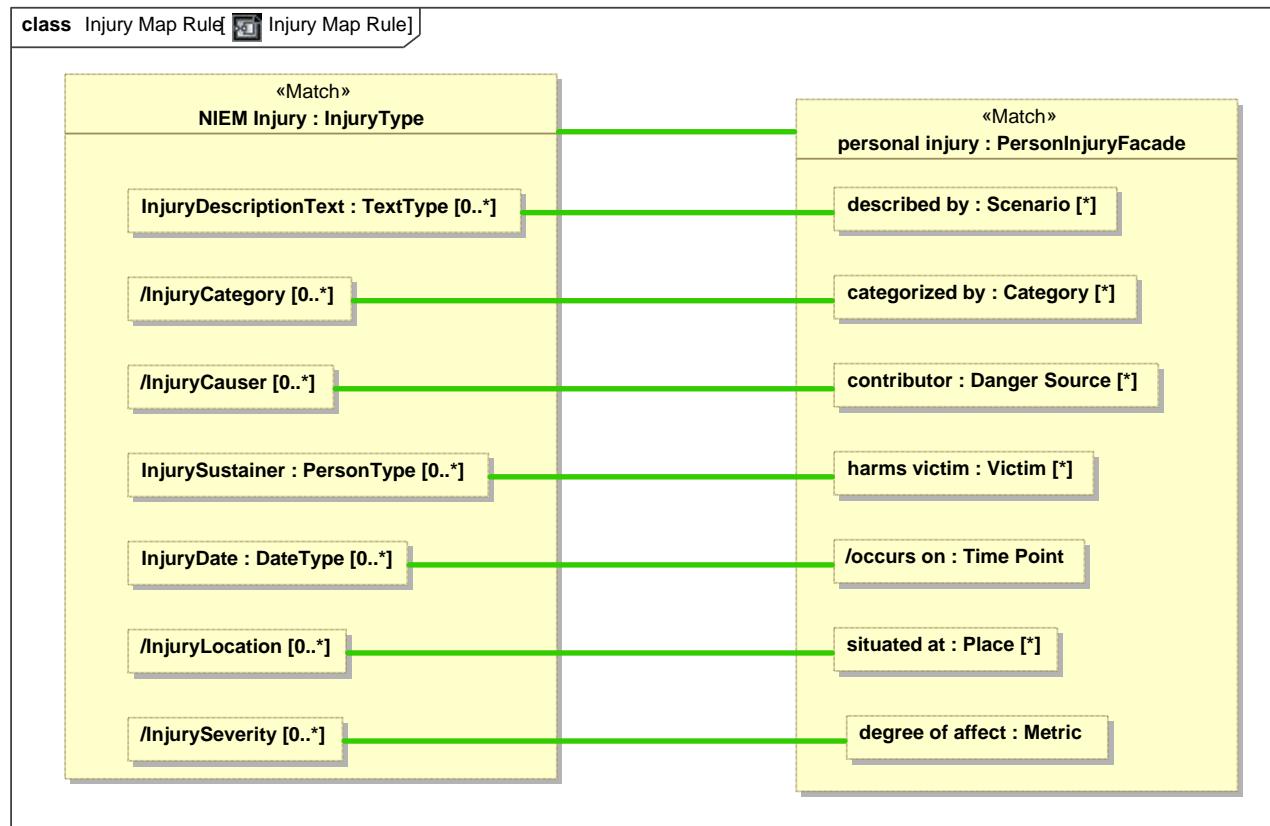


Figure 118. Injury Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Injury

## 10.13 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Item

Mapping specification of NIEM Item to the threat/risk model.

### 10.13.1 Diagram: Item Mapping Summary

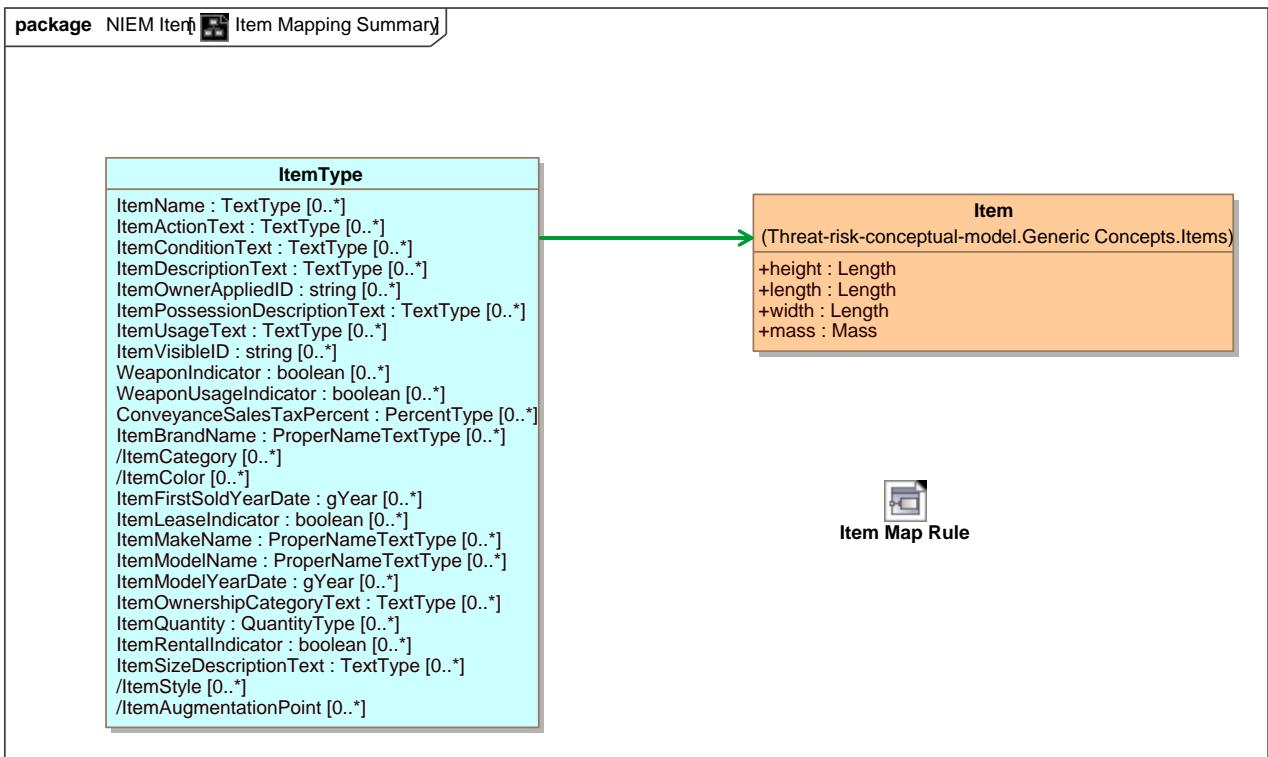


Figure 119. Item Mapping Summary

## 10.13.2 Class Item Map Rule

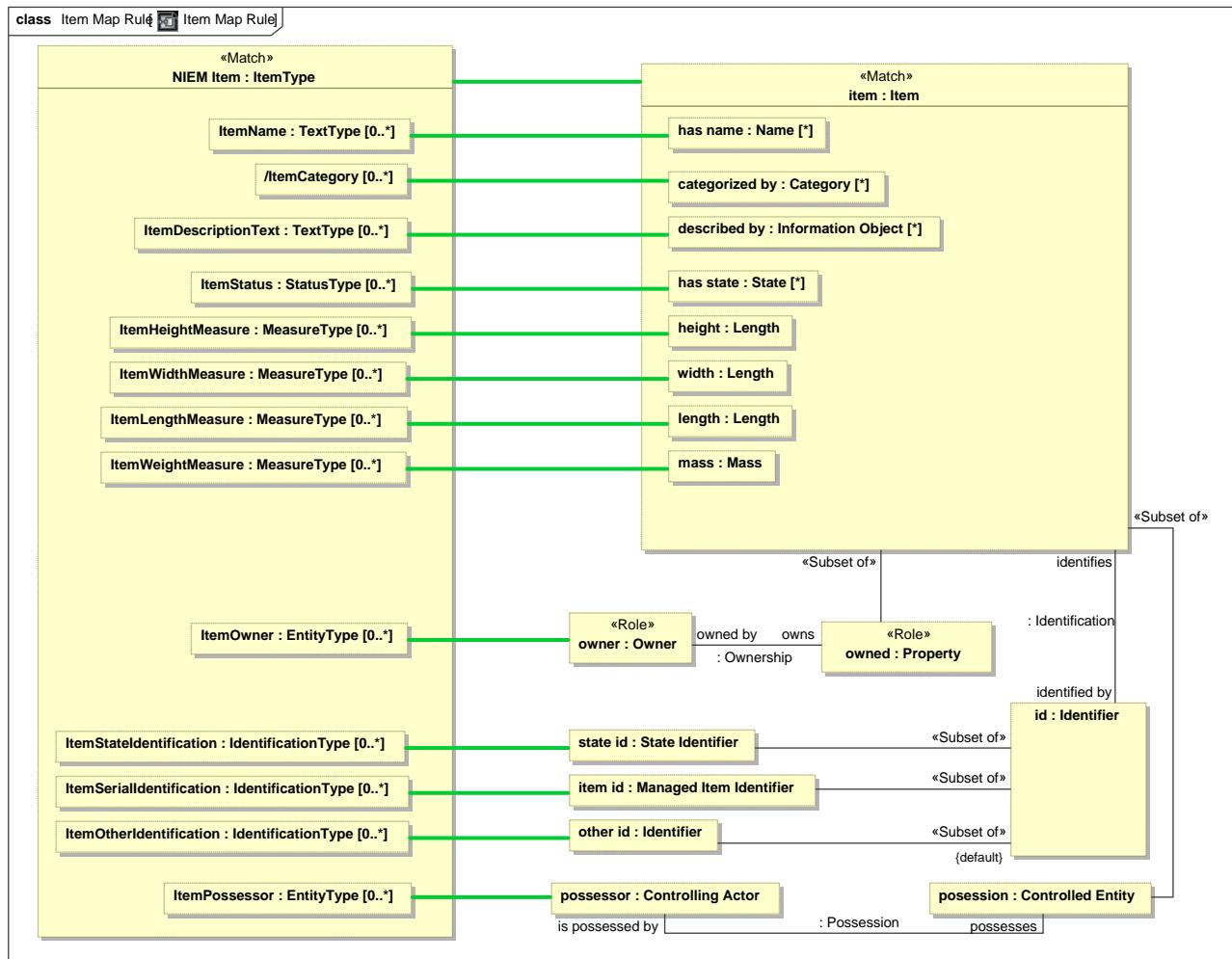


Figure 120. Item Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Item

## **10.14 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location**

Mapping specification of NIEM Location to the threat/risk model.

### 10.14.1 Diagram: Location mapping summary

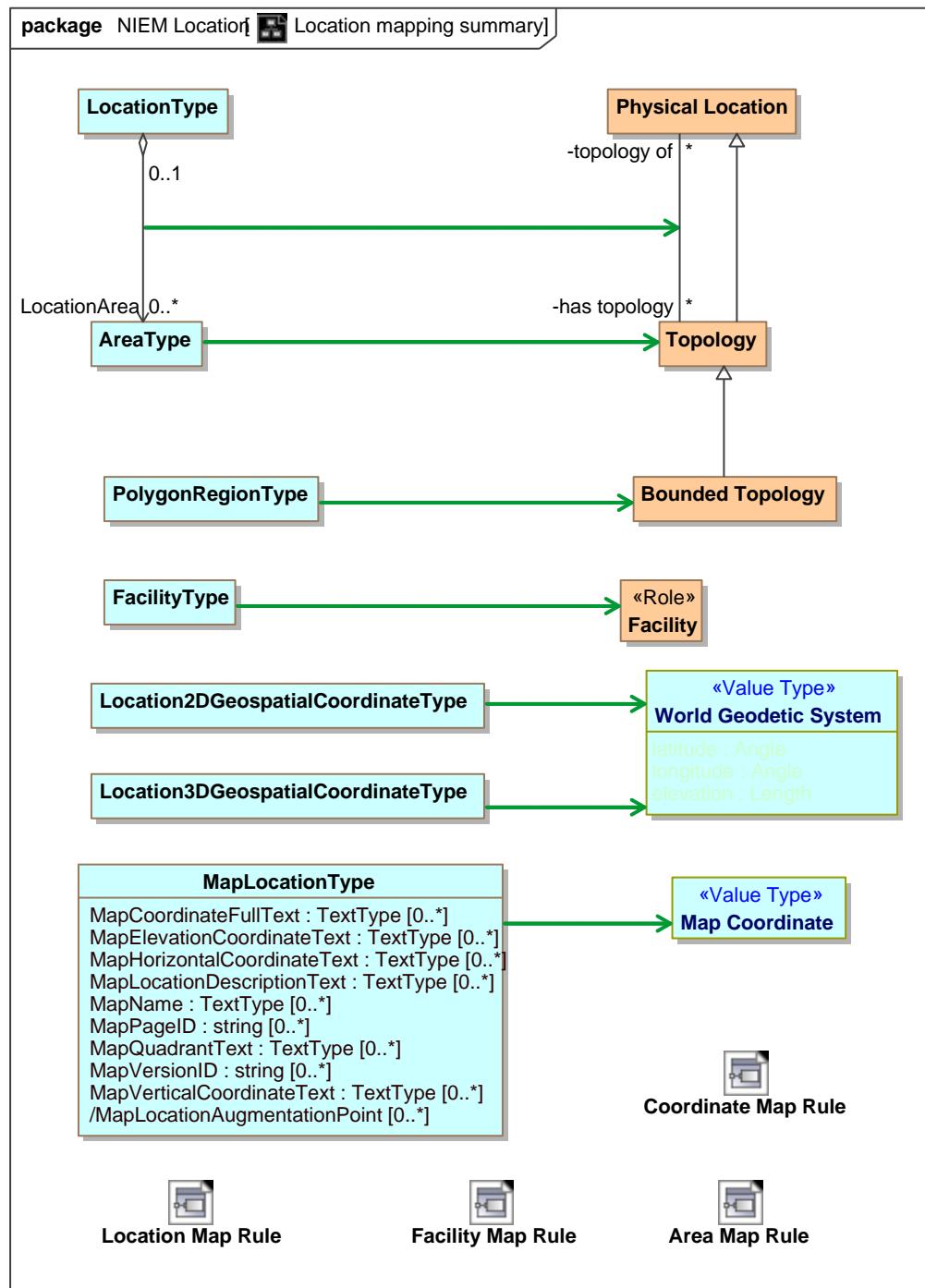


Figure 121. Location mapping summary

## 10.14.2 Class Area Map Rule

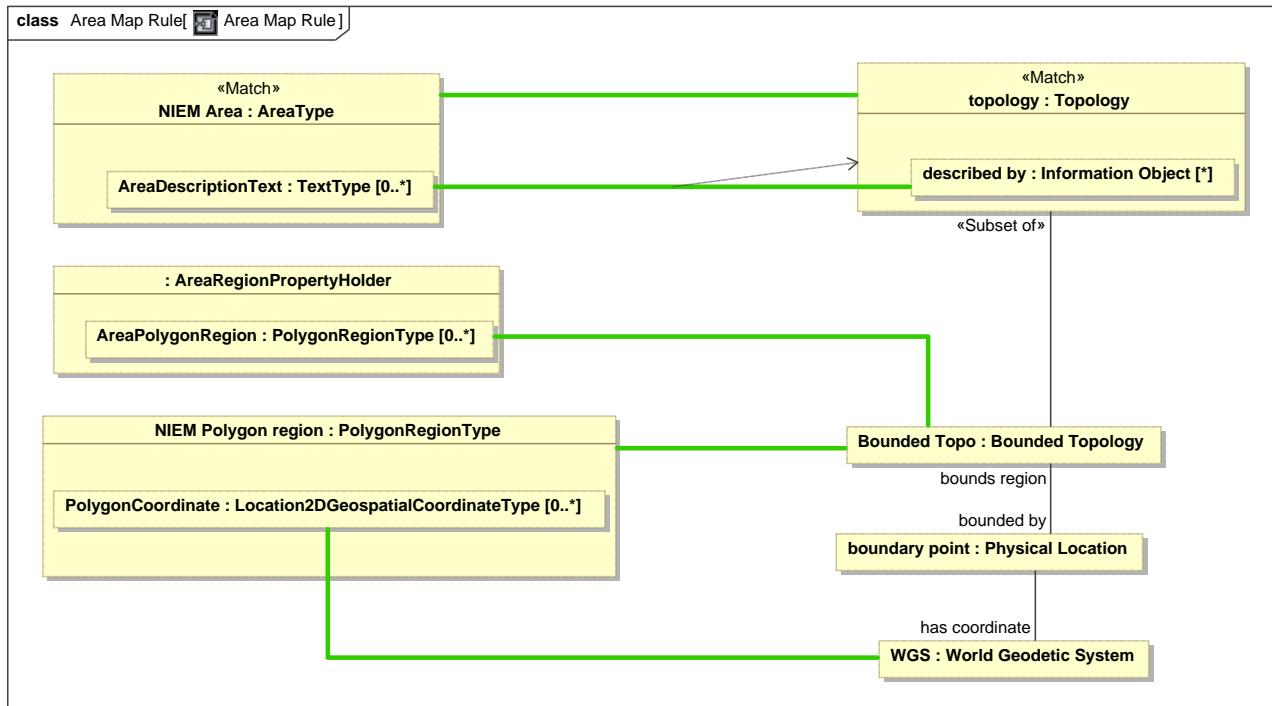


Figure 122. Area Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location

## 10.14.3 Class Coordinate Map Rule

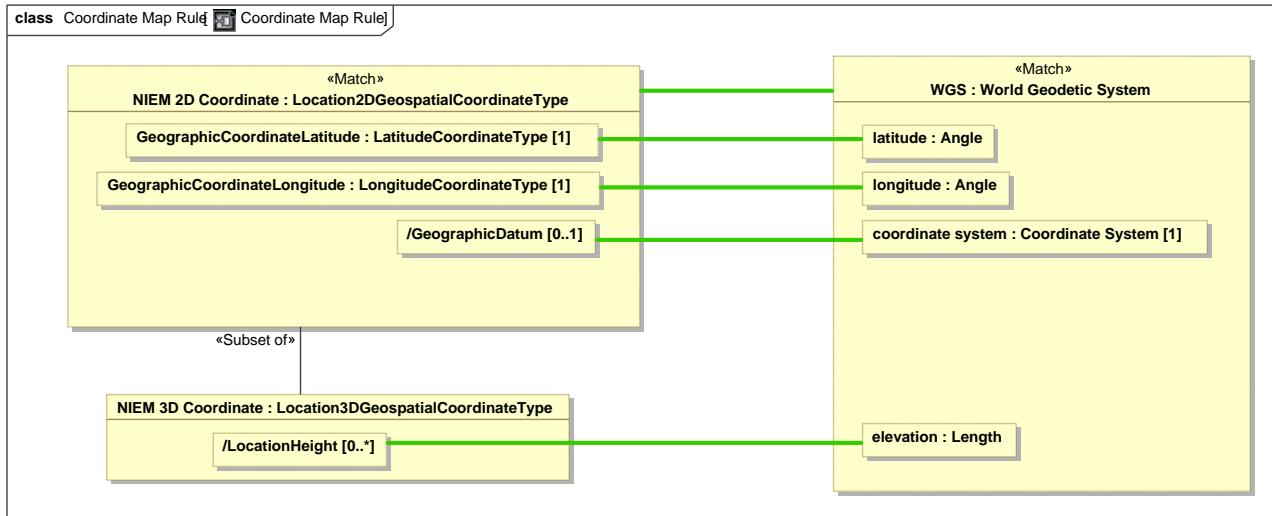


Figure 123. Coordinate Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location

#### 10.14.4 Class Facility Map Rule

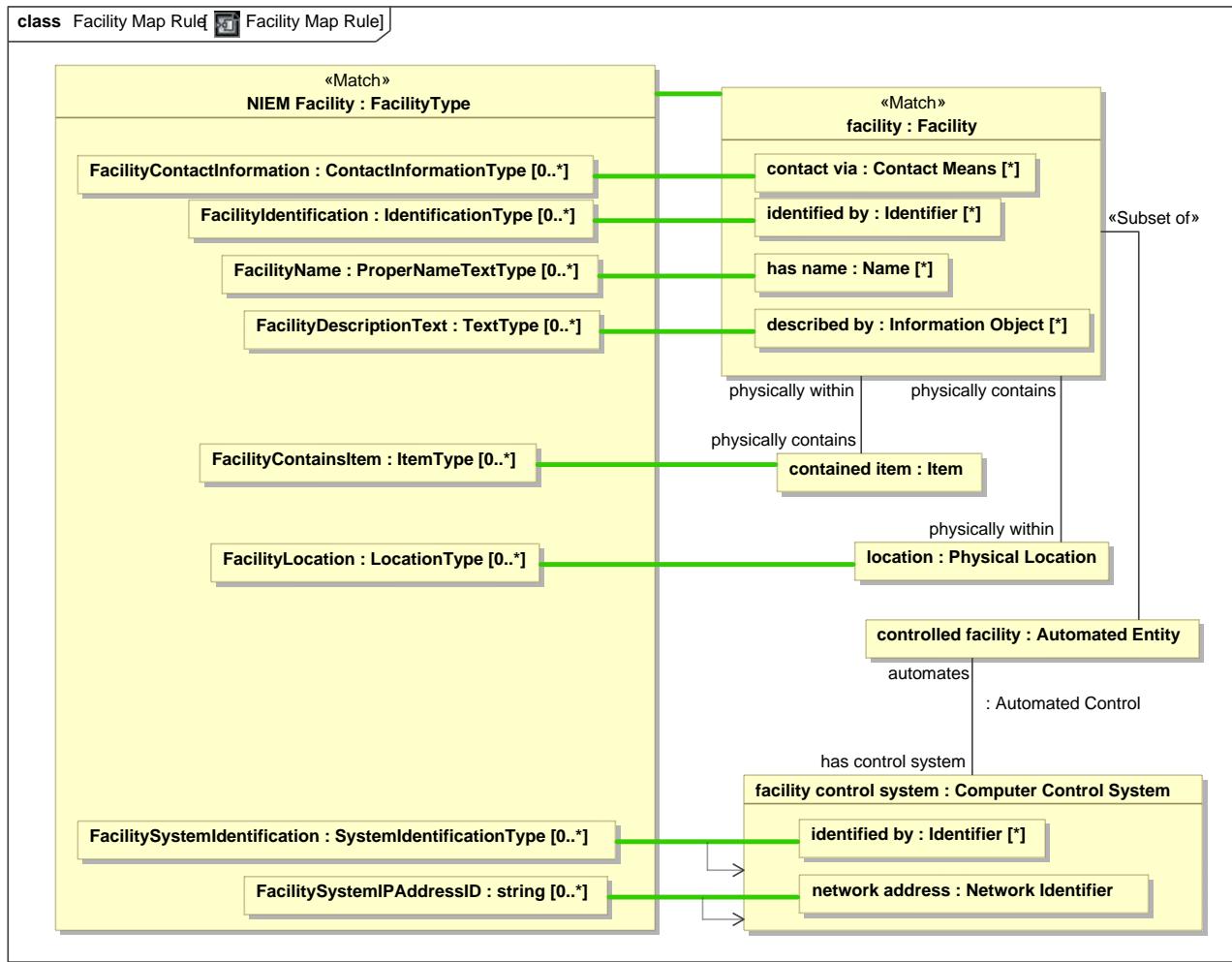


Figure 124. Facility Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location

### 10.14.5 Class Location Map Rule

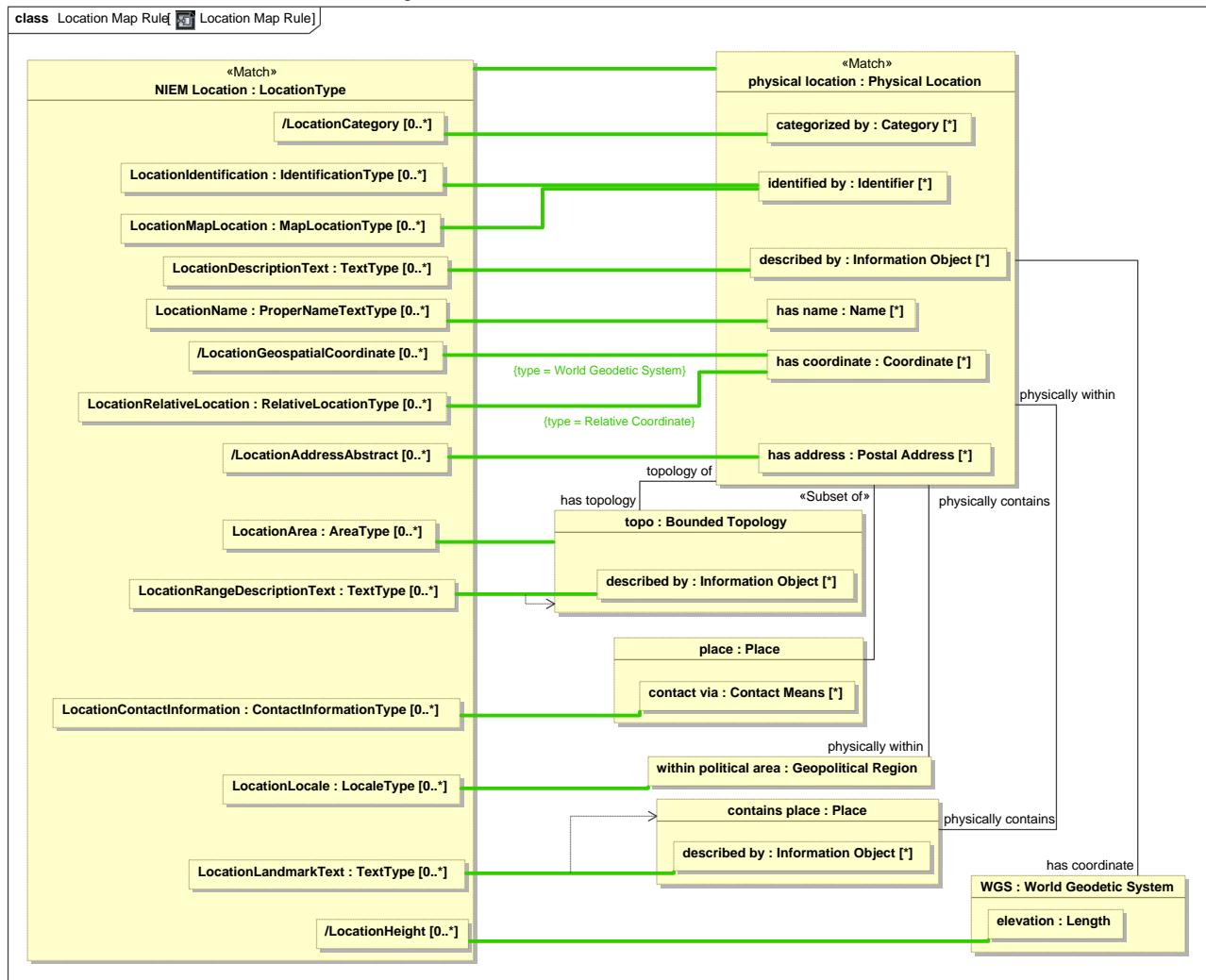


Figure 125. Location Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Location

## 10.15 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Organization

Mapping specification of NIEM Organization to the threat/risk model.

### 10.15.1 Diagram: NIEM Organization Mapping Summary

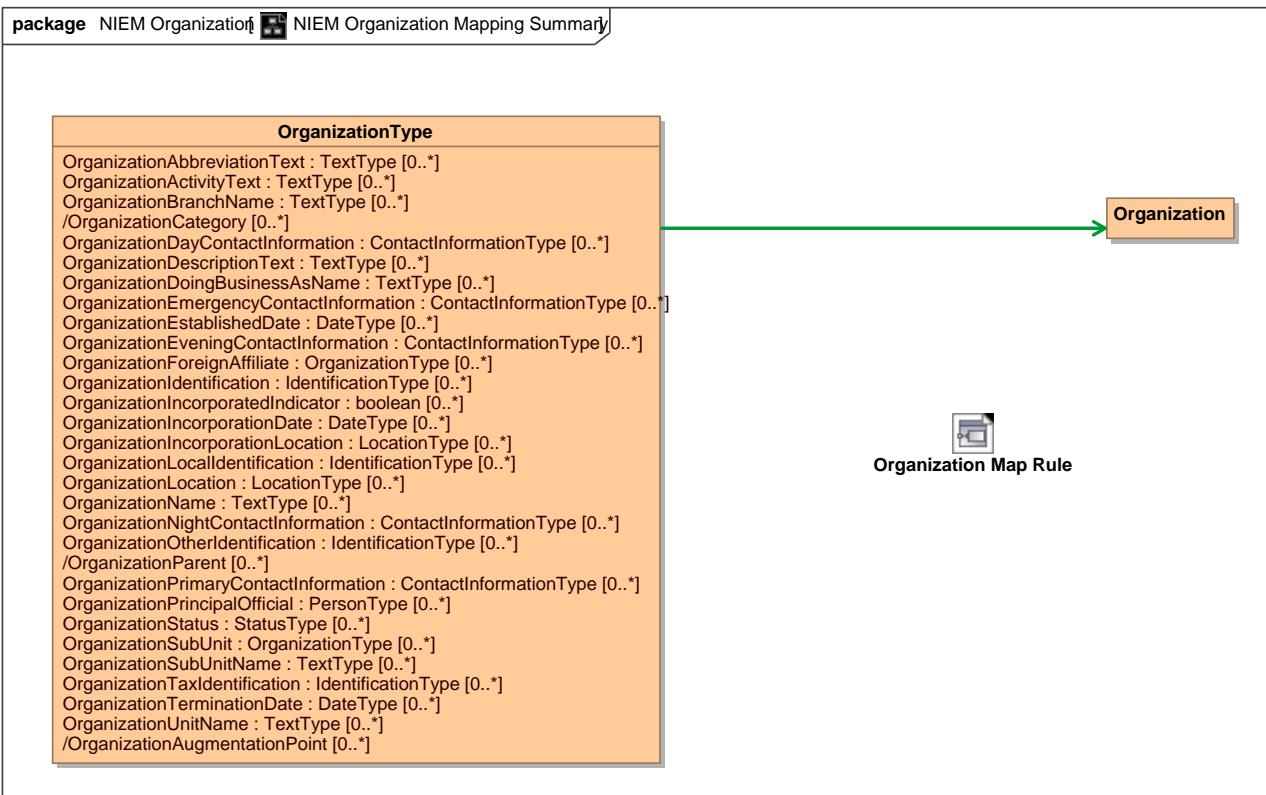


Figure 126. NIEM Organization Mapping Summary

## 10.15.2 Class Organization Map Rule

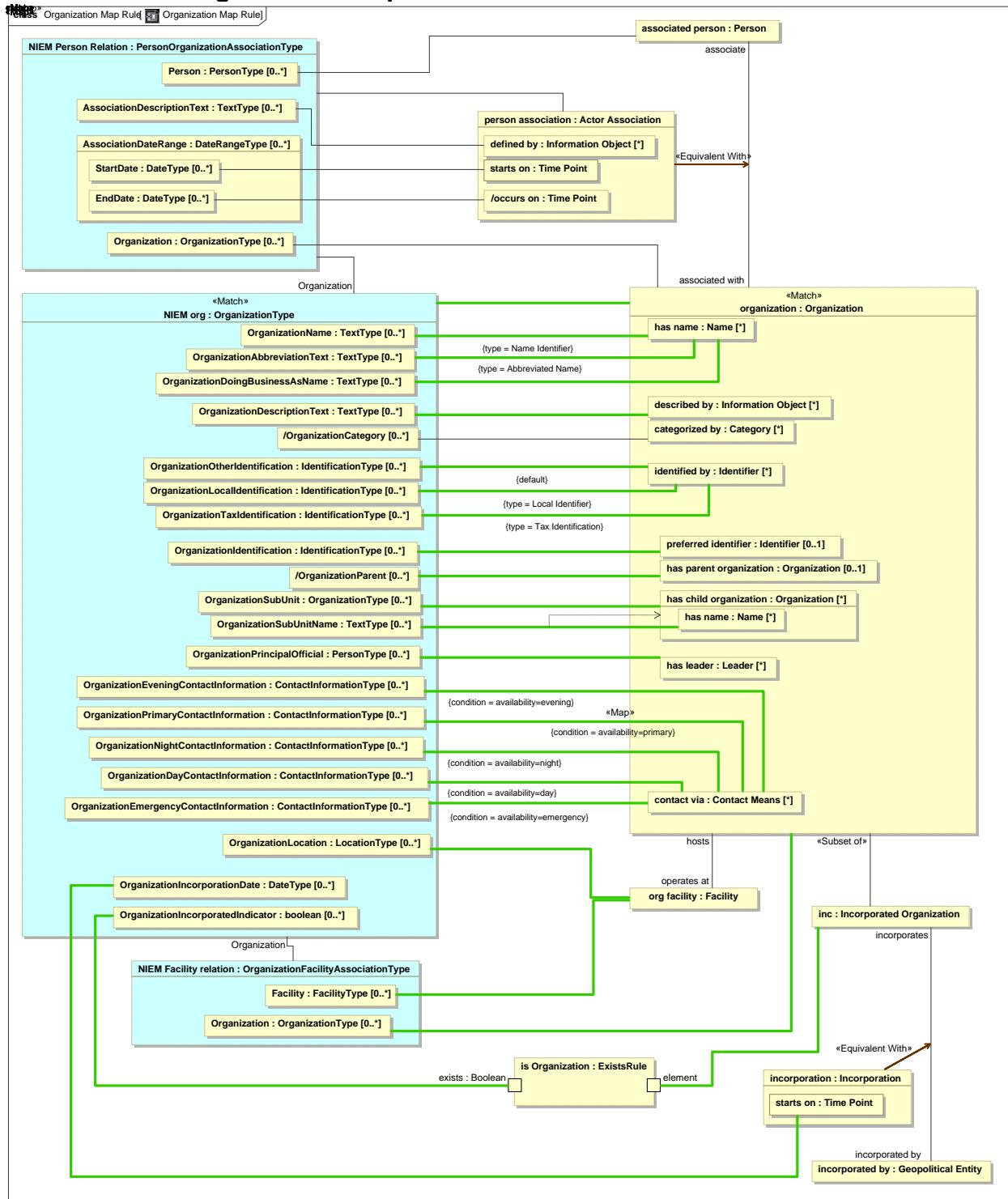


Figure 127. Organization Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Organization

## 10.16 NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Person

Mapping specification of NIEM Person to the threat/risk model.

### 10.16.1 Diagram: Person Mapping Summary

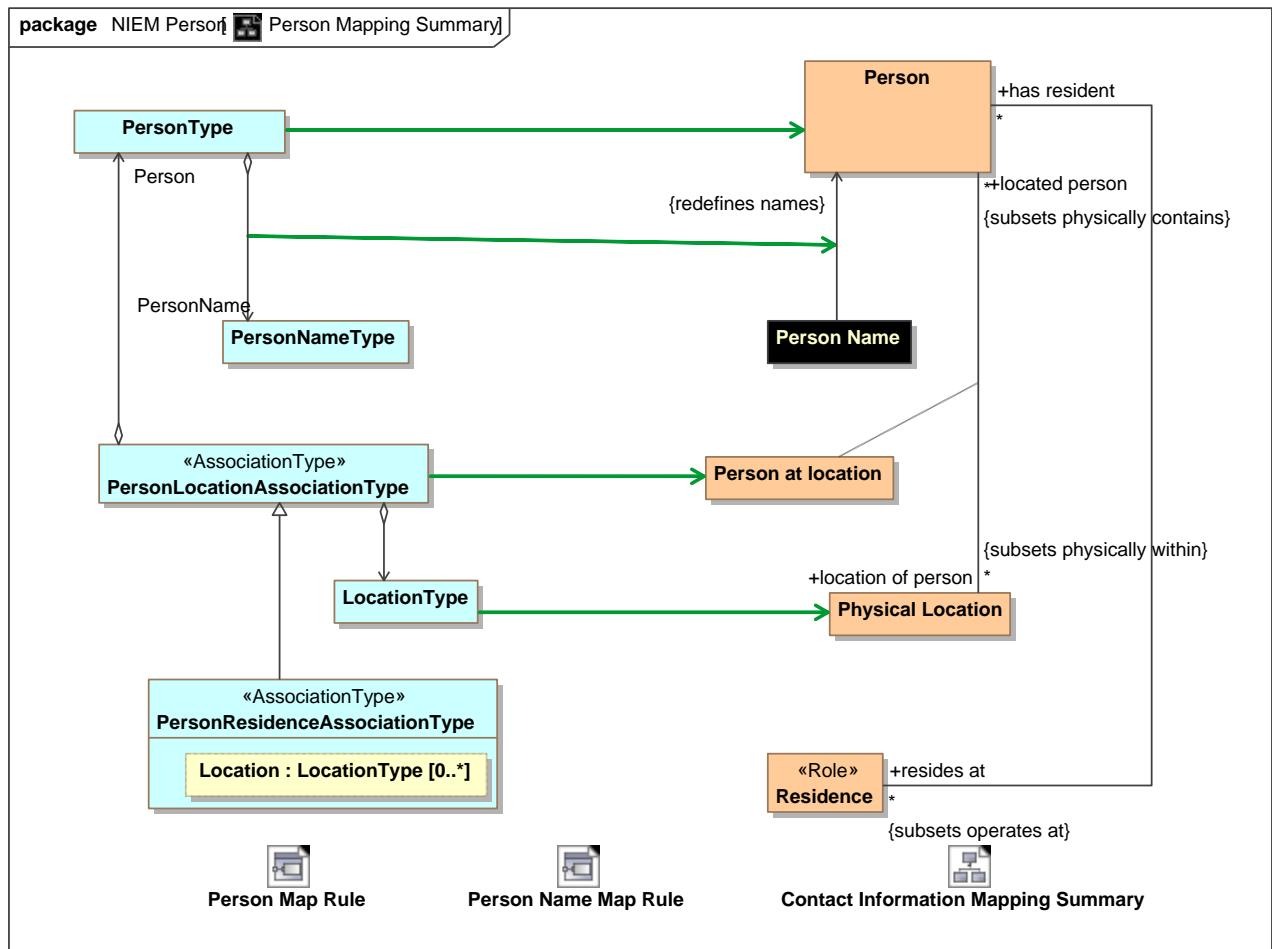


Figure 128. Person Mapping Summary

## 10.16.2 Class Person Map Rule

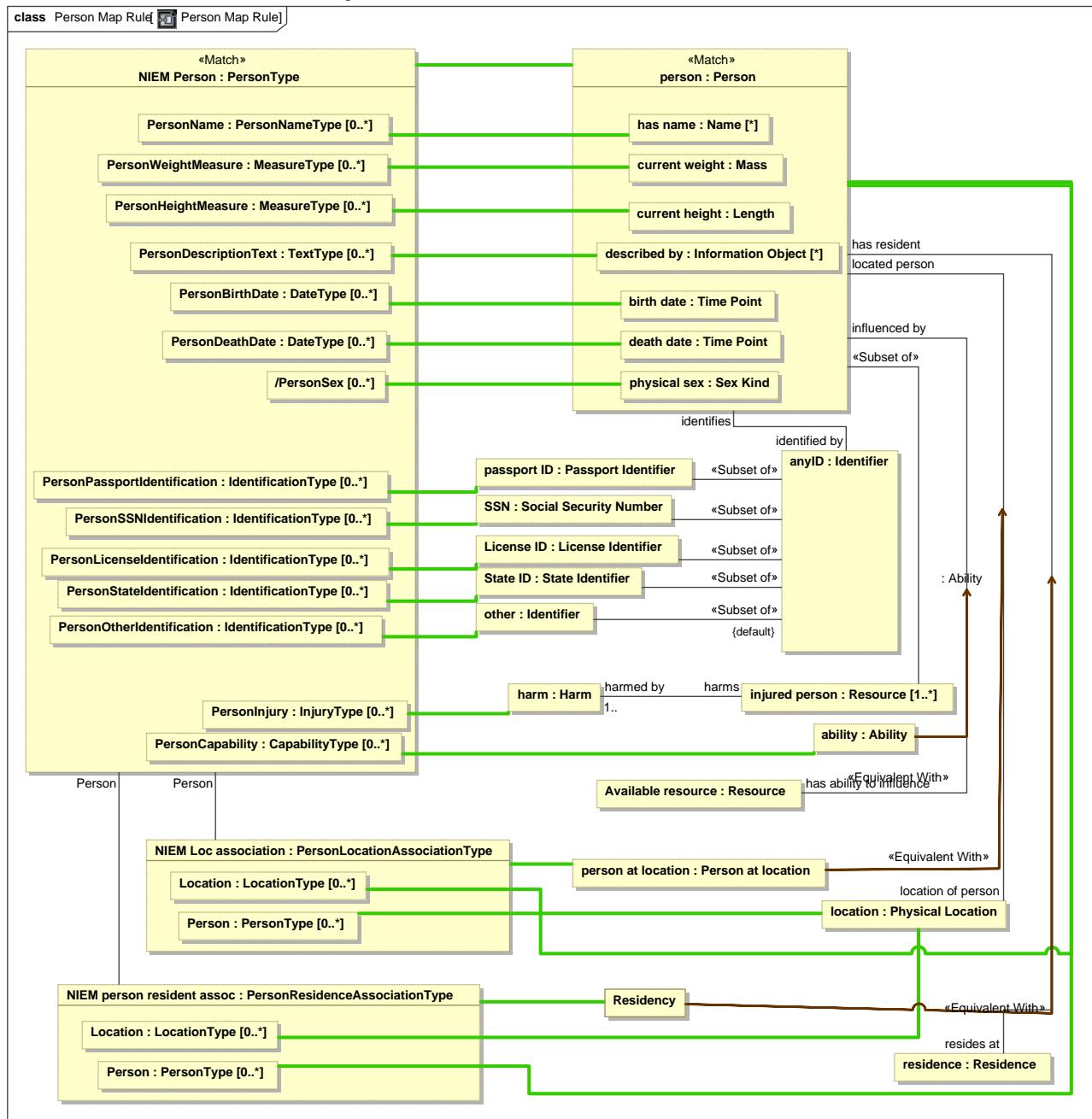


Figure 129. Person Map Rule

package NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Person

### 10.16.3 Class Person Name Map Rule

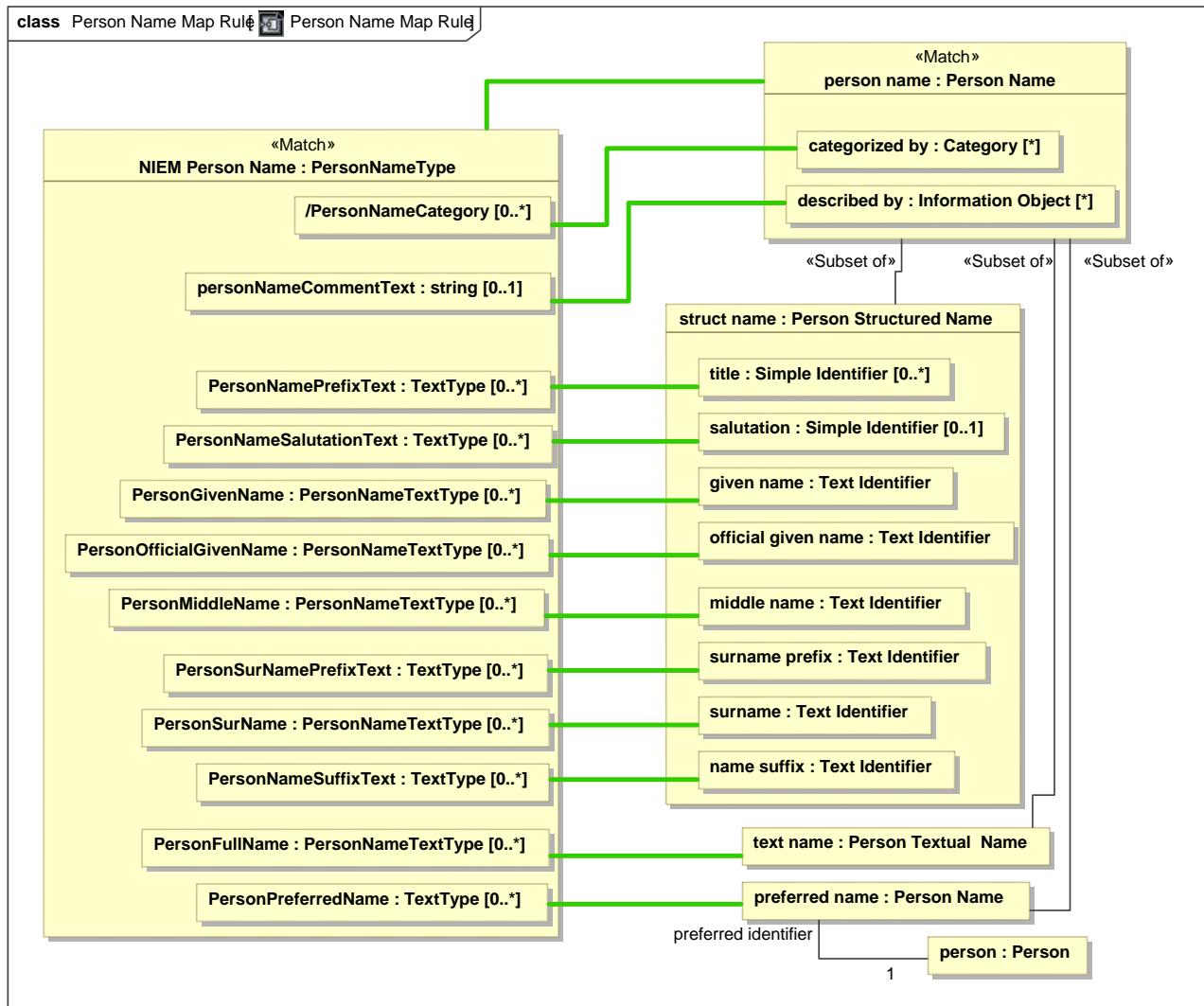


Figure 130. Person Name Map Rule

**package** NIEM Mapping to the threat / risk model::NIEM Mapping Rules and Relationships::NIEM Person

## 10.17 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.

### 10.17.1 Diagram: Primitive Type Mapping

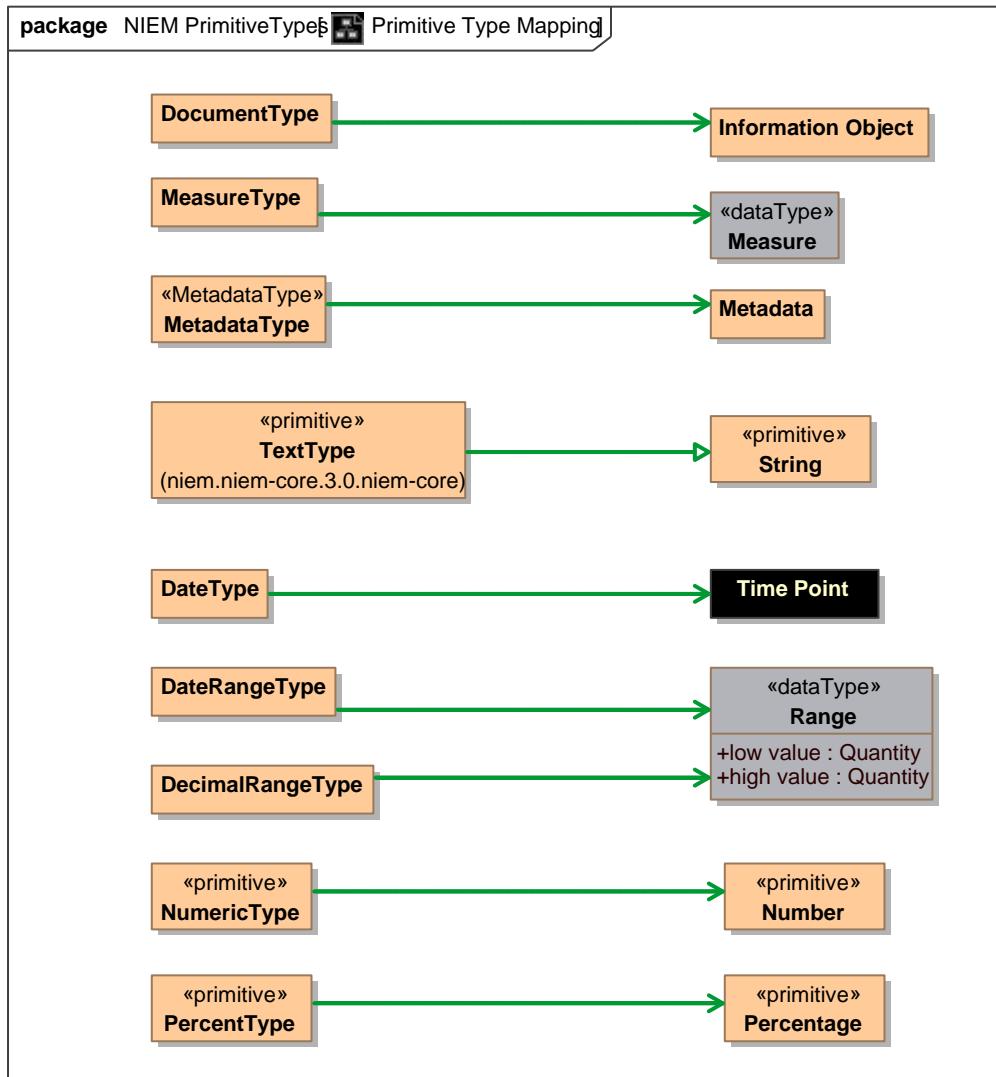


Figure 131. Primitive Type Mapping

# 11 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><b>Access Control (AC)</b></p> <p><b>ACCESS CONTROL POLICY AND PROCEDURES</b></p> <p><b>Control:</b> 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> <a href="#">Control Authority Diagram</a></p> <p> <a href="#">Subject to Authority Association Class</a></p> <p> <a href="#">Authority Class</a></p> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">provides access to Property</a></p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]Association</a></p> <p> <a href="#">Access Identifier Class</a></p> <p> <a href="#">Access Point Class</a></p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary]Association</a></p> <p> <a href="#">Association[has portal:Access Point - enters into:System]Association</a></p> <p> <a href="#">Access Complexity Enumeration</a></p> <p> <a href="#">Access Vector Enumeration</a></p>	<p>The “<u>Provides Access to</u>” property, and association entities, in relationship to “<u>Access Control</u>” family is exploited as the <b>capability</b> 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> <a href="#">Access Control Failure Class</a></p> <hr/> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]Association</a></p> <hr/> <p> <a href="#">Association[Exit Action - exit through:Access Point]Association</a></p> <hr/> <p> <a href="#">security level Property</a></p> <p> <a href="#">Communications Security Level Class</a></p> <p> <a href="#">security level Property</a></p> <p> <a href="#">Security Danger Class</a></p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">Processes Package</a></p> <p> <a href="#">Process and plans Diagram</a></p> <p> <a href="#">Process and plans Process and plansElement Value</a></p> <p> <a href="#">Process and plans Process and plansElement Value</a></p> <p> <a href="#">Invoke Process Class</a></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
<b>Access Control (AC)</b> <b>ACCESS CONTROL POLICY AND PROCEDURES</b> <u>Control:</u> The organization: a. Develops, documents, and disseminates to	<a href="#">Control Authority Diagram</a> <a href="#">Subject to Authority Association Class</a>	This control area (Access Control (AC)) of the 800.53 controls map to the Authority Class of the Threat and Risk Conceptual Model. The Control Authority, Security and Policy Classes and Property of the model address the

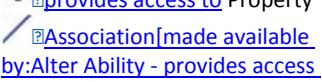
<p><b>[Assignment: organization-defined personnel or roles]:</b></p> <p>1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current:</p> <p>1. Access control policy <b>[Assignment: organization-defined frequency]</b>; and</p> <p>2. Access control procedures <b>[Assignment: organization-defined frequency]</b>.</p>	<p> <a href="#">Authority Class</a></p> <hr/> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">provides access to Property</a></p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity] Association</a></p> <hr/> <p> <a href="#">Access Identifier Class</a></p> <p> <a href="#">Access Point Class</a></p> <hr/> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary] Association</a></p> <p> <a href="#">Association[has portal:Access Point - enters into:System] Association</a></p> <p> <a href="#">Access Complexity Enumeration</a></p> <p> <a href="#">Access Vector Enumeration</a></p> <p> <a href="#">Access Control Failure Class</a></p> <hr/> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point] Association</a></p> <p> <a href="#">Association[Exit Action - exit through:Access Point] Association</a></p> <hr/> <p> <a href="#">security levelProperty</a></p> <p> <a href="#">Communications Security Level Class</a></p> <p> <a href="#">security levelProperty</a></p> <p> <a href="#">Security Danger Class</a></p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">Processes Package</a></p> <p> <a href="#">Process and plans Diagram</a></p> <p> <a href="#">Process and plans Element Value</a></p> <p> <a href="#">Process and plans Process and</a></p>	<p>assignment of the access authority and policies /procedures to facilitate the access or the prevention of access to organizational entities.</p>
---	--	---

	<p><b>plansElement Value</b></p>  <a href="#">Invoke Process Class</a>	
<p><b>Awareness and Training (AT)</b></p> <p>SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES</p> <p><b>Control:</b> The organization:</p> <p>a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b>:</p> <ol style="list-style-type: none"> <li>1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and</li> </ol> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> <li>1. Security awareness and training policy <b>[Assignment: organization-defined frequency]</b>; and</li> <li>2. Security awareness and training procedures <b>[Assignment: organization-defined frequency]</b>.</li> </ol>	<p> <a href="#">Observation Package</a></p> <p> <a href="#">Observation Diagram</a></p> <p> <a href="#">Observation Class</a></p> <p> <a href="#">Observation Tool Class</a></p> <hr/> <p> <a href="#">performs observation Property</a></p> <p> <a href="#">observation Property</a></p> <hr/> <p> <a href="#">Contact Information Package</a></p> <p> <a href="#">Contact Information Diagram</a></p> <p> <a href="#">Contact Information Association Class</a></p> <p> <a href="#">Contact Means Class</a></p> <p> <a href="#">contact for Property</a></p> <hr/> <p> <a href="#">Control Authority Diagram</a></p> <p> <a href="#">Subject to Authority Association Class</a></p> <p> <a href="#">Authority Class</a></p> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">provides access to Property</a></p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]Association</a></p> <p> <a href="#">Access Identifier Class</a></p> <p> <a href="#">Access Point Class</a></p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary]Association</a></p> <p> <a href="#">Association[has portal:Access Point - enters into:System]Association</a></p> <p> <a href="#">Access Complexity Enumeration</a></p>	<p>This control area (<b>Awareness and Training (AT)</b>) of the 800.53 controls map to the <b>Observation Class</b> and Basic Packages (<b>Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning</b>) in the Threat and Risk Conceptual Model. The <b>Observation package, and Contact Information Package</b> of <i>classes and properties</i> address the responsibility, information and coordination among organizational entities for <b>SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES</b>.</p> <p>.</p>

	<p> <a href="#">Access Vector</a> Enumeration</p> <p> <a href="#">Access Control Failure</a> Class</p> <hr/> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a> Association</p> <p> <a href="#">Association[Exit Action - exit through:Access Point]</a> Association</p> <hr/> <p> <a href="#">security level</a> Property</p> <p> <a href="#">Communications Security Level</a> Class</p> <p> <a href="#">security level</a> Property</p> <p> <a href="#">Security Danger</a> Class</p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy</a> Class</p> <hr/> <p> <a href="#">Processes</a> Package</p> <p> <a href="#">Process and plans</a> Diagram</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Invoke Process</a> Class</p>	
<p><b>Audit and Accountability (AU)</b></p> <p>AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES</p> <p><u>Control:</u> The organization:</p> <p>a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]:</b></p> <p>1. An audit and accountability 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 audit and accountability policy and associated audit and accountability controls; and</p> <p>b. Reviews and updates the current:</p>	<p><a href="#">Observation</a> Package</p> <p> <a href="#">Observation</a> Diagram</p> <p> <a href="#">Observation</a> Class</p> <p> <a href="#">Observation Tool</a> Class</p> <p> <a href="#">performs observation</a> Property</p> <p> <a href="#">observation</a> Property</p> <hr/> <p> <a href="#">Control Authority</a> Diagram</p> <p> <a href="#">Subject to Authority</a> Association Class</p>	<p>This control area (<b>Audit and Accountability (AU)</b>) of the 800.53 controls maps to the packages, <b>Control Authority</b>, <b>Provides Access</b>, <b>Security Level</b>, <b>Asserting Policy</b>, <b>Process and Planning</b> and <b>Observation Package</b> of the Threat and Risk Conceptual Model. The <b>Observation package and Contact Information Package</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for <b>AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES</b>.</p>

<p>1. Audit and accountability policy [<b>Assignment: organization-defined frequency</b>]; and</p> <p>2. Audit and accountability procedures [<b>Assignment: organization-defined frequency</b>].</p>	<p> <a href="#">Authority Class</a></p> <hr/> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">provides access to Property</a></p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity] Association</a></p> <p> <a href="#">Access Identifier Class</a></p> <p> <a href="#">Access Point Class</a></p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary] Association</a></p> <p> <a href="#">Association[has portal:Access Point - enters into:System] Association</a></p> <p> <a href="#">Access Complexity Enumeration</a></p> <p> <a href="#">Access Vector Enumeration</a></p> <p> <a href="#">Access Control Failure Class</a></p> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point] Association</a></p> <p> <a href="#">Association[Exit Action - exit through:Access Point] Association</a></p> <hr/> <p> <a href="#">security level Property</a></p> <p> <a href="#">Communications Security Level Class</a></p> <p> <a href="#">security level Property</a></p> <p> <a href="#">Security Danger Class</a></p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">Processes Package</a></p> <p> <a href="#">Process and plans Diagram</a></p> <p> <a href="#">Process and plans Element Value</a></p> <p> <a href="#">Process and plans Process and plans</a></p>
---	--

	<p><i>plansElement</i> Value</p>  <a href="#">Invoke Process Class</a>	
<p><b>Security Assessment and Authorization (CA)</b></p> <p>SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b>:</p> <ol style="list-style-type: none"> <li>1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and</li> </ol> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> <li>1. Security assessment and authorization policy <b>[Assignment: organization-defined frequency]</b>; and</li> <li>2. Security assessment and authorization procedures <b>[Assignment: organization-defined frequency]</b>.</li> </ol>	<p> <a href="#">Control Authority Diagram</a></p> <p> <a href="#">Subject to Authority Association Class</a></p> <p> <a href="#">Authority Class</a></p> <hr/> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">provides access to Property</a></p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]Association</a></p> <p> <a href="#">Access Identifier Class</a></p> <p> <a href="#">Access Point Class</a></p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary]Association</a></p> <p> <a href="#">Association[has portal:Access Point - enters into:System]Association</a></p> <p> <a href="#">Access Complexity Enumeration</a></p> <p> <a href="#">Access Vector Enumeration</a></p> <p> <a href="#">Access Control Failure Class</a></p> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]Association</a></p> <p> <a href="#">Association[Exit Action - exit through:Access Point]Association</a></p> <hr/> <p> <a href="#">security level Property</a></p> <p> <a href="#">Communications Security Level Class</a></p> <p> <a href="#">security level Property</a></p> <p> <a href="#">Security Danger Class</a></p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p>	<p>This control area (<b>Security Assessment and Authorization (CA)</b>) of the 800.53 maps to the packages, <b>Control Authority</b>, <b>Provides Access</b>, <b>Security Level</b>, <b>Asserting Policy</b>, <b>Process and Planning</b> and <b>Assessment</b> areas of the Threat and Risk Conceptual Model. The <b>Control Authority</b>, <b>Asserting Policy</b> and <b>Assessment Package</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES</b>.</p> <p>.</p>

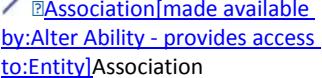
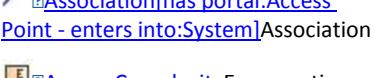
	 <a href="#">Policy Class</a> <hr/>  <a href="#">Assessment Package</a>  <a href="#">Assessment Diagram</a>  <a href="#">has assessment Property</a>  <a href="#">Assessment Activity Class</a>  <a href="#">Assessment Report Class</a>  <a href="#">assessment of Property</a>  <a href="#">assessment score Property</a>   <a href="#">Processes Package</a>  <a href="#">Process and plans Diagram</a>  <a href="#">Process and plans Element Value</a>  <a href="#">Process and plans Value</a>  <a href="#">Invoke Process Class</a>	
<b>Configuration Management (CM)</b> CONFIGURATION MANAGEMENT POLICY AND PROCEDURES  Control: The organization:  a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b> :  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  b. Reviews and updates the current:  1. Configuration management policy <b>[Assignment: organization-defined frequency]</b> ; and  2. Configuration management procedures <b>[Assignment: organization-defined frequency]</b> .	 <a href="#">Control Authority Diagram</a>  <a href="#">Subject to Authority Association Class</a>  <a href="#">Authority Class</a>  <a href="#">has authority over Property</a> <hr/>  <a href="#">provides access to Property</a>  <a href="#">Association[made available by:Alter Ability - provides access to:Entity]Association</a>  <a href="#">Access Identifier Class</a>  <a href="#">Access Point Class</a>  <a href="#">Association[has opening:Access Point - enters through:Boundary]Association</a>  <a href="#">Association[has portal:Access Point - enters into:System]Association</a>  <a href="#">Access Complexity Enumeration</a>	This control area ( <b>Configuration Management (CM)</b> ) of the 800.53 controls maps to the packages, <b>Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning</b> and Patterns of the Threat and Risk Conceptual Model. The <b>Control Authority, Asserting Policy and Assessment Package</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES</b> .

	<p> <a href="#">Access Vector</a>Enumeration</p> <p> <a href="#">Access Control Failure</a>Class</p> <hr/> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a>Association</p> <p> <a href="#">Association[Exit Action - exit through:Access Point]</a>Association</p> <hr/> <p> <a href="#">security level</a>Property</p> <p> <a href="#">Communications Security Level</a>Class</p> <p> <a href="#">security level</a>Property</p> <p> <a href="#">Security Danger</a>Class</p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy</a> Class</p> <hr/> <p> <a href="#">Assessment</a> Package</p> <p> <a href="#">Assessment Diagram</a></p> <p> <a href="#">has assessment</a> Property</p> <p> <a href="#">Assessment Activity</a> Class</p> <p> <a href="#">Assessment Report</a> Class</p> <p> <a href="#">assessment of</a> Property</p> <p> <a href="#">assessment score</a> Property</p> <hr/> <p> <a href="#">Patterns</a> Package</p> <p> <a href="#">Patterns Diagram</a></p> <p> <a href="#">Patterning Generalization Set</a></p> <p> <a href="#">Pattern Involvement</a> Class</p> <p> <a href="#">Situation Pattern</a> Class</p> <p> <a href="#">Indicator Pattern</a> Class</p> <p> <a href="#">ObservablePatternFacade</a> Class</p> <hr/> <p> <a href="#">Processes</a> Package</p>	
--	--	--

	<a href="#">Process and plans</a> Diagram <a href="#">Process and plans</a> Process and plansElement Value <a href="#">Process and plans</a> Process and plansElement Value <a href="#">Invoke Process</a> Class	
<b>Contingency Planning (CP)</b> CONTINGENCY PLANNING POLICY AND PROCEDURES  Control: The organization:  a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b> :  1. A contingency 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 contingency planning policy and associated contingency planning controls; and  b. Reviews and updates the current:  1. Contingency planning policy <b>[Assignment: organization-defined frequency]</b> ; and  2. Contingency planning procedures <b>[Assignment: organization-defined frequency]</b> .	<a href="#">Control Authority</a> Diagram <a href="#">Subject to Authority</a> Association Class <a href="#">Authority</a> Class <a href="#">has authority over</a> Property <hr/> <a href="#">provides access to</a> Property <a href="#">Association[made available by:Alter Ability - provides access to:Entity]</a> Association <a href="#">Access Identifier</a> Class <a href="#">Access Point</a> Class <a href="#">Association[has opening:Access Point - enters through:Boundary]</a> Association <a href="#">Association[has portal:Access Point - enters into:System]</a> Association <a href="#">Access Complexity</a> Enumeration <a href="#">Access Vector</a> Enumeration <a href="#">Access Control Failure</a> Class <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a> Association <a href="#">Association[Exit Action - exit through:Access Point]</a> Association <hr/> <a href="#">security level</a> Property <a href="#">Communications Security Level</a> Class <a href="#">security level</a> Property	This control area ( <b>Contingency Planning (CP)</b> ) of the 800.53 controls maps to the packages, <b>Control Authority</b> , <b>Provides Access</b> , <b>Security Level</b> , <b>Asserting Policy</b> , <b>Process and Planning and Assessment areas</b> of the Threat and Risk Conceptual Model. The <b>Control Authority</b> , <b>Asserting Policy and Assessment Package</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES</b> .

	 <a href="#">Security Danger</a> Class <hr/>  <a href="#">Asserting Policy</a> Association  <a href="#">Policy</a> Diagram  <a href="#">Policy</a> Class <hr/>  <a href="#">Assessment</a> Package  <a href="#">Assessment</a> Diagram  <a href="#">has assessment</a> Property  <a href="#">Assessment Activity</a> Class  <a href="#">Assessment Report</a> Class  <a href="#">assessment of</a> Property  <a href="#">assessment score</a> Property <hr/>  <a href="#">Incident</a> Package  <a href="#">Incident</a> Diagram  <a href="#">Incident</a> Class <hr/>  <a href="#">Processes</a> Package  <a href="#">Process and plans</a> Diagram  <a href="#">Process and plans</a> Process and plansElement Value  <a href="#">Process and plans</a> Process and plansElement Value  <a href="#">Invoke Process</a> Class	
<b>Identification and Authentication (IA)</b> IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b> : 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	 <a href="#">Control Authority</a> Diagram  <a href="#">Subject to Authority</a> Association Class  <a href="#">Authority</a> Class  <a href="#">has authority over</a> Property <hr/>  <a href="#">provides access to</a> Property  <a href="#">Association[made available]</a>	<b>Identification and Authentication (IA)</b> of the 800.53 controls maps to the packages, <b>Control Authority</b> , <b>Provides Access</b> , <b>Security Level</b> , <b>Asserting Policy</b> , <b>Process and Planning</b> , and <b>Contact Information</b> of the Threat and Risk Conceptual Model. The <b>Contact Information</b> , <b>Control Authority</b> , <b>Asserting Policy Package</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>IDENTIFICATION AND AUTHENTICATION</b>

<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"> <li>1. Identification and authentication policy <b>[Assignment: organization-defined frequency]</b>; and</li> <li>2. Identification and authentication procedures <b>[Assignment: organization-defined frequency]</b>.</li> </ol>	<p><a href="#">by:Alter Ability - provides access to:Entity</a>Association</p>  <a href="#">Access Identifier</a> Class  <a href="#">Access Point</a> Class <hr/>  <a href="#">Association[has opening:Access Point - enters through:Boundary]</a> Association  <a href="#">Association[has portal:Access Point - enters into:System]</a> Association  <a href="#">Access Complexity</a> Enumeration  <a href="#">Access Vector</a> Enumeration  <a href="#">Access Control Failure</a> Class <hr/>  <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a> Association  <a href="#">Association[Exit Action - exit through:Access Point]</a> Association <hr/>  <a href="#">security level</a> Property  <a href="#">Communications Security Level</a> Class  <a href="#">security level</a> Property  <a href="#">Security Danger</a> Class <hr/> <p><a href="#">Asserting Policy Association</a></p>  <a href="#">Policy Diagram</a>  <a href="#">Policy</a> Class <hr/>  <a href="#">Processes</a> Package  <a href="#">Process and plans</a> Diagram  <a href="#">Process and plans</a> Process and plansElement Value  <a href="#">Process and plans</a> Process and plansElement Value  <a href="#">Invoke Process</a> Class <hr/>  <a href="#">Contact Information</a> Package	<p><b>POLICY AND PROCEDURES.</b></p>
--	---	--------------------------------------

	<p> <a href="#">Contact Information</a> Diagram</p> <p> <a href="#">Contact Information</a> Association Class</p> <p> <a href="#">Contact Means</a> Class</p> <p> <a href="#">contact for</a> Property</p> <p> <a href="#">Contactable</a> Class</p> <p> <a href="#">contact via</a> Property</p>	
<b>Incident Response (IR)</b> Control: The organization:	<p>a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:</p> <ol style="list-style-type: none"> <li>1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and</li> </ol> <p>b. Reviews and updates the current:</p> <ol style="list-style-type: none"> <li>1. Incident response policy [Assignment: organization-defined frequency]; and</li> <li>2. Incident response procedures [Assignment: organization-defined frequency].</li> </ol>	<p> <a href="#">Control Authority</a> Diagram</p> <p> <a href="#">Subject to Authority</a> Association Class</p> <p> <a href="#">Authority</a> Class</p> <p> <a href="#">has authority over</a> Property</p> <hr/> <p> <a href="#">provides access to</a> Property</p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]</a> Association</p> <p> <a href="#">Access Identifier</a> Class</p> <p> <a href="#">Access Point</a> Class</p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary]</a> Association</p> <p> <a href="#">Association[has portal:Access Point - enters into:System]</a> Association</p> <p> <a href="#">Access Complexity</a> Enumeration</p> <p> <a href="#">Access Vector</a> Enumeration</p> <p> <a href="#">Access Control Failure</a> Class</p> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a> Association</p> <p> <a href="#">Association[Exit Action - exit through:Access Point]</a> Association</p> <hr/> <p> <a href="#">security level</a> Property</p>

	<p> <a href="#">Communications Security LevelClass</a></p> <p> <a href="#">security levelProperty</a></p> <p> <a href="#">Security DangerClass</a></p> <hr/> <p> <a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">Incident Package</a></p> <p> <a href="#">Incident Diagram</a></p> <p> <a href="#">Incident Class</a></p> <hr/> <p> <a href="#">Situation Package</a></p> <p> <a href="#">Situation Diagram</a></p> <p> <a href="#">Situation ClassificationGeneralization Set</a></p> <p> <a href="#">Situation Class</a></p> <p> <a href="#">Actual SituationClass</a></p> <p> <a href="#">Current Situation Class</a></p> <p> <a href="#">Past Situation Class</a></p> <p> <a href="#">Potential Situation Class</a></p> <p> <a href="#">Risky Situation Class</a></p>	
<p><b>Maintenance (MA)</b></p> <p>SYSTEM MAINTENANCE POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b>:</p> <p>1. A system maintenance 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 system maintenance policy and associated system maintenance controls; and</p> <p>b. Reviews and updates the current:</p>	<p> <a href="#">Control Authority Diagram</a></p> <p> <a href="#">Subject to Authority Association Class</a></p> <p> <a href="#">Authority Class</a></p> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">Provides access to Property</a></p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]Association</a></p> <p> <a href="#">Access IdentifierClass</a></p>	<p>This control area (<b>Maintenance (MA)</b>) of the 800.53 controls maps to the packages, <b>Control Authority</b>, <b>Provides Access</b>, <b>Security Level</b>, <b>Asserting Policy</b>, <b>Process and Planning</b> and <b>Mitigation Package</b> of the Threat and Risk Conceptual Model. The <b>Mitigation</b>, <b>Situation</b>, <b>Process plan and Policy Packages</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>SYSTEM MAINTENANCE POLICY AND PROCEDURES</b>.</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> <a href="#">Access PointClass</a></p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary]Association</a></p> <p> <a href="#">Association[has portal:Access Point - enters into:System]Association</a></p> <p> <a href="#">Access ComplexityEnumeration</a></p> <p> <a href="#">Access VectorEnumeration</a></p> <p> <a href="#">Access Control FailureClass</a></p> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]Association</a></p> <p> <a href="#">Association[Exit Action - exit through:Access Point]Association</a></p> <hr/> <p> <a href="#">security levelProperty</a></p> <p> <a href="#">Communications Security LevelClass</a></p> <p> <a href="#">security levelProperty</a></p> <p> <a href="#">Security DangerClass</a></p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">Mitigation ActorClass</a></p> <p> <a href="#">performs mitigationProperty</a></p> <p> <a href="#">Association[mitigated by:Mitigation Actor - performs mitigation:Safeguard Activity]Association</a></p> <p> <a href="#">Association[countermeasure for:Risk Mitigation Strategy - leverages countermeasure:Countermeasure]Association</a></p> <p> <a href="#">Risk Mitigation StrategyClass</a></p>
---	--

	<p><u>Situation Package</u></p>  <p><u>Situation Diagram</u></p>  <p><u>Situation Classification</u>Generalization Set</p>  <p><u>Situation Class</u></p>  <p><u>Actual Situation Class</u></p>  <p><u>Current Situation Class</u></p>  <p><u>Past Situation Class</u></p>  <p><u>Potential Situation Class</u></p>  <p><u>Risky Situation Class</u></p> <hr/> <p><u>Process and plans Diagram</u></p>  <p><u>Plan Class</u></p>  <p><u>Mitigation Plan Class</u></p>  <p><u>plan Property</u></p> <hr/>	
<p><b>Media Protection (MP)</b></p> <p>MEDIA PROTECTION POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b>:</p> <p>1. A media protection 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 media protection policy and associated media protection controls; and</p> <p>b. Reviews and updates the current:</p> <p>1. Media protection policy <b>[Assignment: organization-defined frequency]</b>; and</p> <p>2. Media protection procedures <b>[Assignment: organization-defined frequency]</b>.</p>	 <p><u>Control Authority Diagram</u></p>  <p><u>Subject to Authority Association Class</u></p>  <p><u>Authority Class</u></p>  <p><u>has authority over Property</u></p> <hr/>  <p><u>provides access to Property</u></p>  <p><u>Association[made available by:Alter Ability - provides access to:Entity]Association</u></p>  <p><u>Access Identifier Class</u></p>  <p><u>Access Point Class</u></p>  <p><u>Association[has opening:Access Point - enters through:Boundary]Association</u></p>  <p><u>Association[has portal:Access Point - enters into:System]Association</u></p>  <p><u>Access Complexity Enumeration</u></p>	<p>This control area (<b>Media Protection (MP)</b>) of the 800.53 controls maps to the packages, <b>Control Authority</b>, <b>Provides Access</b>, <b>Security Level</b>, <b>Asserting Policy</b>, <b>Process and Planning</b>. The <b>Security</b>, <b>Means</b>, <b>Control Authority</b>, <b>Asserting Policy and Mitigation</b>, <b>Package of classes and properties</b> address the responsibility, information and coordination among organizational entities for the <b>MEDIA PROTECTION POLICY AND PROCEDURES</b>.</p>

	<p> <a href="#">Access Vector</a>Enumeration</p> <p> <a href="#">Access Control Failure</a>Class</p> <hr/> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]Association</a></p> <p> <a href="#">Association[Exit Action - exit through:Access Point]Association</a></p> <hr/> <p> <a href="#">security level</a>Property</p> <p> <a href="#">Communications Security Level</a>Class</p> <p> <a href="#">security level</a>Property</p> <p> <a href="#">Security Danger</a>Class</p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy</a> Class</p> <hr/> <p> <a href="#">Processes</a>Package</p> <p> <a href="#">Process and plans</a>Diagram</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Invoke Process</a>Class</p> <hr/> <p> <a href="#">contact means</a>Property</p> <p> <a href="#">Contact Means</a>Class</p> <p> <a href="#">Means</a>Class</p> <hr/> <p> <a href="#">Means to end</a>Association</p> <hr/> <p> <a href="#">Mitigation</a> Package</p> <p> <a href="#">Mitigation</a> Diagram</p> <p> <a href="#">Mitigation</a> Class</p> <p> <a href="#">Mitigation Activity</a> Class</p> <p> <a href="#">Mitigation Actor</a> Class</p>
--	---

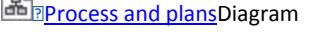
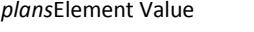
	<ul style="list-style-type: none"> <li> <a href="#">performs mitigation</a> Property</li> <li> <a href="#">Mitigation Plan</a> Class</li> <li> <a href="#">mitigation</a> Property</li> </ul>	
<b>Physical and Environmental Protection (PE)</b> <b>PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES</b> Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 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 b. Reviews and updates the current: 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency].	<ul style="list-style-type: none"> <li> <a href="#">Control Authority</a> Diagram</li> <li> <a href="#">Subject to Authority</a> Association Class</li> <li> <a href="#">Authority</a> Class</li> <li> <a href="#">has authority over</a> Property</li> </ul> <hr/> <ul style="list-style-type: none"> <li> <a href="#">provides access to</a> Property</li> <li> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]</a> Association</li> <li> <a href="#">Access Identifier</a> Class</li> <li> <a href="#">Access Point</a> Class</li> <li> <a href="#">Association[has opening:Access Point - enters through:Boundary]</a> Association</li> <li> <a href="#">Association[has portal:Access Point - enters into:System]</a> Association</li> <li> <a href="#">Access Complexity</a> Enumeration</li> <li> <a href="#">Access Vector</a> Enumeration</li> <li> <a href="#">Access Control Failure</a> Class</li> <li> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a> Association</li> <li> <a href="#">Association[Exit Action - exit through:Access Point]</a> Association</li> </ul> <hr/> <ul style="list-style-type: none"> <li> <a href="#">security level</a> Property</li> <li> <a href="#">Communications Security Level</a> Class</li> <li> <a href="#">security level</a> Property</li> <li> <a href="#">Security Danger</a> Class</li> </ul> <hr/> <a href="#">Asserting Policy Association</a>	This control area ( <b>Physical and Environmental Protection (PE)</b> ) of the 800.53 controls maps to the packages, <b>Control Authority</b> , <b>Provides Access</b> , <b>Security Level</b> , <b>Asserting Policy</b> , <b>Process and Planning</b> and <b>Physical Entity</b> . The <b>Physical Entity</b> , <b>Means</b> , and <b>Control Authority package</b> of <i>classes and properties</i> address the responsibility, information and coordination among organizational entities for the <b>PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES</b> .

	<p> <a href="#">Policy Diagram</a></p> <hr/> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">contact meansProperty</a></p> <p> <a href="#">Contact MeansClass</a></p> <p> <a href="#">MeansClass</a></p> <p> <a href="#">Means to end Association</a></p> <hr/> <p> <a href="#">Mitigation Package</a></p> <p> <a href="#">Mitigation Diagram</a></p> <p> <a href="#">Mitigation Class</a></p> <p> <a href="#">Mitigation Activity Class</a></p> <p> <a href="#">Mitigation Actor Class</a></p> <p> <a href="#">performs mitigation Property</a></p> <p> <a href="#">Mitigation Plan Class</a></p> <p> <a href="#">mitigation Property</a></p> <hr/> <p> <a href="#">Physical Entity DetailDiagram</a></p> <p> <a href="#">Physical VulnerabilityProperty</a></p> <p> <a href="#">physically containsProperty</a></p> <p> <a href="#">physically withinProperty</a></p> <p> <a href="#">Association[physically within:Physical Entity - physically contains:Physical Entity]Association</a></p> <p> <a href="#">Association[Physical Entity - Physical Vulnerability]Association</a></p> <p> <a href="#">Physical ToolClass</a></p> <p> <a href="#">Physical WeaponClass</a></p> <p> <a href="#">Physical LocationProperty</a></p> <p> <a href="#">Physical LocationClass</a></p> <p> <a href="#">Association[location designation:Location Identifier - designates location:Physical Location]Association</a></p>
--	--

	<p> <a href="#">Association[address of:Physical Location - has address:Postal Address]Association</a></p> <p> <a href="#">Association[Physical Location - has coordinate:Coordinate]Association</a></p> <p> <a href="#">Association[Relative Coordinate - relative to:Physical Location]Association</a></p> <p> <a href="#">Association[bounds region:Bounded Topology - bounded by:Physical Location]Association</a></p> <p> <a href="#">Association[relocated by:Relocation - relocates:Physical Entity]Association</a></p> <p> <a href="#">Association[loses via:Relocation - from location:Physical Location]Association</a></p> <p> <a href="#">Association[moved via:Relocation - to location:Physical Location]Association</a></p> <p><a href="#">Association[topology of:Physical Location - has topology:Topology]Association</a></p> <p> <a href="#">Geophysical DangerClass</a></p> <p> <a href="#">Physical System FailureClass</a></p> <p> <a href="#">Physical VulnerabilityClass</a></p> <p> <a href="#">Physical EntityProperty</a></p>	
<b>Planning (PL)</b>  SECURITY PLANNING POLICY AND PROCEDURES  Control: The organization:  a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b> :  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  b. Reviews and updates the current:  1. Security planning policy <b>[Assignment: organization-defined frequency]</b> ; and  2. Security planning procedures <b>[Assignment:</b>	<p> <a href="#">Control Authority Diagram</a></p> <p> <a href="#">Subject to Authority Association Class</a></p> <p> <a href="#">Authority Class</a></p> <hr/> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">provides access to Property</a></p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]Association</a></p> <p> <a href="#">Access IdentifierClass</a></p> <p> <a href="#">Access PointClass</a></p> <p> <a href="#">Association[has opening:Access</a></p>	This control area <b>Planning (PL)</b> of the 800.53 controls maps to the packages, <b>Control Authority</b> , <b>Provides Access</b> , <b>Security Level</b> , <b>Asserting Policy</b> , <b>Process and Planning</b> and <b>Mitigation and (Methods of Contact) and Assessment areas</b> of the Threat and Risk Conceptual Model. The <b>Security</b> , <b>Mitigation</b> , <b>Means</b> , <b>Control Authority</b> , <b>Asserting Policy</b> and <b>Assessment Package</b> of <i>classes and properties</i> address the responsibility, information and coordination among organizational entities for the <b>SECURITY PLANNING POLICY AND PROCEDURES</b> .

<p><i>organization-defined frequency].</i></p>	<p><u>Point - enters through:Boundary</u>Association</p> <p> <a href="#">Association[has portal:Access Point - enters into:System]</a>Association</p> <p> <a href="#">Access Complexity</a>Enumeration</p> <p> <a href="#">Access Vector</a>Enumeration</p> <p> <a href="#">Access Control Failure</a>Class</p> <hr/> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a>Association</p> <p> <a href="#">Association[Exit Action - exit through:Access Point]</a>Association</p> <hr/> <p> <a href="#">security level</a>Property</p> <p> <a href="#">Communications Security Level</a>Class</p> <p> <a href="#">security level</a>Property</p> <p> <a href="#">Security Danger</a>Class</p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">Processes</a>Package</p> <p> <a href="#">Process and plans</a>Diagram</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Invoke Process</a>Class</p> <hr/> <p> <a href="#">Mitigation</a> Package</p> <p> <a href="#">Mitigation Diagram</a></p> <p> <a href="#">Mitigation Class</a></p> <p> <a href="#">Mitigation Activity</a> Class</p> <p> <a href="#">Mitigation Actor</a> Class</p>
--	--

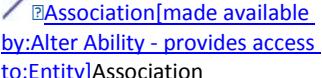
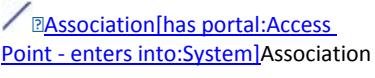
	<p> <a href="#">performs mitigation</a> Property  <a href="#">Mitigation Plan</a> Class  <a href="#">mitigation</a> Property</p> <hr/>	
<b>Personnel Security (PS)</b>  PERSONNEL SECURITY POLICY AND PROCEDURES  Control: The organization:  a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:  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  b. Reviews and updates the current:  1. Personnel security policy [Assignment: organization-defined frequency]; and  2. Personnel security procedures [Assignment: organization-defined frequency].	<p> <a href="#">Control Authority</a> Diagram  <a href="#">Subject to Authority</a> Association Class  <a href="#">Authority</a> Class  <a href="#">has authority over</a> Property</p> <hr/> <p> <a href="#">provides access to</a> Property  <a href="#">Association[made available by:Alter Ability - provides access to:Entity]</a> Association  <a href="#">Access Identifier</a> Class  <a href="#">Access Point</a> Class  <a href="#">Association[has opening:Access Point - enters through:Boundary]</a> Association  <a href="#">Association[has portal:Access Point - enters into:System]</a> Association  <a href="#">Access Complexity</a> Enumeration  <a href="#">Access Vector</a> Enumeration  <a href="#">Access Control Failure</a> Class  <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a> Association  <a href="#">Association[Exit Action - exit through:Access Point]</a> Association</p> <hr/> <p> <a href="#">security level</a> Property  <a href="#">Communications Security Level</a> Class  <a href="#">security level</a> Property  <a href="#">Security Danger</a> Class</p> <hr/>	This control area <b>Personnel Security (PS)</b> of the 800.53 controls maps to the packages, <b>Control Authority</b> , <b>Provides Access</b> , <b>Security Level</b> , <b>Asserting Policy</b> , <b>Process and Planning and Security Levels</b> , <b>Person Identifiers Means</b> , <b>Assessment areas</b> of the Threat and Risk Conceptual Model. The <b>Security</b> , <b>Person Identifiers</b> , <b>Means</b> , <b>Control authority</b> , <b>Mitigation</b> , <b>Situation</b> , <b>Process plan</b> and <b>Policy Packages</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>PERSONNEL SECURITY POLICY AND PROCEDURES</b> .

	<p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">Processes Package</a></p> <p> <a href="#">Process and plans Diagram</a></p> <p> <a href="#">Process and plans Element Value</a></p> <p> <a href="#">Process and plans Element Value</a></p> <p> <a href="#">Invoke Process Class</a></p> <hr/> <p> <a href="#">Person Identifiers Diagram</a></p> <p> <a href="#">Person at location Association Class</a></p> <p> <a href="#">Managed Person Identifier Class</a></p> <p> <a href="#">Person Class</a></p> <p> <a href="#">location of person Property</a></p> <hr/> <p> <a href="#">Mitigation Package</a></p> <p> <a href="#">Mitigation Diagram</a></p> <p> <a href="#">Mitigation Class</a></p> <p> <a href="#">Mitigation Activity Class</a></p> <p> <a href="#">Mitigation Actor Class</a></p> <p> <a href="#">performs mitigation Property</a></p> <p> <a href="#">Mitigation Plan Class</a></p> <p> <a href="#">mitigation Property</a></p>	
<p><b>Risk Assessment (RA)</b></p> <p>RISK ASSESSMENT POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b>:</p> <p>1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational</p>	<p> <a href="#">Control Authority Diagram</a></p> <p> <a href="#">Subject to Authority Association Class</a></p> <p> <a href="#">Authority Class</a></p> <p> <a href="#">has authority over Property</a></p> <hr/>	<p>This control area (<b>Risk Assessment (RA)</b>) of the 800.53 controls maps to the packages, <b>Control Authority, Provides Access, Security Level, Asserting Policy, Process and Planning and Risk</b>. The <b>Risk, Security, Means, Control authority, Mitigation, Situation, Process plan and Policy Packages</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>RISK ASSESSMENT</b></p>

<p>entities, and compliance; and</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> <p>1. Risk assessment policy [<b>Assignment: organization-defined frequency</b>]; and</p> <p>2. Risk assessment procedures [<b>Assignment: organization-defined frequency</b>].</p>	<p> <a href="#">Provides access to</a> Property  <a href="#">Association[made available by:Alter Ability - provides access to:Entity]</a> Association</p> <p> <a href="#">Access Identifier</a> Class  <a href="#">Access Point</a> Class</p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary]</a> Association</p> <p> <a href="#">Association[has portal:Access Point - enters into:System]</a> Association</p> <p> <a href="#">Access Complexity</a> Enumeration  <a href="#">Access Vector</a> Enumeration</p> <p> <a href="#">Access Control Failure</a> Class</p> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a> Association</p> <p> <a href="#">Association[Exit Action - exit through:Access Point]</a> Association</p> <hr/> <p> <a href="#">Security level</a> Property</p> <p> <a href="#">Communications Security Level</a> Class</p> <p> <a href="#">Security level</a> Property</p> <p> <a href="#">Security Danger</a> Class</p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy</a> Class</p> <hr/> <p> <a href="#">Processes</a> Package  <a href="#">Process and plans</a> Diagram</p> <p><input checked="" type="checkbox"/> <a href="#">Process and plans</a> Process and plans Element Value</p> <p><input checked="" type="checkbox"/> <a href="#">Process and plans</a> Process and plans Element Value</p> <p> <a href="#">Invoke Process</a> Class</p>	<p><b>POLICY AND PROCEDURES.</b></p>
--	--	--------------------------------------

	<p> <a href="#">Risk and Threat Concepts Package</a></p> <p> <a href="#">Transfer Risk Class</a></p> <p> <a href="#">Risk Treatment Package</a></p> <p> <a href="#">Risk Treatment Diagram</a></p> <p> <a href="#">Risk Treatment Option Class</a></p> <p> <a href="#">risk level accepted Property</a></p> <p> <a href="#">Risky Situation Class</a></p> <p> <a href="#">risk owner Property</a></p> <p> <a href="#">risk to Property</a></p> <hr/> <p><a href="#">security level Property</a></p> <p> <a href="#">Communications Security Level Class</a></p> <p> <a href="#">security level Property</a></p> <p> <a href="#">Security Danger Class</a></p> <hr/> <p> <a href="#">Mitigation Package</a></p> <p> <a href="#">Mitigation Diagram</a></p> <p> <a href="#">Mitigation Class</a></p> <p> <a href="#">Mitigation Activity Class</a></p> <p> <a href="#">Mitigation Actor Class</a></p> <p> <a href="#">performs mitigation Property</a></p> <p> <a href="#">Mitigation Plan Class</a></p> <p> <a href="#">mitigation Property</a></p>	
<p><b>System and Services Acquisition (SA)</b></p> <p>SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b>:</p> <p>1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p>	<p> <a href="#">Control Authority Diagram</a></p> <p> <a href="#">Subject to Authority Association Class</a></p> <p> <a href="#">Authority Class</a></p> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">provides access to Property</a></p>	<p>This control area (<b>System and Services Acquisition (SA)</b>) of the 800.53 controls maps to the packages, <b>Control Authority</b>, <b>Provides Access</b>, <b>Security Level</b>, <b>Asserting Policy</b>, <b>Process and Planning</b> and <b>System</b>. The <b>Person Identifiers</b>, <b>Means</b>, <b>Control authority</b>, <b>Mitigation</b>, <b>Situation</b>, <b>Process plan</b> and <b>Policy Packages</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>SYSTEM AND SERVICES ACQUISITION POLICY AND</b></p>

<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> <ol style="list-style-type: none"> <li>1. System and services acquisition policy [Assignment: <i>organization-defined frequency</i>]; and</li> <li>2. System and services acquisition procedures [Assignment: <i>organization-defined frequency</i>].</li> </ol>	<p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]Association</a></p> <p> <a href="#">Access IdentifierClass</a></p> <p> <a href="#">Access PointClass</a></p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary]Association</a></p> <p> <a href="#">Association[has portal:Access Point - enters into:System]Association</a></p> <p> <a href="#">Access ComplexityEnumeration</a></p> <p> <a href="#">Access VectorEnumeration</a></p> <p> <a href="#">Access Control FailureClass</a></p> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]Association</a></p> <p> <a href="#">Association[Exit Action - exit through:Access Point]Association</a></p> <hr/> <p> <a href="#">security levelProperty</a></p> <p> <a href="#">Communications Security LevelClass</a></p> <p> <a href="#">security levelProperty</a></p> <p> <a href="#">Security DangerClass</a></p> <p> <a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">ProcessesPackage</a></p> <p> <a href="#">Process and plansDiagram</a></p> <p> <a href="#">Process and plans Process and plansElement Value</a></p> <p> <a href="#">Process and plans Process and plansElement Value</a></p> <p> <a href="#">Invoke ProcessClass</a></p> <hr/> <p> <a href="#">System Package</a></p>	<p><b>PROCEDURES.</b></p>
--	--	---------------------------

	<p> <a href="#">System Diagram</a></p> <p> <a href="#">System Class</a></p> <p> <a href="#">has subsystem Property</a></p> <hr/> <p> <a href="#">Subsystem Association</a></p> <hr/> <p> <a href="#">security level Property</a></p> <p> <a href="#">Communications Security Level Class</a></p> <p> <a href="#">security level Property</a></p> <p> <a href="#">Security Danger Class</a></p> <hr/> <p><a href="#">Process and plans Diagram</a></p> <p> <a href="#">Plan Class</a></p> <p> <a href="#">Mitigation Plan Class</a></p> <p> <a href="#">plan Property</a></p>	
<p><b>System and Communications Protection (SC)</b></p> <p>SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES</p> <p>Control: The organization:</p> <p>a. Develops, documents, and disseminates to <b>[Assignment: organization-defined personnel or roles]</b>:</p> <p>1. A system and communications protection 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 system and communications protection policy and associated system and communications protection controls; and</p> <p>b. Reviews and updates the current:</p> <p>1. System and communications protection policy <b>[Assignment: organization-defined frequency]</b>; and</p> <p>2. System and communications protection procedures <b>[Assignment: organization-defined frequency]</b>.</p>	<p> <a href="#">Control Authority Diagram</a></p> <p> <a href="#">Subject to Authority Association Class</a></p> <p> <a href="#">Authority Class</a></p> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">provides access to Property</a></p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity] Association</a></p> <p> <a href="#">Access Identifier Class</a></p> <p> <a href="#">Access Point Class</a></p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary] Association</a></p> <p> <a href="#">Association[has portal:Access Point - enters into:System] Association</a></p> <p> <a href="#">Access Complexity Enumeration</a></p> <p> <a href="#">Access Vector Enumeration</a></p>	<p>This control area <b>System</b> and maps to the packages, <b>Control Authority</b>, <b>Provides Access</b>, <b>Security Level</b>, <b>Asserting Policy</b>, <b>Process and Planning</b> and I. The Risk, <b>Security</b>, <b>Means</b>, <b>Control authority</b>, <b>Mitigation</b>, <b>Situation</b>, <b>Process plan and Policy Packages</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>RISK ASSESSMENT POLICY AND PROCEDURES</b>.</p>

	<p> <a href="#">Access Control Failure</a> Class</p> <p> <a href="#">Association</a>[traversed using:Entry Action - enters through:Access Point]Association</p> <p> <a href="#">Association</a>[Exit Action - exit through:Access Point]Association</p> <hr/> <p> <a href="#">security level</a>Property</p> <p> <a href="#">Communications Security Level</a>Class</p> <p> <a href="#">security level</a>Property</p> <p> <a href="#">Security Danger</a>Class</p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy</a> Diagram</p> <p> <a href="#">Policy</a> Class</p> <hr/> <p> <a href="#">Processes</a> Package</p> <p> <a href="#">Process and plans</a> Diagram</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Invoke Process</a>Class</p> <hr/> <p> <a href="#">System</a> Package</p> <p> <a href="#">System</a> Diagram</p> <p> <a href="#">System</a> Class</p> <p> <a href="#">has subsystem</a> Property</p> <p> <a href="#">Subsystem</a> Association</p> <hr/> <p> <a href="#">Risks</a> Package</p> <p> <a href="#">Risk</a>Diagram</p> <p> <a href="#">Risk Metrics</a>Diagram</p> <p> <a href="#">Accept Risk</a>Class</p> <p> <a href="#">Risk Treatment</a> Risk Treatment/Element Value</p>	
--	--	--

	<p> <a href="#">Risk Treatment</a> Risk TreatmentElement Value</p> <p> <a href="#">risk level accepted</a> Property</p> <p> <a href="#">: Risk Owner</a> Property</p> <hr/> <p> <a href="#">Mitigation Package</a></p> <p> <a href="#">Mitigation Diagram</a></p> <p> <a href="#">Mitigation Class</a></p> <p> <a href="#">Mitigation Activity Class</a></p> <p> <a href="#">Mitigation Actor Class</a></p> <p> <a href="#">performs mitigation</a> Property</p> <p> <a href="#">Mitigation Plan Class</a></p> <p> <a href="#">mitigation</a> Property</p> <hr/> <p> <a href="#">Means</a>Class</p> <p> <a href="#">Means to end</a> Association</p> <p><a href="#">Process and plans Diagram</a></p> <p> <a href="#">Plan</a> Class</p> <p> <a href="#">Mitigation Plan</a> Class</p> <p> <a href="#">plan</a> Property</p>	
<p><b>System and Information Integrity (SI)</b></p> <p>SYSTEM AND INFORMATION INTEGRITY 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 system and information integrity 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 system and information integrity policy and associated system and information integrity controls; and</p> <p>b. Reviews and updates the current:</p> <p>1. System and information integrity policy [Assignment: organization-defined frequency]; and</p> <p>2. System and information integrity procedures</p>	<p> <a href="#">Control Authority</a> Diagram</p> <p> <a href="#">Subject to Authority</a> Association Class</p> <p> <a href="#">Authority</a> Class</p> <p> <a href="#">has authority over</a> Property</p> <hr/> <p> <a href="#">provides access to</a> Property</p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]</a> Association</p> <p> <a href="#">Access Identifier</a>Class</p> <p> <a href="#">Access Point</a>Class</p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary]</a> Association</p>	<p>This control area (<b>System and Information Integrity(SI)</b>) of the 800.53 controls maps to the packages, <b>Control Authority</b>, <b>Provides Access</b>, <b>Security Level</b>, <b>Asserting Policy</b>, <b>Process and Planning</b> and <b>System</b>, of the Threat and Risk Conceptual Model. The <b>Risk</b>, <b>Security</b>, <b>Means</b>, <b>Control authority</b>, <b>Mitigation</b>, <b>Situation</b>, <b>Process plan</b> and <b>Policy Packages</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES</b>.</p>

<p>[Assignment: organization-defined frequency].</p>	<p> <a href="#">Association[has portal:Access Point - enters into:System]Association</a></p> <p> <a href="#">Access ComplexityEnumeration</a></p> <p> <a href="#">Access VectorEnumeration</a></p> <p> <a href="#">Access Control FailureClass</a></p> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]Association</a></p> <p> <a href="#">Association[Exit Action - exit through:Access Point]Association</a></p> <hr/> <p> <a href="#">security levelProperty</a></p> <p> <a href="#">Communications Security LevelClass</a></p> <p> <a href="#">security levelProperty</a></p> <p> <a href="#">Security DangerClass</a></p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">Processes Package</a></p> <p> <a href="#">Process and plans Diagram</a></p> <p> <a href="#">Process and plans Element Value</a></p> <p> <a href="#">Process and plans Element Value</a></p> <p> <a href="#">Invoke ProcessClass</a></p> <hr/> <p> <a href="#">System Package</a></p> <p> <a href="#">System Diagram</a></p> <p> <a href="#">System Class</a></p> <p> <a href="#">has subsystem Property</a></p> <p> <a href="#">Subsystem Association</a></p> <hr/> <p> <a href="#">security level Property</a></p>	
--	---	--

	<p> <a href="#">Communications Security Level Class</a></p> <p> <a href="#">security level Property</a></p> <hr/> <p> <a href="#">Security Danger Class</a></p> <hr/> <p> <a href="#">Process and plans Diagram</a></p> <p> <a href="#">Plan Class</a></p> <hr/> <p> <a href="#">Mitigation Plan Class</a></p> <p> <a href="#">plan Property</a></p> <hr/> <p> <a href="#">Risks Package</a></p> <p> <a href="#">Risk Diagram</a></p> <p> <a href="#">Risk Metrics Diagram</a></p> <p> <a href="#">Accept Risk Class</a></p> <p> <a href="#">Risk Treatment Risk TreatmentElement Value</a></p> <p> <a href="#">Risk Treatment Risk TreatmentElement Value</a></p> <p> <a href="#">risk level accepted Property</a></p> <p> <a href="#">Risk Owner Property</a></p>	
<p><b>Program Management</b> (PM)</p> <p>INFORMATION SECURITY PROGRAM PLAN</p> <p>Control: The organization:</p> <p>a. Develops and disseminates an organization-wide information security program plan that:</p> <ol style="list-style-type: none"> <li>1. 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;</li> <li>2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;</li> <li>3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and</li> <li>4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission,</li> </ol>	<p> <a href="#">Control Authority Diagram</a></p> <p> <a href="#">Subject to Authority Association Class</a></p> <p> <a href="#">Authority Class</a></p> <p> <a href="#">has authority over Property</a></p> <hr/> <p> <a href="#">provides access to Property</a></p> <p> <a href="#">Association[made available by:Alter Ability - provides access to:Entity]Association</a></p> <p> <a href="#">Access Identifier Class</a></p> <p> <a href="#">Access Point Class</a></p> <p> <a href="#">Association[has opening:Access Point - enters through:Boundary]Association</a></p> <p> <a href="#">Association[has portal:Access Point - enters into:System]Association</a></p>	<p>This control area (<b>Program Management (PM)</b>) of the 800.53 controls maps to the packages, <b>Control Authority</b>, <b>Provides Access</b>, <b>Security Level</b>, <b>Asserting Policy</b>, <b>Process and Planning</b> and <b>Risk</b> of the Threat and Risk Conceptual Model. The <b>Process plan</b>, <b>System</b>, <b>Resources</b>, <b>Security</b>, <b>Means</b>, <b>Control authority</b>, <b>Mitigation</b>, <b>Situation</b>, <b>Risk</b>, and <b>Policy Packages</b> of <i>classes and properties</i> addresses the responsibility, information and coordination among organizational entities for the <b>INFORMATION SECURITY PROGRAM PLAN</b>.</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> <a href="#">Access Complexity</a> Enumeration</p> <p> <a href="#">Access Vector</a> Enumeration</p> <p> <a href="#">Access Control Failure</a> Class</p> <hr/> <p> <a href="#">Association[traversed using:Entry Action - enters through:Access Point]</a> Association</p> <p> <a href="#">Association[Exit Action - exit through:Access Point]</a> Association</p> <hr/> <p> <a href="#">security level</a> Property</p> <p> <a href="#">Communications Security Level</a> Class</p> <p> <a href="#">security level</a> Property</p> <p> <a href="#">Security Danger</a> Class</p> <hr/> <p><a href="#">Asserting Policy Association</a></p> <p> <a href="#">Policy Diagram</a></p> <p> <a href="#">Policy Class</a></p> <hr/> <p> <a href="#">Processes</a> Package</p> <p> <a href="#">Process and plans</a> Diagram</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Process and plans</a> Process and plansElement Value</p> <p> <a href="#">Invoke Process</a> Class</p> <p><a href="#">Process and plans Diagram</a></p> <p> <a href="#">Plan</a> Class</p> <p> <a href="#">Mitigation Plan</a> Class</p> <p> <a href="#">plan</a> Property</p> <hr/> <p>w  <a href="#">System</a> Package</p> <p> <a href="#">System</a> Diagram</p> <p> <a href="#">System</a> Class</p> <p> <a href="#">has subsystem</a> Property</p> <p> <a href="#">Subsystem</a> Association</p>
--	--

- |  |   |  |
|--|---|--|
|  | <ul style="list-style-type: none"> <li> <a href="#">Resources</a> Package</li> <li> <a href="#">Resource</a> Diagram</li> <li> <a href="#">Resource</a> Class</li> <li> <a href="#">harmed resource</a> Property</li> </ul> <hr/> <ul style="list-style-type: none"> <li><a href="#">Risk and Threat Concepts</a> Package</li> <li> <a href="#">Transfer Risk</a> Class</li> <li> <a href="#">Risk Treatment</a> Package</li> <li> <a href="#">Risk Treatment</a> Diagram</li> </ul> <hr/> <ul style="list-style-type: none"> <li> <a href="#">Mitigation</a> Package</li> <li> <a href="#">Mitigation</a> Diagram</li> <li> <a href="#">Mitigation</a> Class</li> <li> <a href="#">Mitigation Activity</a> Class</li> <li> <a href="#">Mitigation Actor</a> Class</li> <li> <a href="#">performs mitigation</a> Property</li> <li> <a href="#">Mitigation Plan</a> Class</li> <li> <a href="#">mitigation</a> Property</li> </ul> <hr/> <ul style="list-style-type: none"> <li><a href="#">security level</a> Property</li> <li> <a href="#">Communications Security Level</a> Class</li> <li> <a href="#">security level</a> Property</li> <li> <a href="#">Security Danger</a> Class</li> </ul> <hr/> <ul style="list-style-type: none"> <li><a href="#">Control Authority</a> Diagram</li> <li> <a href="#">Subject to Authority</a> Association Class</li> <li> <a href="#">Authority</a> Class</li> <li> <a href="#">has authority over</a> Property</li> </ul> |  |
|--|---|--|

## 12 Annex A: UML Conceptual Modeling Profile Semantics (non-normative)

This section defines the UML profile for conceptual modeling and mapping. In order to improve UML's suitability for modeling real-world concepts, this profile interprets standard with semantic features, as detailed below:

### 12.1 Introduction

A concept model can be expressed in UML with the concept modeling profile. The profile defines the interpretation of UML concepts used, extends UML concepts with "stereotypes" and makes some UML semantics more specific to concept modeling. While there are some extensions, every effort is made to use "generic UML" class diagrams, as they are well understood and supported. It only provides stereotypes to extend UML to make concept models more expressive. For example, without complex OCL constraints, UML normally has no way to express that, in the context of some class, some values must be of some type, all values must be of some type, or that the property chain *has father • has brother* is equivalent to the property *has uncle*. These extended notions are introduced here, in subsequent sections. Readers are referred to the UML specification and the many books and courses on UML for an in-depth treatment of generic UML.

This section is intended to define the semantics of UML used in this specification to represent concept models. The subset of UML used for concept modeling is primarily that known as "Class models", the most commonly used part of UML. Our scope further narrows what we utilize to exclude behaviors and methods – elements used for object oriented design. Those elements may be present, but they are ignored for the purposes of concept modeling.

The goal of a concept model is to unambiguously define durable conceptualizations of the real or an imaginary world. One can think of a concept model as a "subject area", which can be as small or large as desired (e.g., the concepts across the entire financial industry, or merely the concepts within one organization). Concepts are, of course, the foundation of a concept model. Concepts are the elements of how we think about the world. They are modeled as combination of classes, datatypes, enumerations, associations, and properties. A related goal of a concept model is to be as non-technical and business-friendly as possible. That means that names for concepts should contain spaces rather than what's called "CamelCasedWords" or "Underscore\_Separated\_Words". It is the job of the transformations to convert those names into lexemes that are acceptable to more technical tooling.

A concept model owned by subject matter experts is more durable than a logical information model designed with a particular system in mind. Thus, one definition of concepts and properties can be represented by multiple logical information models, each optimizing for different technical goals.

A concept model is not an information or data model. When we think about concepts, we think about real-world things, not data structures about those things. These real-world concepts become the pivot points around which we define and relate the many data structures that describe those things. For example, every Person *has mother* one Person, which is essential to the definition of a Person. Such concepts provide criteria that narrow the definition of what a Person concept is, it does not specify that a system should store every person's mother. For another example, it would be reasonable for a concept model to assert that an eye has a measurable visual acuity, but not to define how visual acuity will be represented within a computer as bits and bytes, or how often visual acuity will be stored within a database. Such technical concerns should be elaborated in a logical information model, which has elements that can be well defined by a concept model. Note, however, that things such as tables and columns are valid concepts in their own right, but they are different from the real-world concepts they might represent.

Concept models can be modular. A concept model may refer to things in a number of other concept models. This is useful for refining another organization's concept model, separately maintaining overlapping concepts between organizations, or more easily managing smaller subject areas.

A concept model consists of a network of concepts with a simple essential structure. That structure is the definition of classes, relations between them and their characteristics. Classes represent the "things" in our world – including physical things like trees or people and "made up" things like agreements.

Other concepts connect those things - the relations between things are UML associations that have properties. Things have characteristics such as weight or color. Things can also have properties that are attributes of a class. This basic

network of classes, associations, and properties forms the foundation of the concept model and defines the conceptual framework and vocabulary of a domain. Each of these concepts may have names, which form the vocabulary of a domain of interest. Various assertions are then made about these concepts and their connections that further refine the semantics of those concepts – multiplicities of relationships, specializations between concepts, essential properties of things, etc.

One of the fundamental ways we understand and organize concepts is their arrangement into hierarchies, where general concepts are specialized to form more specific concepts within a specific context or with more specific characteristics. A concept model can arrange all the fundamental elements into hierarchies using generalization relationships. In contrast, another kind of hierarchy is a structural data hierarchy – where data elements contain other data elements. As the purpose of a concept model is not representing data, data hierarchies are not part of a concept model, they are typically part of logical information models that are related to a concept model. To allow for the many viewpoints that can exist for any concept, a concept can be in many generalization hierarchies at the same time.

The following section defines how basic UML is used to represent the foundational network of concepts using classes, associations, and properties. Additional constraints are then attached to this basic framework to enhance semantic expression and the ability of automation to federate and analyze information about those concepts.

### 12.1.1 Classes

Classes specify, or classify, a set of things, according to some set of rules or understanding. Classification is the essential mechanism of conceptualization we use. Classes specify a set of things belonging to that class – this is called the class's *extent*. Each element of the class is an *instance* of that class – it is something the class classifies. Classifications may be arranged in hierarchies.

In the UML concept model, a class is diagrammed as a box with a name at the top. In some cases a definition is also shown next to the box in a “note” form.

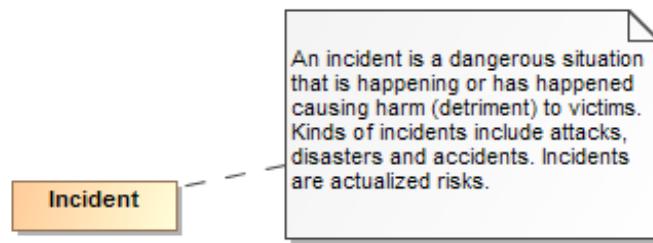


Figure 12 Example of a Class

The above example shows the class “Incident” and its definition. It should be noted that a class is *a way* to classify something. It is natural to classify something multiple ways. For example we may classify a situation as also being a danger or, to someone else, an opportunity to do harm. This is different from many technology models (e.g. Java) that only allow something to be classified in one way and the classification is fixed. *The basic assumption of the concept model is that unless specified otherwise, something may be classified in any number of ways and those classifications may change over time.*

### 12.1.2 Instances

While not usually used in the definition of the concept model, instances can also be shown in UML and are utilized to illustrate examples. Since the model is conceptual, instances of classes are proxies for the “real thing” in the world – not data about them or other technology artifacts. However we sometimes want to show information about instances.

Instances are also shown as a box, but have a “:” separating the name of the instance from its classes.

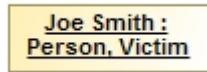


Figure 13 Instance Example

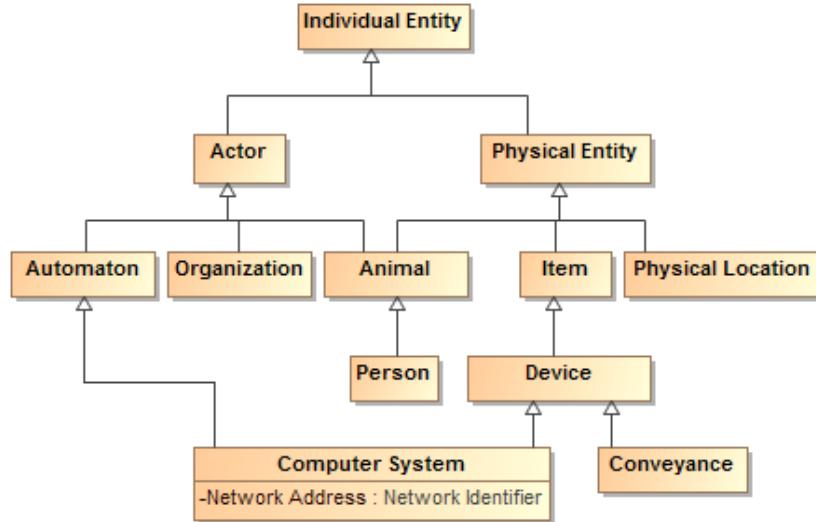
The above example shows a information about an instance named “Joe Smith” that is classified as a “Person” and a “Victim”.

### 12.1.3 Class Generalization

Since Aristotle, classes have been arranged in hierarchies – from most general concepts to more specific ones. In UML this is shown as a Generalization – an arrow with a solid line from the more specific concept to the more general. The more general class is known as the *Superclass* (or *Supertype*) and the more specific the *Subclass* (or *Subtype*). Generalization has some specific semantic rules:

- Everything that is true about the superclass must be true about all its subclasses
- The extent of the subclass is a subset of the extent of the superclass
- All properties and associations that apply to instances of a class also apply to instances of all its subtypes

In a concept model, a class may have any number of superclasses or subclasses. In contrast, some technologies (Like XML Schema) limit the number of superclasses to one.



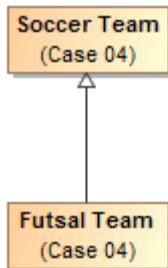
**Figure 14 Class Hierarchy Example**

The above example shows a class hierarchy with multiple levels.

*Note that all properties and associations defined for all superclasses of a class apply to that class. For that reason a complete understanding of a class and its potential properties must include such superclasses.*

A generalization is a subsumption relationship between a more general class and a more specific class. Every instance of the specific class is also an instance of the subsuming general class. Because of this subsumption relationship, the specific class inherits all of the necessary conditions of the more general classifier.

For a simple example, if we define “Futsal Team” as a subclass of “Soccer Team”, then the set of individuals in “Futsal Team” must be a subset of the set of individuals in “Soccer Team”.



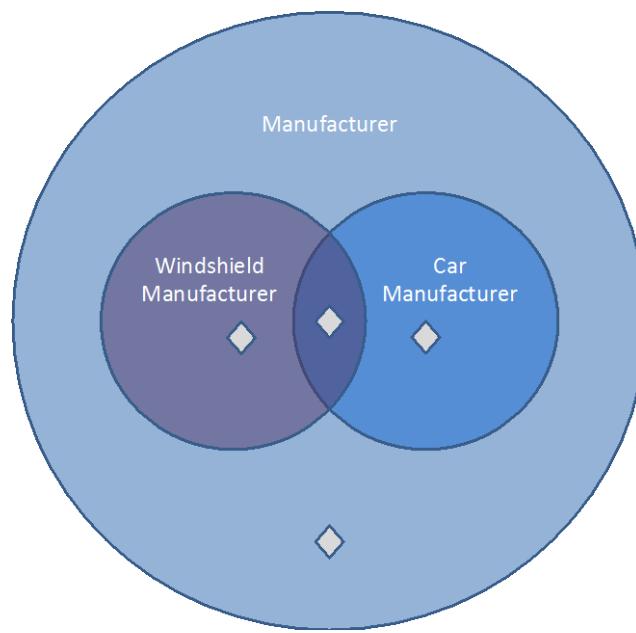
**Figure 15 Simple Generalization Example**

There are four variations on generalization described in the following subsections. The first variation corresponds to the example above: overlapping and incomplete subclasses. That variation is the default in both UML and concept modeling.

### 12.1.31 Overlapping and Incomplete Subclasses

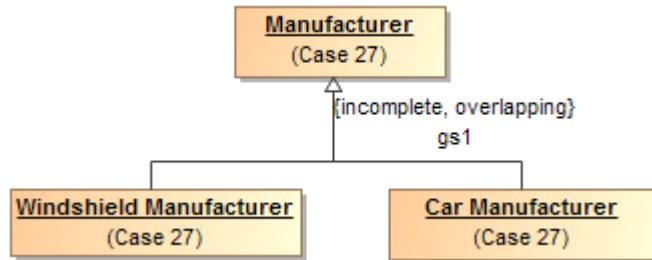
This variation is the default in both UML and in concept modeling. In this variation, an instance can be a member of the superclass and / or any number of subclasses. In this sense, the classification of instances is “incomplete”—sometimes an instance is classified by one or more specific subclasses, and sometimes it is not.

For example, the diagram below shows four instances. One is an instance of “Manufacturer”, one is an instance of “Windshield Manufacturer”, one is an instance of “Car Manufacturer”, and one is an instance of both “Windshield Manufacturer” and “Car Manufacturer”.



**Figure 16 An example of incomplete subclasses**

In both standard UML and in concept modeling, incomplete and overlapping subclasses are shown with either no notation, or with the equivalent notation {incomplete, overlapping} near the generalization arrow.

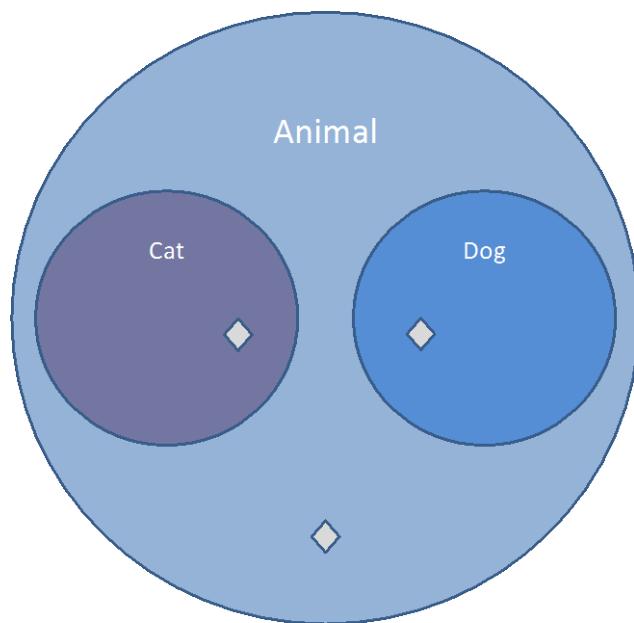


**Figure 17 Incomplete and overlapping subclasses in standard UML notation**

### 12.1.32 Disjoint and Incomplete Subclasses

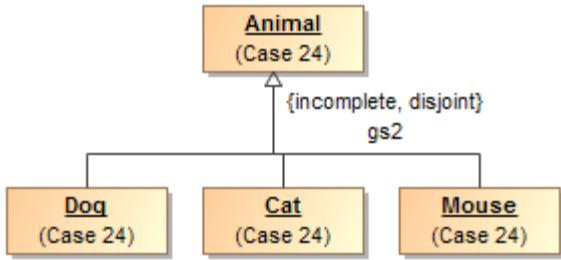
This variation means that an instance can only be classified by at most one of the disjoint classes. Disjoint classes cannot have any overlap in their instances.

The diagram below shows three instances. One is an instance of “Cat”, one is an instance of “Dog”, and one is an instance of “Animal”. An instance classified as both “Cat” and “Dog” is impossible because there is no overlap between the two classes. In the most basic terms, an instance of a “Cat” cannot be an instance of a “Dog”, and vice versa.



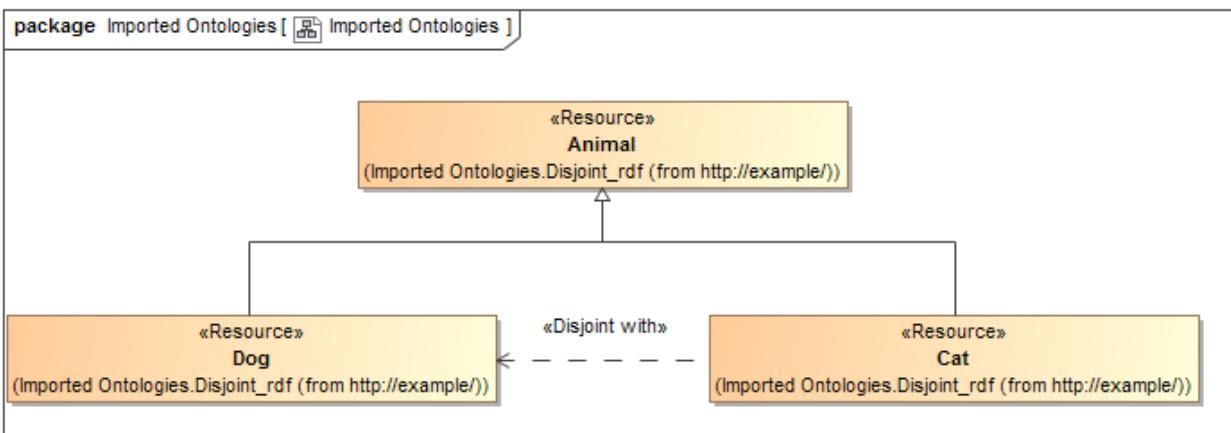
**Figure 18 Disjoint Subclasses**

The following diagram shows an example of disjoint subclasses in standard UML notation. It shows that “Dog”, “Cat”, and “Mouse” are all subclasses of “Animal”. In addition, the standard UML {incomplete, disjoint} notation declares all of the subclasses to be incomplete and disjoint. Intuitively, an instance of the subclass “Dog” is an instance of the superclass “Animal”, but it cannot also be an instance of the “Cat” or “Mouse” subclasses.



**Figure 19 Incomplete and disjoint subclasses in standard UML notation**

The profile also supports a dependency stereotyped as «Disjoint With» to specify disjoint subclasses. For example, the class Animal has three disjoint subclasses, Cat and Dog.

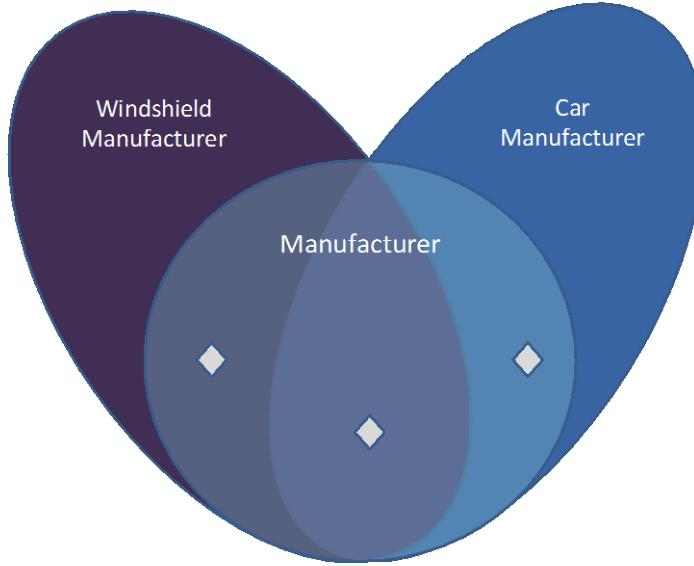


**Figure 20 Alternative «Disjoint With» Stereotype**

### 12.1.33 Complete and Overlapping Subclasses

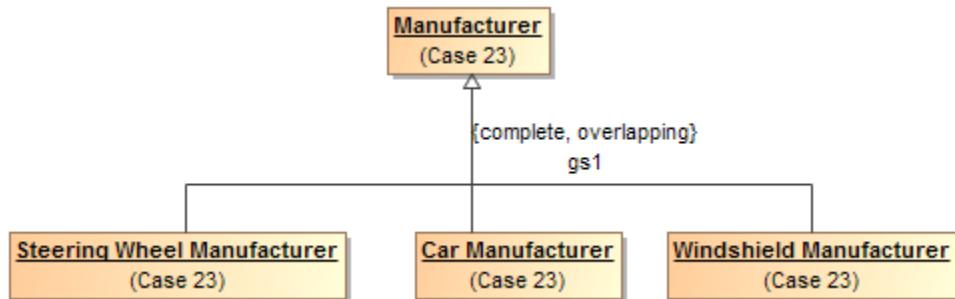
This variation means that an instance can only be classified by at least one of the subclasses; it cannot be classified by only the superclass. Keep in mind that an instance of a subclass is indirectly an instance of a superclass at the same time.

For example, the following diagram shows three instances. One is an instance of “Windshield Manufacturer”, one is an instance of “Car Manufacturer”, and one is an instance of both “Car Manufacturer” and “Windshield Manufacturer”. Note that there can be no instance of “Manufacturer” that is not also an instance of one of the subclasses.



**Figure 21 An example of complete subclasses**

The diagram below shows an example of complete and overlapping subclasses in standard UML notation. The diagram shows that “Steering Wheel Manufacturer”, “Car Manufacturer”, and “Windshield Manufacturer” are all subclasses of “Manufacturer”. In addition, the standard UML {complete, overlapping} notation declares that the subclasses are complete and overlapping.

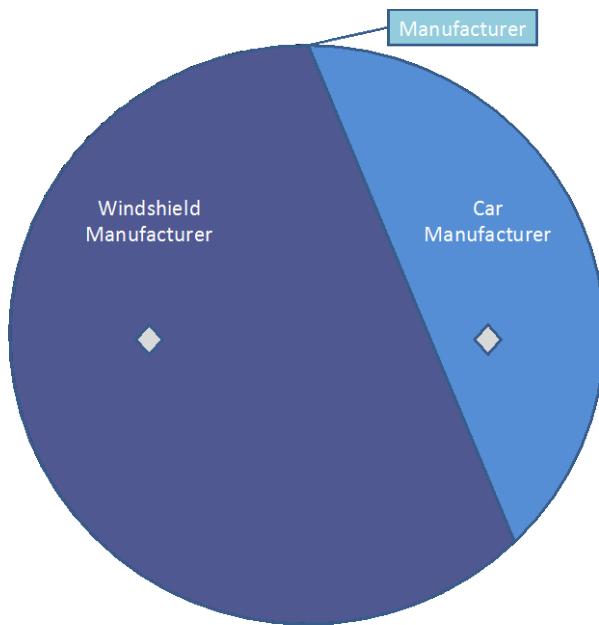


**Figure 22 Complete subclasses in standard UML notation**

#### 12.1.34 Disjoint and Complete Subclasses

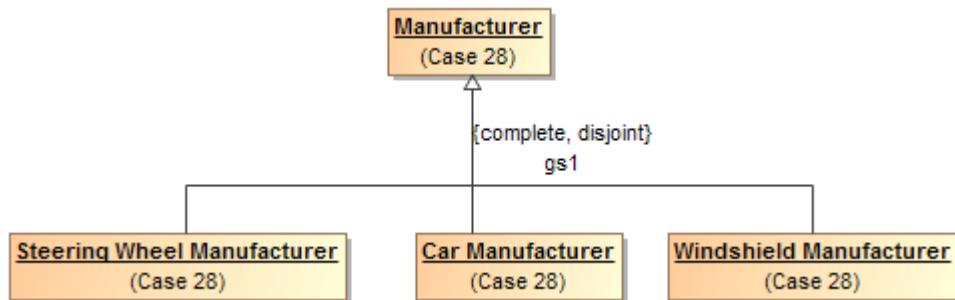
This variation means that an instance can only be classified by one of the subclasses. The instance cannot be classified as only the superclass, and it cannot be classified by two subclasses at the same time.

For example, in the subsequent diagram, two instances are shown. One is an instance of “Windshield Manufacturer”, and one is an instance of “Car Manufacturer”. There can be no instance of “Manufacturer” that is not also an instance of one of the subclasses, and there can be no instance that is classified as both a “Windshield Manufacturer” and a “Car Manufacturer” at the same time.



**Figure 23 Disjoint and complete instances**

The diagram below shows an example of disjoint and complete subclasses in standard UML notation. The diagram shows that “Steering Wheel Manufacturer”, “Car Manufacturer”, and “Windshield Manufacturer” are all subclasses of “Manufacturer”. In addition, the standard UML {complete, disjoint} notation declares that the subclasses are complete and disjoint.



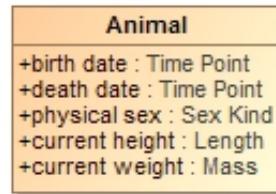
**Figure 24 Disjoint and complete subclasses in standard UML notation**

#### 12.1.4 Properties

Properties represent qualities inherent in something, such as size, weight or a time. Each property has a “type” for the kind of value that represents that quality. A property is a characteristic that an individual can have, or, as explained in a subsequent section, an individual *must* have to qualify as a particular concept.

Most properties are relations between concepts, usually expressed as a verb phrase, such as "Heart *comprised of* Chamber" or "Geographic Region *identified by* Address". This kind of property is generally drawn as a UML association end, as part of a UML association.

Some properties are **relations with data types**, such as a **standard UML Date**, usually expressed as a prepositional phrase, such as "Person *born on* Date" or a noun phrase, such as "Person *birth date* Time Point". This kind of property is generally drawn as a UML attribute, within an attribute compartment of **the most general classifier that can have that quality**.



**Figure 25 Example of Properties**

The above example shows that an animal has the qualities of birthdate, **death date**, physical sex, height and weight. Note that **these** is no **assumption** that these qualities may be known, required or that different data sources may or may not agree on them – just that an Animal has these qualities. Instances of properties are facts about the entity they describe. In concept models, attributes are only used for qualities, never to relate different entities.

A much smaller number of properties **represent metadata**, usually expressed as a noun phrase, such as "Anything *description String*" or "Anything *see also URI*". This profile provides a stereotype called «Annotation Property» that can be applied to a standard UML property in a concept model.

Note that because every class ultimately specializes the special class «Anything», when that special class has properties, those properties can be used by instances of any subclasses. Moreover, subclasses can have constraints on the values of properties that only hold from that subclass and below in the generalization hierarchy. See subsequent sections for further explanation.

### 12.1.5 Associations

Associations describe facts about how entities are related. Associations are shown as lines between the classes that have related instances. At each end of the line is an "association end" property – the association end describes how the instances of the class on the far end relate to those of the near end. If there are limits to how many instances may be related, these are also shown. Since an association has two ends, the association may be read in either direction, but is the same "fact". The properties involved are considered "inverse properties". The association end **properties are** typically verbs or verb phrases, but in some cases, such as **when an association is reified as a class**, the association ends can become noun phrases. In either case the name denotes the intent of the class *at the other end of the line*.



**Figure 26 Association Example**

The above example says that there are relations between actors and activities such that the *actor performs the activity* and the *activity is performed by the actor*. These are considered two ways to "read" the same fact. Like any fact, relations may be true for some period of time or in some specific situation.

As can be seen in the example the ends of associations are typically verb phrases which can then be read as <the actor> **performs** <the activity>. In other cases the ends are nouns in which case they represent a role being played. If a role were used above instead of "performed by" it could read: <activity> has **performer** <actor> (the *has* in this sentence being implied by **english grammar**).

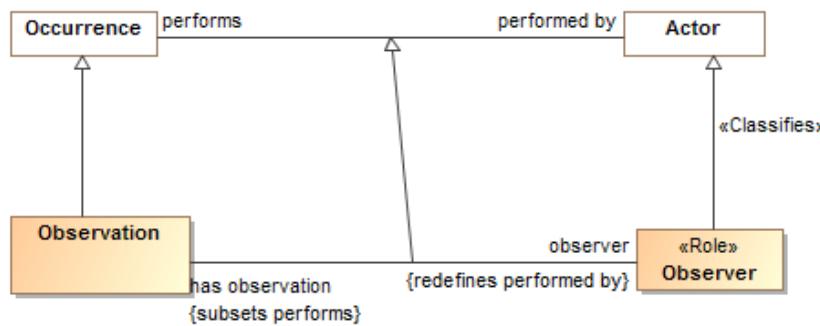
This combination of classes and associations with ends forms the basis for nouns and verbs common to human language. The terms used for the nouns and verbs should be both consistent with their semantics and resonate with stakeholders – sometimes this is a bit of a challenge.

In some cases the ends of the relation are sufficient to define it, in other cases it makes more sense to give the association a name and its own definition. Associations and association ends, like classes, can be part of a hierarchy.

Note that unspecified multiplicities are interpreted as unconstrained: having a minimum cardinality of 0 and a maximum cardinality of “\*”.

### 12.1.6 Property and association end hierarchies

Like class hierarchies, attributes and association ends (we will just call both properties **from now on**) can also be arranged in hierarchies of more or less specific properties. In UML, property hierarchies are represented **using with** either “Subsets” or “Redefines”. What a property subsets or redefines is shown next to its **definition** in the diagram (Note that by convention this is not shown on **summary diagrams**, only the primary definition of the property). If a property completely **subsumes the other in a particular context** it uses a “Redefines” – that is the **redefining and redefined properties have the same set of values**. If the more general concept can also be used in the context a “Subsets” is used.



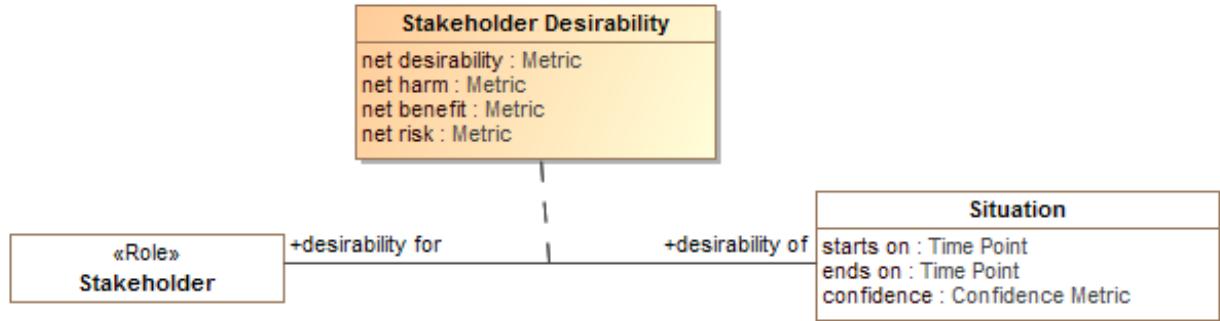
**Figure 27 Example of Association End Hierarchy**

The above example shows that the “has observation” and “observer” properties are specializations of the “performs” and “performed by” concepts. The property “observer” **redefines “performed by”** – that is, an **Observation always has an observer, never a “performed by” actor**. Likewise “has observation” specializes “performs” but an instance of **Observer** can perform other activities as well. Note the generalization between the associations is implied, but is shown in this example for clarity.

Where a **redefined** or **subset** property has no name, it is an indication that the property type and/or multiplicity is merely constrained in some way. **No new properties or associations are actually defined for a constraint (more on this below)**.

### 12.1.7 Association Classes

In a concept model any “fact” may have properties. Of particular importance is the “provenance” of the fact – where the fact came from and thus how much it can be trusted. Facts can also be time-bound, true for some period. Where an association may have additional specific properties or may participate in other relationships, an “association class” is used. As implied by its name, an association class has both the properties of an association and the properties of a class. More complex associations between things use association classes. An association class is diagrammed as an association line and a class box with a dashed line between the association line and its class. While the association line and box may seem somewhat visually distinct – they are the “same concept”.



**Figure 28 Association Class Example**

The above example shows the “Stakeholder Desirability” relation. Between any situation and any stakeholder there can be some metrics as to how much that stakeholder desires or wants to avoid that situation. The Stakeholder Desirability association class represents these as properties of the association: net desirability, net harm, net benefit and net risk – which can all be positive or negative reflecting a benefit or harm, respectively.

## 12.1.8 Annotation

This profile provides a way to comment on any element using *annotations*. One can annotate classes, properties, and models using an open-ended system of *annotation properties*. An annotation property defines a type of annotation with a relatively refined meaning. Any property can be made an *annotation property* using the «Annotation Property» stereotype on a UML property.

Every «Annotation» is a textual value for an «Annotation Property». An annotation describes some subject using an annotation property and a (usually textual) value. An annotation should specify a tagged value called “value for” that refers to an «Annotation Property».

For example, the following diagram illustrates several UML comments stereotyped with «Annotation»

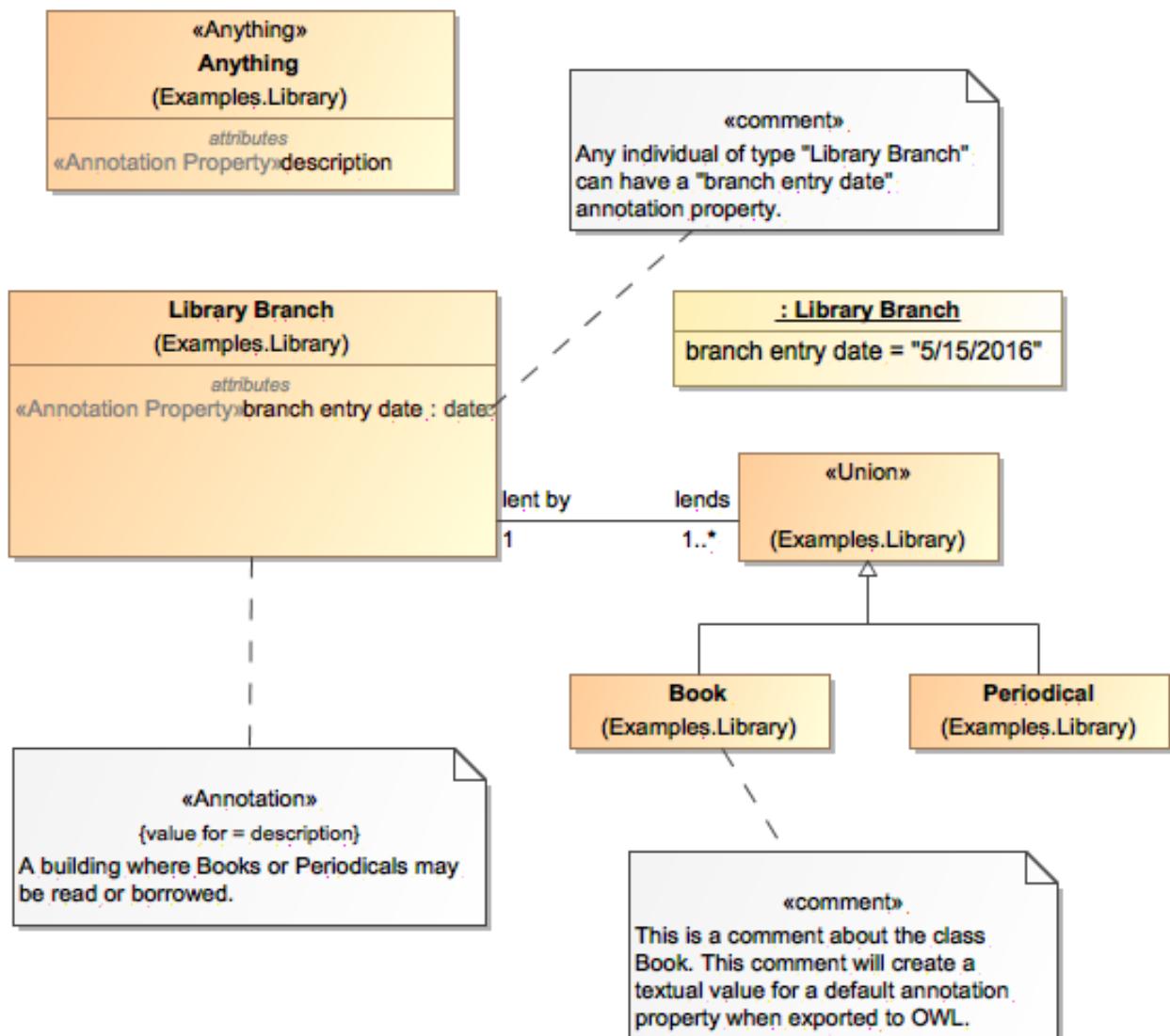


Figure 29 Annotation Examples

## 12.1.9 Specific kinds of classes

There are additional concept modeling specific stereotypes documented [in the reference section](#) that further define the semantics of a class. Some of these [stereotypes](#) are very important for understanding the concept model and are further explained here. These are roles, phases and quantity kinds.

### 12.1.91 Anything

The stereotype «Anything» can be applied to any class to make it special. Every such special class is equivalent to one topmost class ([T](#)) of which all other classes are subclasses. Thus, [a property of a class](#) marked as «Anything» is inherited by all subclasses. In addition, while the name of a such a marked class is irrelevant, [consistently naming such classes](#) “Anything” in all concept models avoids any confusion with normal classes.

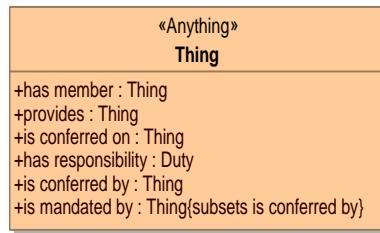


Figure 30 «Anything» Example

### 12.1.92 Union

A «Union» is a class that has an extent (set of instances) which is equivalent to the union of the extents of all types that specialize the Union (Subclasses). Specializing types shall include subtypes and [types that realize the union](#). The union can be either named or unnamed. When it is unnamed, it can only be used [at the domain or range](#) of a property.

Note: UML realizations are included to support unions across [external models](#) because UML generalization can not be used across external models due to the ownership of generalization.

An anonymous union class always implies a [complete](#) subclass generalization.

The following diagram states that an instance of a Person may have a value of type Cat or Dog for the *cares for* property. The [diagram also](#) states that an instance of a Cat or a Dog may have a value of type Person for the *cared for by* property.

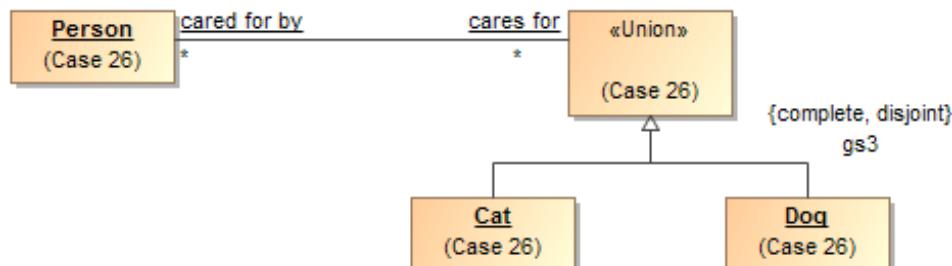


Figure 31 A union class

### 12.1.93 Intersection

An «Intersection» is a class that has an extent (set of instances) equivalent to the intersection of the extents of all supertypes. **Intersection is a stronger statement than a subtype, as a subtype may be a subset of the intersection.** An instance of all the supertypes implies an instance is also an instance of the intersection type.

For intersection, The SIMF profile considers UML generalization and UML realization equivalent. This is due to ownership and legacy considerations in UML. Generalization is the preferred representation.

Note: Realizations are included to support unions across external models. **UML generalization can not be used across external models due to the ownership of generalization.**

### 12.1.94 Context specific types and <<Classifies>>

Some types may be considered the “fundamental” type of something that is essential to its being for its entire lifetime; this is the default assumption of most classes. Other types classify something in a specific context or for a period of time, SIMF calls these “classifications”. The types an instance is classified with **is expected to change over time and may be only valid within a particular context or viewpoint.** Classifications are defined with a <<Classifies>> generalization to another type, the type of thing that can be so classified. For example, “Policeman” can classify a “Person”.

Context specific types such as Roles and Phases are classifications and expected to be used in this more contextual and dynamic fashion; these types may be assigned to or removed from an instance over time or in a context.

For an instance to be classified with a classification, it must also have the type of what the classification <<classifies>>. To use the example above, a **“Policeman” can’t classify a Toaster since the toaster is not a person.** Please see the “Role” and “Phase” discussion for more usage scenarios of <<Classifies>>.

**Implementation note:** most programming languages do not allow for direct representation of multiple classifications, multiple inheritance or context. A common implementation pattern is to represent classifications, roles and phases as independent objects related to the object they classify. An example of this is the IUnknown pattern in .NET.

The following stereotypes define additional classification semantics.

### 12.1.95 Roles

Roles are classes that are expected to be dynamic and contextual, such as teacher, victim or president. A role is defined as a class with the <<Role>> stereotype. Implementation technologies should interpret roles as classifications that may be added to or removed from an instance over time and may be defined **in a particular context.** A role is usually required to be a role of some particular other class, for example a teacher is expected to be a role of a person (at least until a computer takes her job). The constraint of what a role must be a role of is defined using a <<Classifies>> stereotype of a generalization.

Many implementation languages don’t have the capacity to represent roles, so roles are defined as the single and unchangeable “type” of a class or DBMS table. The problem with this is that the same individual may not be connected across all their roles. Specifically representing roles allows the same individual to play multiple roles and for these roles to change – this better reflects the reality of the world and the way we think about it.

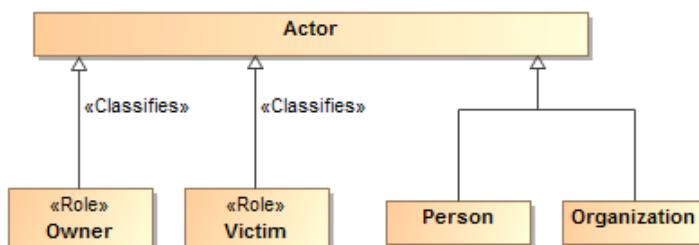


Figure 32 Role Example

The above example shows that an actor can be a person or organization and that either could be classified as being able to play the Owner and/or a Victim role.

Roles help to decouple concepts in models and specifically allow an instance to “play” multiple roles at the same time or over time. Roles, when combined with quantification constraints, clearly define the semantics of roles. For example, we could say that a victim must be a victim of some incident and an owner must own something.

By convention, properties typed by roles may have the same name as the role, this can be read as “has <role>”, e.g. “has victim”, however full verb phrases may be more appropriate in some situations.

### 12.1.96 Phases

Phases are classes that are expected to classify an instance over a specific span of time, such as a teenager, “legal adult” or “Paid Invoice”. A teenager is a person between the ages of 13 and 19 (inclusive) – perhaps “legal adult” is of age 19 or older – we may also want to consider people living or dead, thus alive and dead would be phases. Phase may be considered a synonym for the “State” of something.

A phase is defined as a class with the <<Phase>> stereotype. Like roles, phases use the <<Classifies>> stereotype of a generalization to define what a phase must be a phase of.

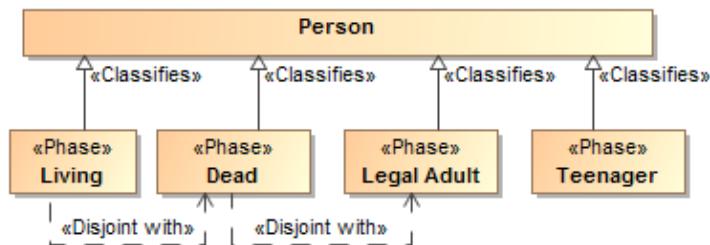


Figure 33 Phases of a person

Also like roles, phases help to decouple concepts in models and specifically allow an instance to “be in” multiple phases (or multiple roles) at the same time or over time. If an instance cannot be in two phases at the same time or be in a role and a phase a “disjoint with” constraint can be used to state that restriction. For example, “Dead” is disjoint with “Legal Adult” and “Living”. Only a “Legal adult” can commit to a contract.

### 12.1.97 Quantity kinds and units

Fundamental to understanding and describing something is physical and other qualities such as temperature, length and color. Many data models fail to capture units of measure explicitly which can and has<sup>5</sup> resulted in dramatic systems failures. A concept for something’s weight should properly be typed by a measure of weight, not an “int” or “real” – which are just ways to represent numbers without knowing what they mean. Of course there needs to be numbers, but in relation to their units.

In that there are different units that can represent the same kind of measure, such as degrees Celsius and degrees Fahrenheit can represent the same temperature – an abstraction is used above like units. The abstraction for a measurable unit is called a <<Quantity Kind>>. Examples of quantity kinds include Length, mass, temperature, frequency, etc.

As any element of measurement data must be specific to a specific unit in a specific data exchange, the <<Unit>> stereotype is used to define a unit for a quantity kind. A <<Represents>> stereotype of generalization (Diagrammed as a green arrow) is used to say that the unit represents the quantity kind.

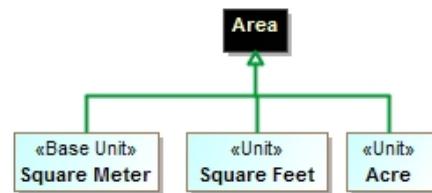
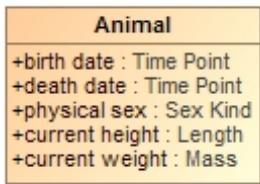


Figure 34 "Area" Example of quantity kinds and units

<sup>5</sup> [https://en.wikipedia.org/wiki/Mars\\_Climate\\_Orbiter](https://en.wikipedia.org/wiki/Mars_Climate_Orbiter)



**Figure 35 - "Animal" example of using quantity kinds.**

In the example above, the “Area” quantity kind (indicated by a black shaded class) can be represented by (the green lines) “Square Meter”, “Square Feet” or an “Acre”. One unit may be nominated as the “Base Unit” and will be used to express conversion factors between the units. As per SI specifications, the Square Meter is the base unit.

By convention quantity kinds are used in fully concept models whereas units are used in data models. The “Animal” example shows quantity kinds being used to define properties of animals.

### 12.1.10 Assertions about concepts

Above we defined the network of essential concepts as classes, relationships and properties. Additional assertions may be made about those concepts using both UML foundational and extended profile capabilities. The following define the kinds of assertions that can be made. Note that the term “property” applies to both simple properties and the ends of associations.

#### 12.1.101 Property Ownership

The concept modeling profile of UML interprets the owner of a property definition as the subject of that property (its domain) and the context in which that property must conform to certain constraints.

Constraints may be placed on a property. These constraints can include multiplicity, which includes a minimum cardinality and a maximum cardinality, a type for the property, existential quantification, and universal quantification. When an instance is a member of a class, all of that class’ constraints must be met.

Property ownership is not interpreted as “slots” in an object. Property values may or may not be independent of the instance that defined them, thus supporting an OWL/RDF, or “open world”, interpretation of properties and associations.

#### 12.1.102 Cardinality

Cardinality defines how many instances of a property may exist for a particular subject instance. For example, how many ages can a person have? The obvious answer is that a person can have at most one age at any one point in time. Thus cardinalities represent the number of instances at any one time.

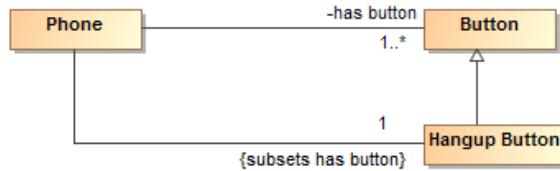
UML allows the cardinality of a property to be left unspecified. The concept modeling profile interprets unspecified cardinalities as being unconstrained - zero to many (“0..\*”), this is consistent with our general rule that anything unsaid is unconstrained.

### 12.1.11 Constraining properties and associations

A cardinality of one or more defined for a property requires that an instance of the related element must exist for an instance of the domain (owning class) of that property or association end to be valid. For example, a living person must have exactly one living brain. This is known as an existential quantification ( $\exists$ ) or qualified constraint in first order logic. Existential quantification is defined using UML cardinality and subsets.

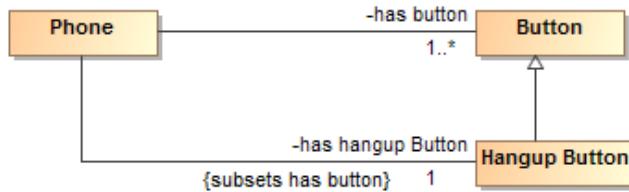
An existential quantification can be stated for a newly defined property or an existing one. For a newly defined property this is done by simply stating cardinality greater than one. For example, a phone must have at least one button with a “has buttons” association end property and a cardinality of “1..\*”. When a new property is being defined it is given a name. If an existing property is being constrained (without a new property being defined) it subsets or redefines the existing property and does not have a name. In the concept modeling interpretation of UML, any cardinality greater than zero creates an existential quantification constraint.

A property is not limited to a minimum and a maximum cardinality (known as multiplicity) for just one type. A property can have a multiplicity for a superclass, while at the same time having a more specific multiplicity for one or more subclasses of that superclass. This type of constraint is an assertion that, among other possible values, the number of values of one of these subclasses is between some minimum and maximum cardinality.



**Figure 36 Phone constraint: A phone must have a hangup button**

For example, we may say a phone must have any number buttons with a “has buttons” property but exactly one of those buttons must be the “hang up button”. We would then define an unnamed property with the type “hang up button” that subsets the “has button” property with a cardinality of 1. If we wanted the hang up button to also define a new property, we would give that property a name.



**Figure 37 Hangup button with new property**

In the concept modeling interpretation of UML, subsetting or redefining a property without giving the new property a different name (or leaving off the new property name altogether) creates a constraint without defining a new property.

As {subsets} or {redefines} with an omitted name is not well defined in UML, in the concept modeling profile it is used to state that a subset of values must meet the stated cardinality and type constraints of the subsetting property. It does not create a new property, although it does create a context in which this constraint holds: the owning class and its subclasses.

The diagram below shows an existential quantification constraint on the global property “is conferred by” (from the Anything “Thing”). The multiplicity is such that at least one of the instances of the property constraint must be one of the types in the union.

Note that the property adding the constraint is unnamed. This is equivalent, in this case, to naming this property the same as the property being constrained (“is conferred by” from the Anything “Thing”).

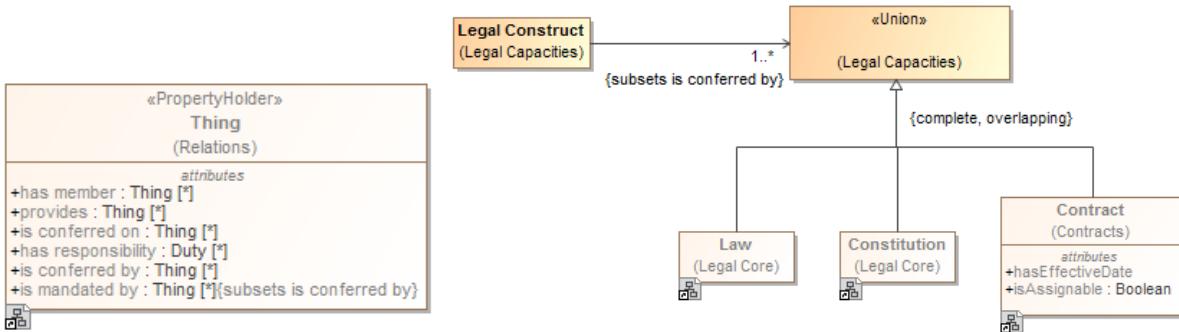


Figure 38 Constraining a global property

### 12.1.12 Tightening a property's type

Sometimes it is necessary, in the context of some class, to constrain *all* the values of a property to a particular type. When defining a new property the type of that property asserts that all values of that property must be of the given type. This is known as a *universal quantification* or *for-all* constraint ( $\forall$ ) in first order logic. This kind of constraint is an assertion that only values of the specified type are valid, and the number of values must be between some minimum and maximum cardinality.

Where all values of a property must be of a given types in a specialized property, UML *{redefines}* is used. In the concept modeling interpretation of UML, introducing a new property or redefining an existing property creates a universal quantification constraint in the context of the owning class. If the redefined property is given a name, a new property with the quantification is defined. If the redefined property does not have a name the existing property is constrained in the more specialized context (usually a subclass).

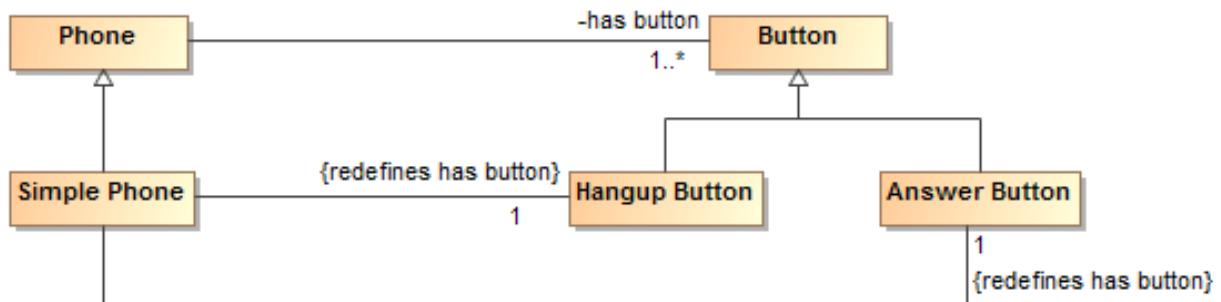


Figure 39 Example of redefines

The example above shows a “simple phone” that has exactly two buttons and they must be an answer button and a hangup button. Since redefines is used, no other buttons are allowed.

The diagram below shows the introduction of a new property “consists of”, defining a universal quantification constraint on the property. The constraint states that, in the context of Soccer Team and any of its subclasses, all values of this property must be of the type “Soccer Player” and that there must be between 5 and 11 values of this property.

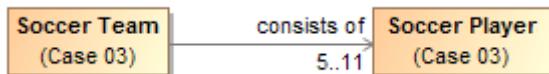
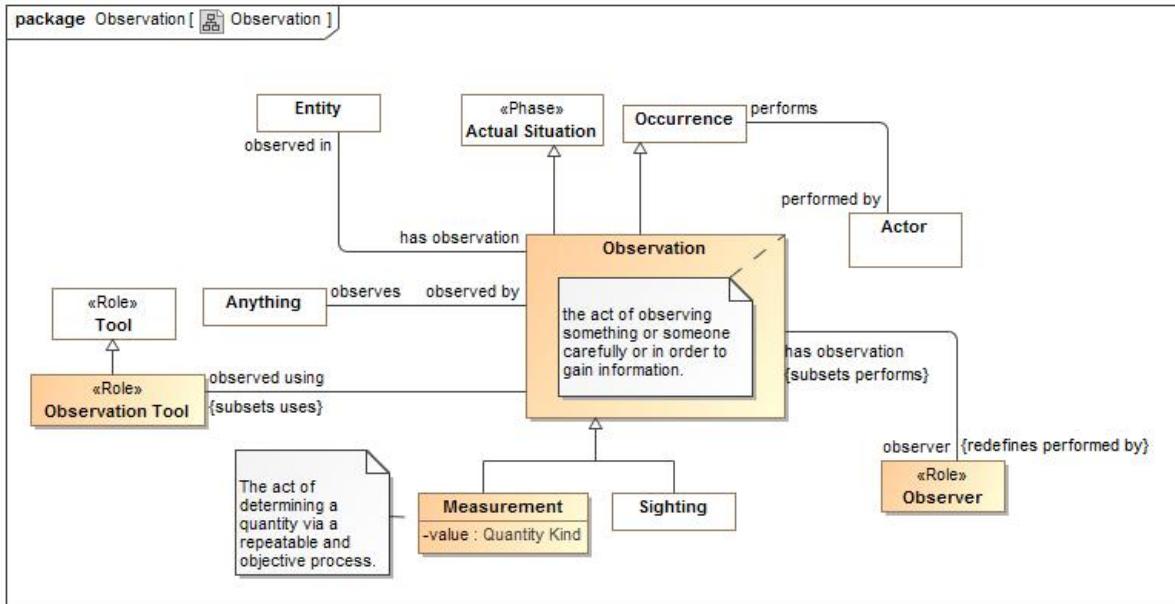


Figure 40 Example of cardinality range

The diagram below shows a universal quantification constraint on the property “observer”. Where any occurrence can be performed by any actor, an observation must be performed by an entity in the role of observer.

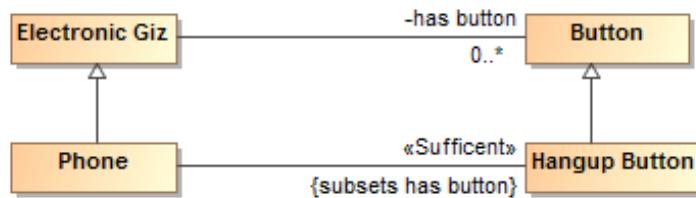


**Figure 41 Observation Example**

### 12.1.13 Inferring a type from its properties

A property's multiplicity or type is declared in the context of an owning class or a special «Anything» class. These declarations are always *necessary* conditions for an instance to be a member of the owning class, or, in the case of «Anything», for *an instance to be valid at all*.

Another kind of condition is known as *necessary and sufficient*. A class with at least one necessary and sufficient condition is known as a *defined class*, which means the differentiating characteristics of the class that make it distinguishable from its parent and sibling classes are defined. Note that using a necessary and sufficient condition on a *property with a minimum cardinality of zero is not meaningful*.



**Figure 42 Phone example for sufficient**

The *diagram above defines* a phone as *any “electronic giz” that has a hangup button*. The existence of a hangup button is sufficient to know something is a phone.

In the concept modeling interpretation of UML, a property that has the «Sufficient» stereotype applied to it indicates that when an instance satisfies the multiplicity and type constraints for all the sufficient properties' values, not only is a *necessary* condition for being an instance of the class met, a *sufficient* condition is also met to assume *that the domain of that property* is of that class. This necessary and sufficient condition allows *an inferencing engine* to classify that instance

as a member of the class that owns the property. All <>sufficient<> constraints must be met for an instance's type to be inferred.

In the concept modeling interpretation of UML, a property that has the «Sufficient» stereotype applied to it indicates that when an instance satisfies the multiplicity and type constraints for all the sufficient properties' values, not only is a necessary condition for being an instance of the class met, a *sufficient* condition is also met. This necessary and sufficient condition allows an inferencing engine to classify that instance as a member of the class with that condition. Once an instance is classified automatically, the conditions on any other properties that have the «Sufficient» stereotype, including those inherited from superclasses, merely become *necessary* conditions the instance must meet to be a *valid* member of the owning class. An instance satisfying the constraints of all the «Sufficient» properties is enough for an inferencing engine to automatically classify an instance.

The diagram below shows that when an instance with the property “has contract with” satisfies specific multiplicity (“1..\*”) and type constraints (of type ‘Steering Wheel Manufacturer’ and “Windshield Manufacturer”) for the property’s values, the instance meets necessary and sufficient conditions to be a member of the class “Car Manufacturer”. Therefore, an inferencing engine would classify this as an instance of the class “Car Manufacturer”. As discussed above, an instance meeting all of these necessary and sufficient conditions is enough to classify the instance. The conditions on the values of these properties become necessary conditions on an instance for it to be a valid member of class “Car Manufacturer.” Also, an instance meeting all of the necessary and sufficient conditions is enough to distinguish instances of the class “Car Manufacturer” from its parent class “Manufacturer.”

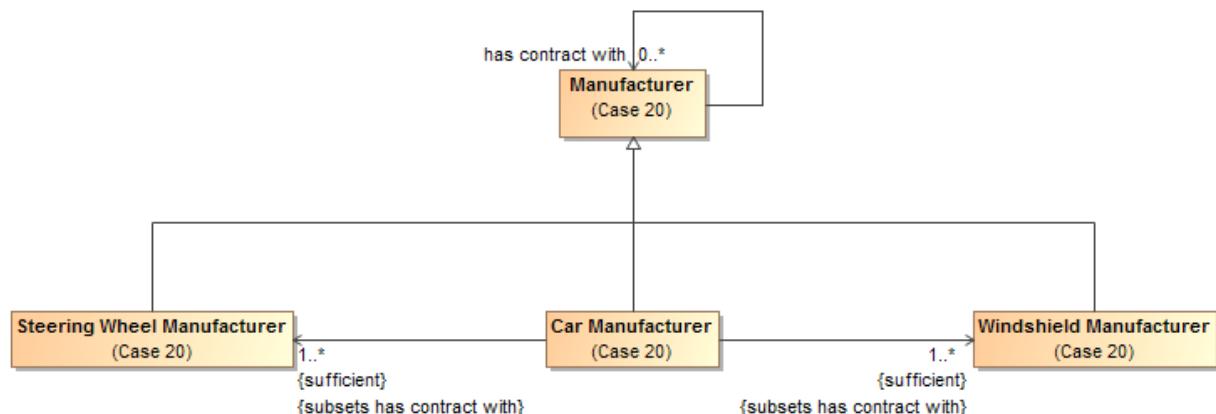


Figure 43 An example of necessary and sufficient condition

### 12.1.14 Property Chain

A property chain is useful for composing a property from two or more other properties that are put together in a chain. It defines the property with reference to the other properties. The property chain allows you to navigate from a starting class (the one with the stereotype «Equivalent Property») through a chain of properties that take a path through multiple classes.

A property chain is an ordered list of linked properties, therefore, it should have two or more “chain” tagged values.

Note	<ul style="list-style-type: none"> <li>• An existential or universal quantification restriction <i>cannot</i> have or be a part of a subproperty chain, although the property it restricts <i>can</i>.</li> <li>• A sub-property <i>can</i> have or be part of a subproperty chain for another property.</li> </ul>
------	---

The following example describes a Person class that has two instances “Female Person” and “Male Person”, and four properties “has parent”, “has father”, “has uncle”, and “has brother”. The stereotype of the property “has uncle” will be «Equivalent Property», and the tagged value is **chain = has father, has brother**. (Note that the «Equivalent Property» stereotype is suppressed in this diagram, but the tagged values are not.)

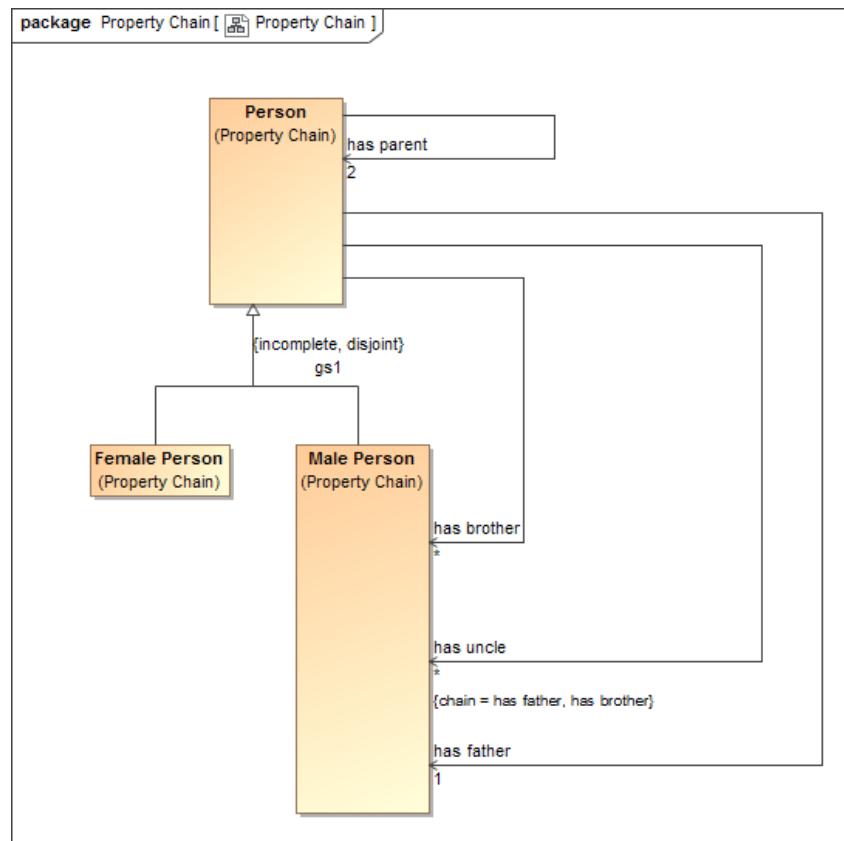


Figure 44 Property Chain Example

### 12.1.15 Equivalent Property

An «Equivalent Property» allows you to represent equivalent properties in a model. You can make two or more properties equivalent to each other by applying the stereotype «Equivalent Property» to the target property and the tagged value “equivalent to” the equivalent property.

#### Note

- An existential or universal quantification restriction *cannot* have or be an equivalent property, although the property it restricts *can*.
- A sub-property can have or be an equivalent property.

The following figure shows the equivalent properties in a diagram.

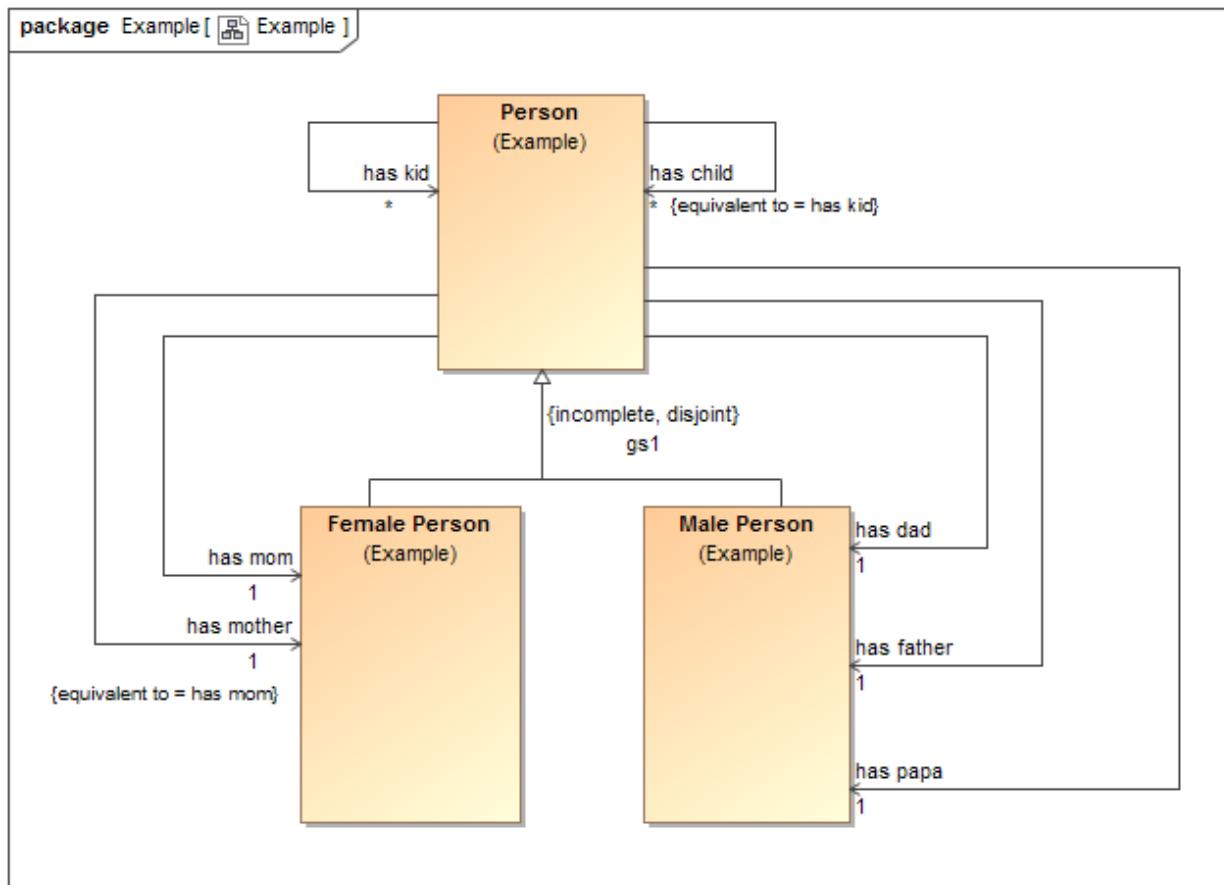


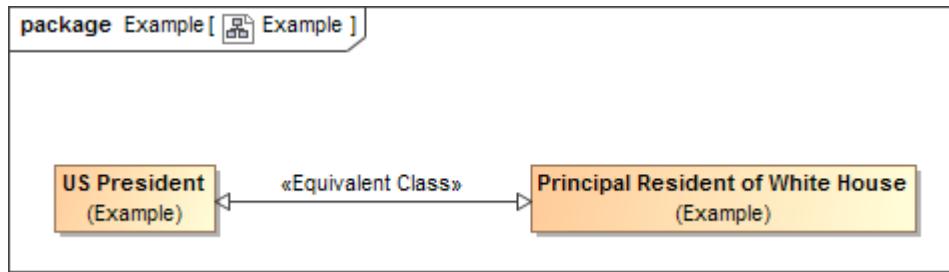
Figure 45 Equivalent properties Example

In the example, the property “has mother” is equivalent to the property “has mom”.

### 12.1.16 Equivalent Class

An «Equivalent Class» stereotype applied to a generalization can specify equivalence between two classes. Class equivalence expresses a generalization relationship stereotyped as «Equivalent Class». Tools should draw this with a double-headed arrow.

The following figure shows two equivalent classes in a diagram.



**Figure 46 Two Equivalent Classes in the Concept Modeler**

In the example, the equivalence class arrow defines that the two classes are semantically equivalent to each other.

## 12.2 SIMF Profile::SIMF Concept Modeling Profile Reference

The conceptual modeling profile defines the conceptual modeling capabilities of SIMF in UML.

### 12.2.1 Diagram SIMF Conceptual Modeling Profile

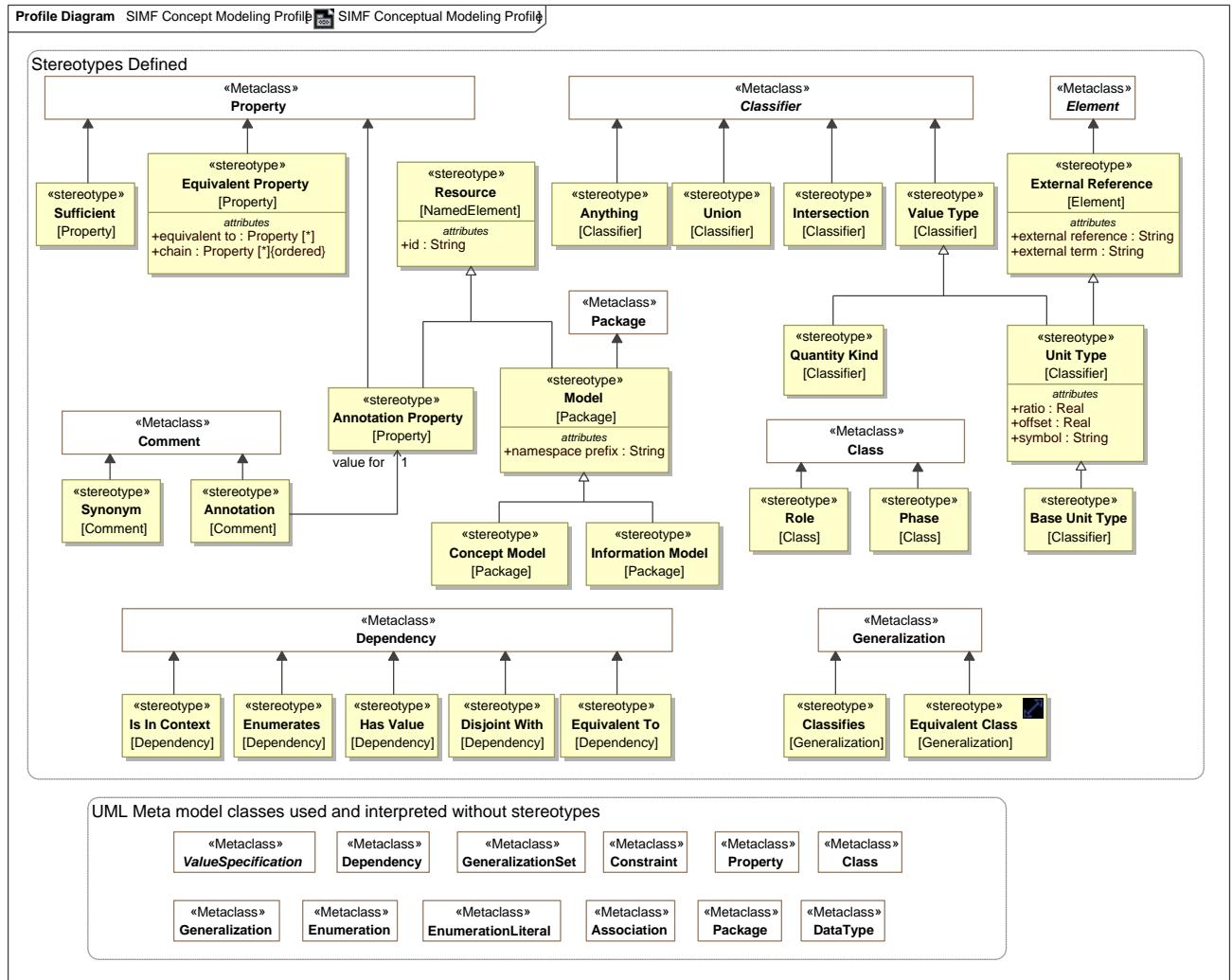


Figure 47 SIMF Conceptual Modeling Profile

### 12.2.2 Stereotype Annotation

An <<Annotation>> comment provides a textual "body" as a "value for" one <<Annotation Property>> describing the annotatedElement(s).

#### Base Classes

- **Comment**

#### Tag Definitions

### ◊ **value for : Annotation Property [1]**

<value for> is the property for which the <<Annotation>> is providing a value.

## 12.2.3 Stereotype Annotation Property

An <<Annotation Property>> is a kind of <<Resource>> that asserts a property represents metadata rather than assertions about the subject domain.

### *Base Classes*

- *Property*

### *Direct Supertypes*

- *Resource*

## 12.2.4 Stereotype Anything

<<Anything>> is a class that represents anything and is equivalent to all other classes of anything in any other model or logic. The defined class is equivalent to SIMF:Anything, OWL:Thing and other "top level" classes.

Because of this equivalence, every class in every model virtually inherits from Anything, just as all OWL classes virtually inherit from owl:Thing.

<<Anything>> classes may be used to define "global properties".

### *Base Classes*

- *Classifier*

## 12.2.5 Stereotype Base Unit Type

<<Base Unit Type>> is a kind of <<Unit Type>> that marks one unit type of a quantity kind as the base unit type within a model. The base unit type provides the basis for conversions between units of the same quantity kind. The base unit always has a ratio of one and an offset of zero.

### *Base Classes*

- *Classifier*

### *Direct Supertypes*

- *Unit Type*

## 12.2.6 Stereotype Classifies

A classification defined by a <<Classifies>> generalization or realization is a "mix in" or "non rigid" classification of an entity beyond any fundamental entity type.

An instance must be typed by the classifies supertype for it to also be classified as the classifies subtype. A classification may be contextual, such as within a relation, situation and/or time frame. Instances may have any number of types and classifications may change over time.

Classification is used in defining what a <<Role>> may be a role of, and for phases, what a <<Phase>> is a phase of.

Classifications may be added to or removed from an individual over time and in different context.

#### *Base Classes*

- *Generalization*

### **12.2.7 Stereotype Concept Model**

A <<Concept Model>> is a kind of <<Model>> that represents concepts in a real or possible world. Instances of elements in a concept model are "real world" things, not data about those things.

#### *Base Classes*

- *Package*

#### *Direct Supertypes*

- *Model*

### **12.2.8 Stereotype Disjoint With**

A <<Disjoint With>> dependency is an assertion that two model elements do not and may not denote any of the same set of entities.

When applied to a classifier, every element of the classifier's extent (set of instances) is included in the set of disjoint things.

#### *Base Classes*

- *Dependency*

### **12.2.9 Stereotype Enumerates**

An <<Enumerates>> dependency asserts that the supplier of the dependency is a type and the client of the dependency is a package containing a complete set of possible instance specifications. In this way, <<Enumerates>> is more general than a UML Enumeration because it can enumerate more than just UML data types.

#### *Base Classes*

- *Dependency*

### **12.2.10 Stereotype Equivalent Class**

A <<Equivalent Class>> generalization is an assertion that two classes have the same extents (set of instances). Unlike ontological languages it is not assumed that the two elements are consistent, as statements from different context may or may not agree.

#### *Base Classes*

- *Generalization*

### **12.2.11 Stereotype Equivalent Property**

<<Equivalent Property>> is a declaration that a property is equivalent to one or more other properties (using "equivalent to") or is equivalent to a chain of other properties (using "chain"). <<Equivalent Property>> with at least one value for the "equivalent to" property is an alternative way of expressing <<Equivalent To>>, without introducing crossing lines on a diagram.

Either "equivalent to" or "chain" must have a value.

### *Base Classes*

- *Property*

### *Tag Definitions*

- ◊ **chain : Property [\*]**

An ordered set of properties forming a "property composition" expressing a traversal path that is equivalent to the stereotyped property. This is similar to a "property chain". (Note that in an OWL property chain, the property composition is not equivalent, it is a subproperty.)

Due to potential "missing information" in creating a chain, a chain may or may not be able to be determined from asserting the chained property. Such a determination is defined in the mapping rules for that property in a particular context.

Note that a chain may also be defined with mapping rules.

- ◊ **equivalent to : Property [\*]**

A set of properties that the <<Equivalent Property>> is equivalent to. Note that equivalence can also be declared with a <<Equivalent To>> dependency.

### **12.2.12 Stereotype Equivalent To**

An <<Equivalent To>> dependency is an assertion that two model elements represent the same thing or the same set of things. Unlike ontological languages it is not assumed that the two elements are consistent, as statements from different contexts may or may not agree.

### *Base Classes*

- *Dependency*

### **12.2.13 Stereotype External Reference**

<<External Reference>> provides traceability to the source of a "fact" in a model based on some external information resource. This references helps to facilitate provenance. Reference is a statement about the model data and has no semantic implication. Source reference may impact the trust in a statement but the evaluation of trust is outside of this specification.

External reference is combined with the owned comment(s) to create SIMF descriptions as defined in the SIMF meta model..

### *Base Classes*

- *Element*

### *Tag Definitions*

- ◊ **external reference : String**

Specifies the location URL of the external resource. The format must comply with [RFC3987].

○ ***external term : String***

The external term or location of the information in the source. The form of expression of the term or term path is dependent on the referenced technology.

#### **12.2.14 Stereotype Has Value**

A <<Has Value>> dependency asserts that the client of the dependency is a type and the supplier of the dependency is an instance specification that defines acceptable values for one or more properties of that type. Each slot of the instance specification is a value for a corresponding property in the type.

<<Has Value>> corresponds to one or more OWL property restrictions containing a "hasValue" constraint.

##### *Base Classes*

- ***Dependency***

#### **12.2.15 Stereotype Information Model**

An <<Information Model>> is a kind of <<Model>> that represents

a model for some purpose, independent of technical implementation. An information model may contain logical models or data models, as well as other logical viewpoints.

##### *Base Classes*

- ***Package***

##### *Direct Supertypes*

- ***Model***

#### **12.2.16 Stereotype Intersection**

An <<Intersection>> is a class that has an extent (set of instances) equivalent to the intersection of the extents of all supertypes. Intersection is a stronger statement than a subtype, as a subtype may be a subset of the intersection. An instance of all the supertypes implies an instance is also an instance of the intersection type.

For intersection, The SIMF profile considers UML generalization and UML realization equivalent. This is due to ownership and legacy considerations in UML. Generalization is the preferred representation.

Note: Realizations are included to support unions across external models. UML generalization can not be used across external models due to the ownership of generalization.

##### *Base Classes*

- ***Classifier***

### 12.2.17 Stereotype Is In Context

<<Is In context>> is an assertion that the client of the dependency is in the context of the supplier of the dependency. All assertions and rules defined in the supplier context apply to the client and everything in the context of the client (i.e., it is transitive). Packages, classes, situations and instances are typical contexts. Note that <<Is In Context>> is the default interpretation of a dependency, if no stereotype is specified it will be interpreted as <<Is In Context>>.

#### Base Classes

- *Dependency*

### 12.2.18 Stereotype Model

<<Model>> is stereotype of package that may have an id (see <<Resource>>) and/or a namespace prefix (like the "dc" in "dc:title").

#### Base Classes

- *Package*

#### Tag Definitions

- **namespace prefix : String**

A hint as to an appropriate abbreviation for a model that may be used in some technology mappings, such as XML. The prefix should be short and contain only letters and numbers and must start with a letter. e.g., "dc" in "dc:title".

#### Direct Supertypes

- *Resource*

### 12.2.19 Stereotype Phase

A <<Phase>> (a.k.a. "State") is a classification of an entity based on change of that entity over time. A <<Phase>> <<Classifies>> the types that may have that phase (e.g., "Teenager").

A phase is a "non rigid sortal", a type that may change over the lifetime of an entity.

#### Base Classes

- *Class*

### 12.2.20 Stereotype Quantity Kind

<<Quantity Kind>> is an aspect common to mutually comparable quantities represented by one or more units. Units with a common quantity kind may be algorithmically converted to any other unit of that quantity kind. e.g. temperature.[ JCGM 200:2008].

Units with a common quantity kind may be algorithmically converted to any other unit of that quantity kind. e.g. temperature. SIMF takes a wider view of quantity kinds to include conversions that may be contextual and time dependent, such as currencies.

#### Base Classes

- *Classifier*

#### Direct Supertypes

- *Value Type*

### 12.2.21 Stereotype Resource

A <<Resource>> is anything that can be referenced by an identifier in a model, ontology or vocabulary. This identifier is often an IRI.

#### *Base Classes*

- *NamedElement*

#### *Tag Definitions*

- *id : String*

A unique identifier for any resource.

When defined for a Package, id has the format defined in [RFC3987]. In this case, it is equivalent to UML:URI, and setting one will set the other.

### 12.2.22 Stereotype Role

A <<Role>> is a classification of an entity based on that entity's behavior, participation in a situation, or capabilities. A <<Role>> <<Classifies>> the types that may play that role. e.g., "Teacher".

A role is a "non rigid sortal", a type that may change over the lifetime of an entity.

#### *Base Classes*

- *Class*

### 12.2.23 Stereotype Sufficient

Specifying <<Sufficient>> for one or more of a type's properties means that an instance having an acceptable cardinality of values for all of those properties implies that the instance is an instance of that type.

#### *Base Classes*

- *Property*

### 12.2.24 Stereotype Synonym

<<Synonym>> defines an alternate name for the annotated elements of the comment. The alternate name is the body of the comment.

The alternate name will not be the "preferred name" of the element.

#### *Base Classes*

- *Comment*

### 12.2.25 Stereotype Union

A <<Union>> is a class that has an extent (set of instances) which is equivalent to the union of the extents of all types that specialize the Union (Subclasses). Specializing types shall include subtypes and types that realize the union.

Note: UML realizations are included to support unions across external models because UML generalization can not be used across external models due to the ownership of generalization.

[MathWorld] Given two sets A and B, the union is the set that contains elements or objects that belong to either A or to B or to both.

#### *Base Classes*

- *Classifier*

### **12.2.26 Stereotype Unit Type**

A <<Unit Type>> is a <<Value Type>> and an <<External Reference>> that represents a type of a quantity value referencing a specific unit. A Unit Type [?TBD] a required type of a property representing a quantity.

[JCGM 200:2008] A Unit is a real scalar quantity, defined and adopted by convention, with which any other quantity of the same quantity kind can be compared to express the ratio of the two quantities as a number. e.g. Degrees Centigrade, Miles.

Each unit type represents refinement of a quantity kind using generalization and is thus substitutable for that quantity kind. Typically quantity kinds are used in conceptual models and unit types in physical or logical models.

Unit types may only subtype quantity kinds and numbers.

Note that unit types are not units, but the type of quantity values expressed in a common unit as defined in [JCGM 200:2008].

Each instance of a unit type shares a common unit (as defined by standards) with a reference defined by "external reference" and "external term".

#### *Base Classes*

- *Classifier*

#### *Tag Definitions*

○ **offset : Real**

The difference between zero in the unit and zero in the base unit after the ratio is applied to the base unit as defined within the same model.

○ **ratio : Real**

The multiplier by which to multiply the unit to convert to the base unit as defined within the same model.

○ **symbol : String**

The accepted symbol for a unit. e.g. "g" for "Gram".

#### *Direct Supertypes*

- *External Reference*
- *Value Type*

#### **12.2.27 Stereotype Value Type**

A <<Value Type>> is a type representing an atomic unit of information without independent identity. Values include numbers, strings and enumerations. In some cases values may have internal structure.

Quantity kinds and units are also values. Values may stereotype any classifier. UML data types, including primitives and enumerations, are implicitly values.

#### *Base Classes*

- *Classifier*

## 12.3 UML Profile – SIMF Rules & Model Mapping Semantics

Rules provide a general framework for stating the consistency of and between SIMF models and elements. The primary use of consistency rules is for mappings between data models and conceptual models however a <<Rule>> may be used to assert consistency within a model, for example to represent generic assertions such as “all birds have feathers”. Rules are declarative in nature and intended to be implemented with a rules engine.

Mapping rules define how a particular data model or schema <<Represents>> information about the concepts defined in conceptual models. This facilitates an “n-way” mapping of information represented using different data models. Since conceptual models are not data models they do not have any particular representation for “data instances” of that model. Instances of a conceptual model would be the real things in the real world. The real-world concepts are the “pivot points” between the data representations. Of course implementations may automate data models that correspond closely to the conceptual model, but that is outside of this specification.

Due to the various ways to represent information, mappings can become complex. The UML representation of mappings simplifies these mappings and much as possible. Note that details of the mapping relations are defined in the profile specification.

### 12.3.1 Structure of Rule Specifications



Figure 48. Structure of Rule Specifications

There is an expected structure for defining rules. This normally starts with a <<Rule Model>> package that contains other rules. Note that any “namespace” can contain rules, including classes. By default, rules will hold within the namespace they are defined in but another namespace may be specified by setting the <holds within> tag of a rule. Packages stereotyped as <<Rule Model>> are considered to hold universally within any model in which they are included. Within a rule context, such as a <<Rule Model>> there may be generic rules marked as <<Rule>>, <<Represents>> rules or <<Mapping Rule>>s.

<<Rule>>s and <<Mapping Rule>>s contain <<Pattern Element>>s that define the pattern of the rule. Pattern elements can be UML “Parts” (which are properties), connectors and connector ends. There are various stereotypes for pattern elements to further define their effect on the pattern. A <<Mapping Rule>> may also contain <<Map Rules>> which specify how different pattern elements may represent the same facts. Mapping rules are bi-directional and can map changes between “either side” of the mapping.

The difference between a <<Rule>> and a <<Mapping Rule>> is that a <<Rule>> simply states something that must hold (be true) within a model. For example, that fish can swim. A <<Mapping Rule>> creates a correspondence between different representations of the same facts using <<Map>> rules.

### 12.3.2 Rule Model

<<Rule model>> is a stereotype of a package to indicate that the contents should be asserted and validated as rules.



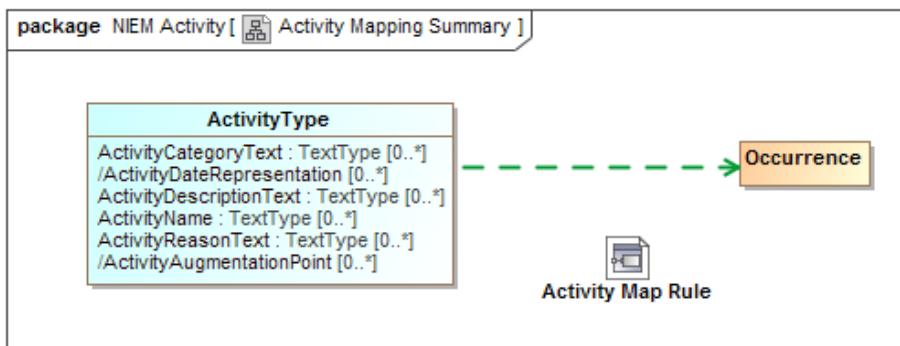
**Figure 49 Example Rule Model**

The package SIMFProfileToModelMapping is a rule model and will hold within any model in which it is included.

### 12.3.3 Representations

The foundation of mapping is the <<Represents>> dependency between classes. Represents says that a particular type found in a logical or physical model represents information about a concept in a conceptual model. By default, <<Represents>> does not implement a mapping, it defines what elements can be mapped and thus restricts mappings. For simple “one-one” mappings there is an optional tag for <<Represents>> to <<map-all>> known instances of one type to another.

#### Example



**Figure 50 Activity Mapping Summary Example**

The above example shows that an “ActivityType” from NIEM-Core represents an Occurrence as defined in the threat/risk conceptual model. By convention we show the represents dependency as a green dashed arrow and do not explicitly show the represents stereotype. Representations provide the highest level of mapping. This diagram also shows that there is a more detailed activity map rule which will map the properties and relationships between these types.

What this means is that *some* ActivityType instances represent *some* information about occurrences in “real world” activities. This also implies that relationships involving an occurrence can be validly mapped to relationships involving an activity and that properties of an occurrence can validly be mapped to properties of an activity.; <<Represents>> relations provide type-safety for mappings.

What this does not say is that ActivityType and Occurrence are equivalent and can necessarily be mapped 1..1. How they are mapped is detailed in mapping rules. However, if the <<map-all>> tag of <<Represents>> is set true then ActivityType and Occurrence will be mapped 1..1, bidirectionally (mapping of types and properties is considered independent, each property must also be mapped). Note that <<map-all>> implies nothing about the properties and relationships, only the mapped types (each type, property and relationship is an independent concept that is mapped independently).



**Figure 51 {map all} Example**

In **Figure 27** all UML classes stereotyped as <<Role>> will be mapped to the Role class in the SIMF model.

#### 12.3.4 Mapping Rules

The detail of mappings happens in classifiers stereotyped as <<Mapping Rule>>s. Mapping Rules define patterns of data types and patterns of concepts that have map correspondence rules. The <<Map>> correspondence rules do the real work, mapping element by element.

Mapping representation rules are, externally, not that interesting. They are just a class (or component) stereotyped as <<Mapping Rule>>. However, note that Mapping Rules may specialize other rules – in which case they include the more general rule but may restrict the <<Match>> elements. Mapping rules may also <<Subsume>> other rules, in which case they take precedence over the other rule.

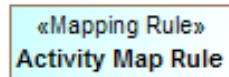


Figure 52 Representation Rule External Example

The above defines a mapping rule for activities that is an assertion that the enclosed pattern must hold and provides a context (in this case the enclosing package) where the map rules are asserted. If we look inside the Activity Map Rule we see the structure and maps.

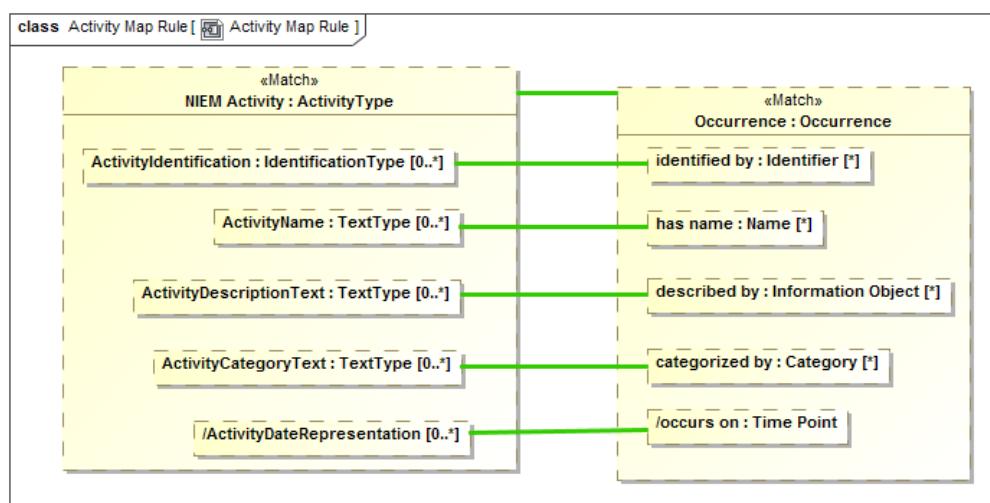


Figure 53 Representation Rule Internal Structure

The above example is the internal “structure” of the Activity Map Rule. In this case the mapping is very 1..1 and simple. Inside of the rule we see “parts” that represent “ActivityType” named “NIEM Activity” and “Occurrence” named “Occurrence”. The green line between them is a “Map” rule, represented as a UML connector stereotyped as <<Map>>. This states that in this simple pattern NIEM Activities and Occurrences map 1..1. We could also have put filter constraints on that mapping, but in this case did not.

We also see the “<<Match>> on “Occurrence” and NIEM Activity. Match defines the “starting point” for the pattern with respect to the model containing the <<Match>> element. A mapping engine will find all instances of Occurrence (in any data format) and map those to NIEM Activity. It will also find all NIEM Activities and map them to Occurrences. All other parts of this mapping become relative to the “Match” elements.

Within both NIEM Activity and Occurrence we see other parts, parts of those types. The green lines create mapping assertions between those parts *within the context of this rule*. This within this rule “ActivityName: maps to “has name”.

A map correspondence is essentially “best efforts”, the types of the mapped elements must either match or have a mapping rule that allows them to be mapped. If, for example, an occurrence had an identifier that was an image and

NIEM did not allow for image identifiers, that “fact” would not be mapped. How a mapping engine handles maps excluded by type is outside of this specification.

Mapping for primitive data types, such as strings and numbers, is provided by the mapping engine implementation based on each mapped technology. This allows, for example, an identifier that is represented as an integer to be mapped to a string.

The important point to remember is that mapping any fact requires that the types are compatible. That type compatibility is defined by <>Represents<> rules between the types. The requirement for type matching may be overridden by setting the <coerce> tag of the <>Map<> rule, but in most cases type safety of <>Map<> rules is desirable.

In that there may be multiple <>Map<> rules between the same thing, one can be marked as the <>Default<>. A default rule will be applied only if no other rules have fired.



Figure 54. Default <>Map<> Example

Figure 30 shows a <>Mapping Rule<> fragment of three properties mapped to one based on types of the identifiers. If none of the more specific identifiers match “OrganizationOtherIdentification” will be the default. Similar defaults may be defined for subsets.

### 12.3.5 <>Match<> Elements

The foundation of SIMF rules is patterns. When a rule is asserted the SIMF implementation attempts to “match” the pattern to existing situations and then “assert” that the pattern is “true”. The <>Match<> elements are those that must *pre-exist* for the pattern to even be considered. Relating this to a SQL Query, the <>Match<> elements would be in the “Where” clause.

If there is more than one related <>Match<> element, they must all be “true” for the pattern to hold (be asserted). If there are any constraints for the <>Match<> elements they must also hold. Constraints include condition expressions, the type(s) of the pattern elements and multiplicities.

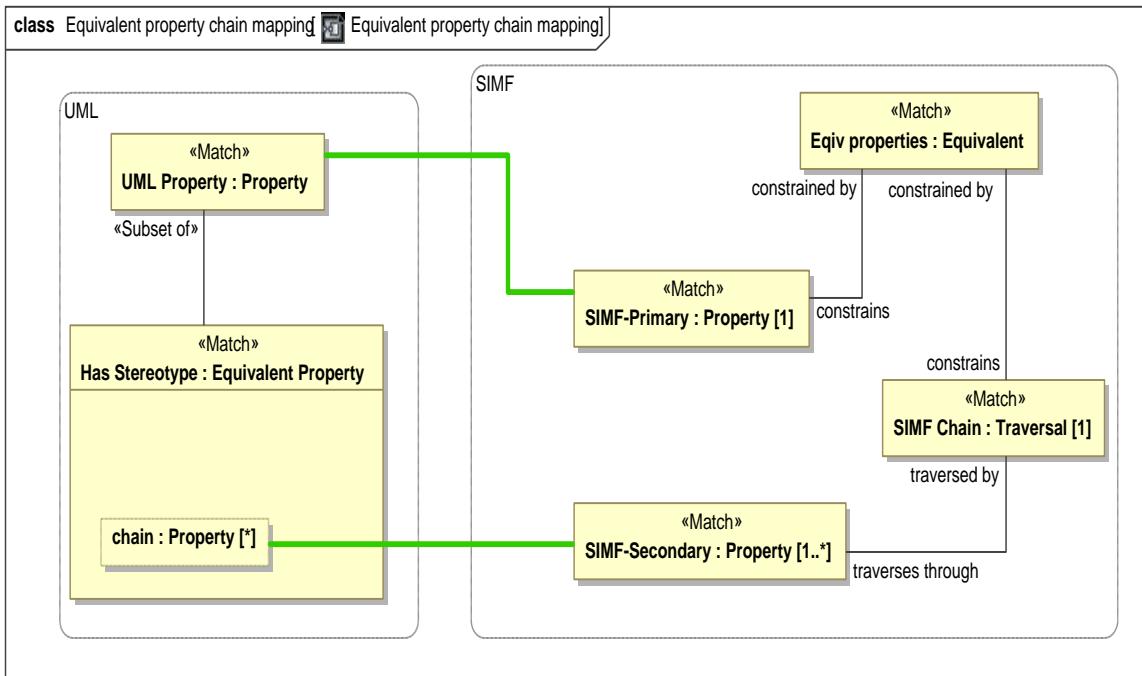
Once a pattern is <>Matched<>, all properties, relationships and subsets from the match elements are “filled in” from existing information.

What happens if, as these other elements are being filled in, some other constraint is violated? This depends on the kind of rule. For a general rule the constraint will be asserted – made to be true by attempting to each required element. In the case of a mapping rule the rule is in an error state, the behavior of an implementation in response to an error state is implementation specific.

In a mapping rules, after the <>Match<> elements have been matched and any relationships followed, any <>Map<> rules for the pattern are applied.

Note that for a mapping rule there will be two “sides” that are matched – normally the “Conceptual” side and the “Physical/logical” side. Each “side” is considered a separate match set. Sides are determined by <>Match<> elements connected by anything other than a <>Map<> rule.

Figure 28 shows simple a <>Match<> that is simple – just matching a single element on each side. The next example shows more complex matches.



**Figure 55. More Interesting <<Match>> Example**

Figure 29 shows very specific match patterns on both sides. On the UML side (left) a <<Match>> property must have a subset that is a <<Match>> Equivalent Property stereotype (this means match all properties that have the <<Equivalent Property>> stereotype applied. If “UML Property” is not a “Property” or there does not exist a subset of it that has the type :Equivalent Property then this “side of the pattern doesn’t match.

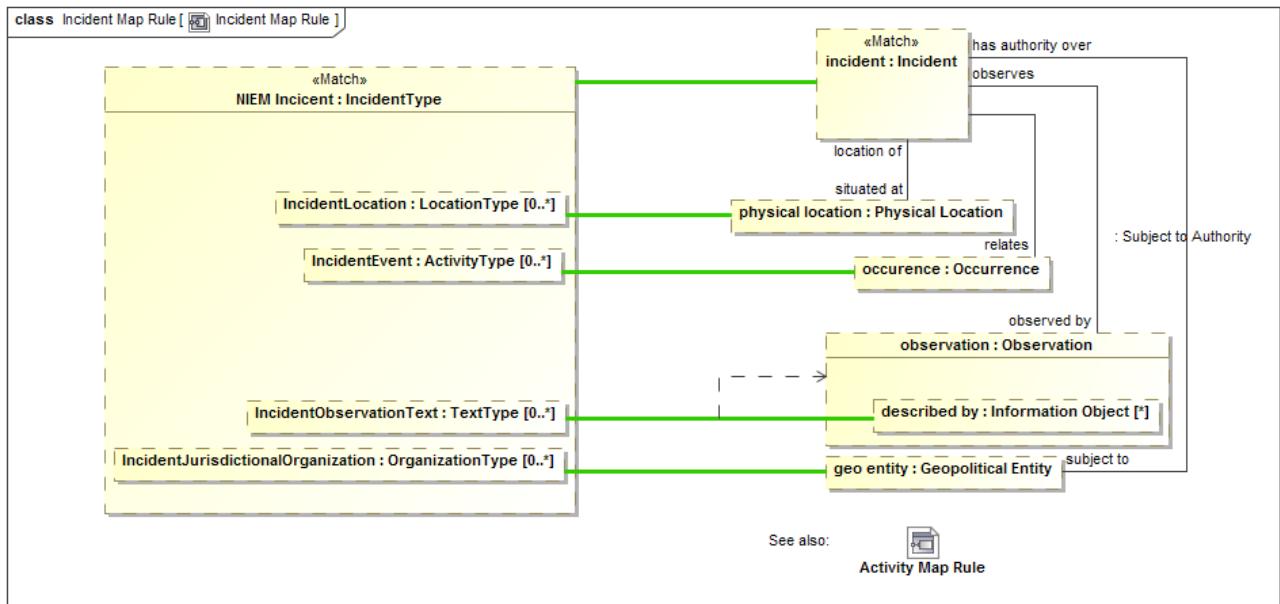
On the other side (the SIMF meta model) there must be a pattern of an “Equivalent” constraint that constrains exactly one “Property” and also constraints exactly one “Traversal”. These patterns are very specific because there are very specific ways to represent general concepts (like equivalence) in the UMLprofile.

Once a pattern on one side is matched, the other side is “asserted”, creating the required elements.

### 12.3.6 Pattern element traversals and patterns

The above Activity Map Rule is simple and 1..1, when we get such a simple mapping we shout for joy – because our job is easy. However, there is frequently complexity on “both sides” of the mapping – something in the data model may map to multiple things in the conceptual model or require a “Path” through multiple concepts. Likewise, there may be intermediate “technical artifacts” that have no real meaning in a conceptual model. This is why we say we are mapping patterns.

For our next example we will look at Incidents, which are a subclass of activities in NIEM and occurrences in the threat/risk conceptual model. Since these are subclasses on “both sides”, we only need to describe the additional properties of an incident.



**Figure 56 More detailed map rule**

The example above shows how a NIEM Incident (named NIEM Incident) maps to a conceptual incident (named “incident”). Incident Map is a subtype of Activity Map so the Activity map rules will all apply to incidents so we don’t need to repeat them here.

We will start with a <<Match>> of “Incident”. Note the line from “incident” to “physical location” labeled “situated at”. The mapping engine will start with an incident and fill in the set of “physical locations iff the “situated at” relationship exists *for that instance and what it relates to is a Physical Location*. If that relationship does not exist, “physical location” will be null (empty). Note that physical location could also have multiple values since “situated at” does not have a restricted cardinality.

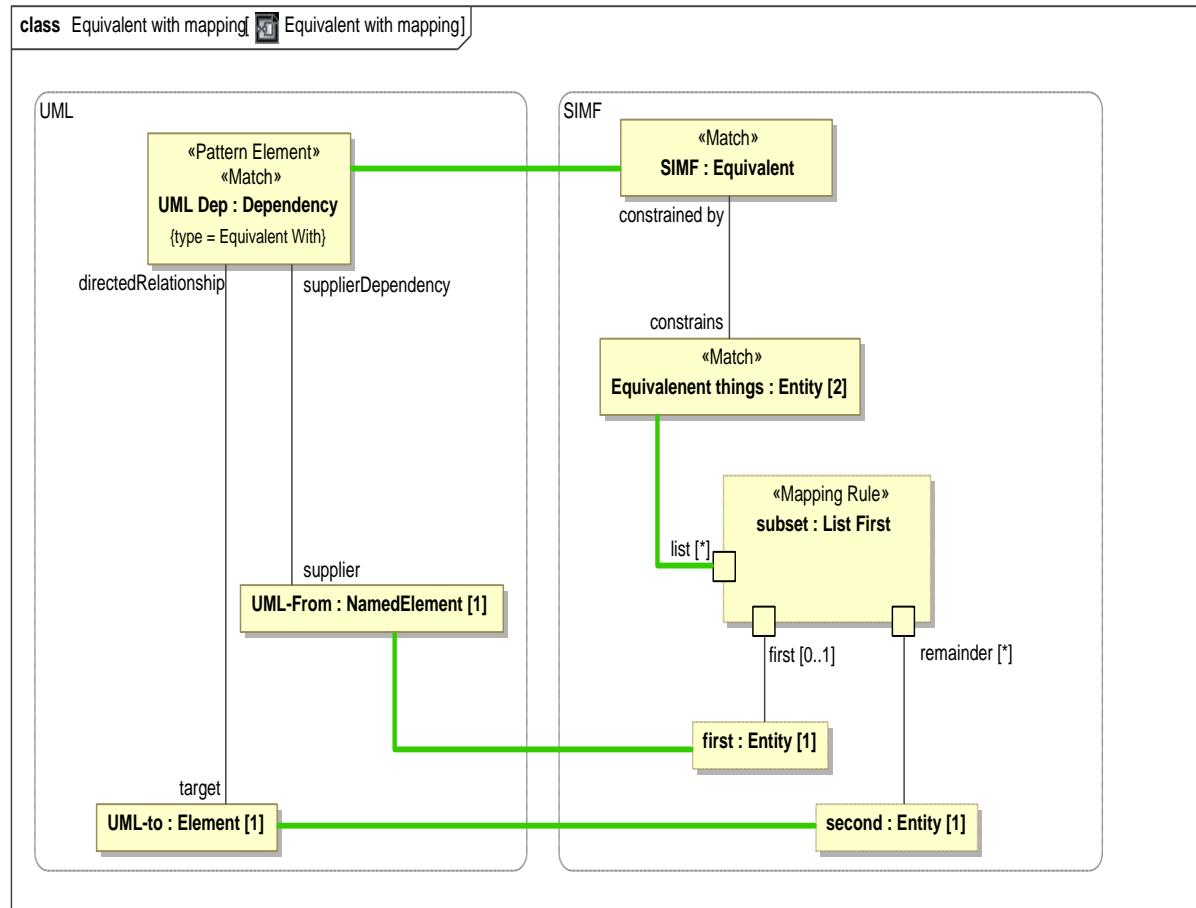
The values that “end up” in “physical location” will be mapped to “IncidentLocation” in NIEM. Likewise, any mapping in the other direction will hold – any populated “IncidentLocation” will populate “physical location” as well as the relationship to an incident. Once the rule is satisfied, the pattern will hold for all instances of NIEM IncidentType and Incidents. How cardinality mismatches are handled is not specified by SIMF, a mapping engine could, for example, log issues.

Now consider the element “described by” within “observation”. This will be populated if the “has observation” relation exists from an incident *and* that instance has a “described by” property. IncidentObservationText is mapped to “described by” within such an observation. But, in this case, UML notation is a bit misleading, “described by” is a part of the Observation type, not this particular observation part. Since other objects in this rule may have a “described by” property it becomes non-deterministic which “described by” we are talking about. We want to say that we are mapping to the “described by” in the context of the “observation” part. The dependency from the green line to “observation” defines that the context of this map rule is only valid in the context of “observation”, thus making the map deterministic. As many context dependencies as are necessary may be specified for any map rule. All map rules are considered to be in the context of the enclosing Representation Rule. <<Match>> properties take precedence for resolution - some tools may report if a map is non deterministic.

### 12.3.7 Multiplicity constraints in patterns

It is sometimes necessary to constraint pattern properties to have a specific number of values. This may occur either in matching the pattern or as the result of following various paths. The same multiplicity constraint that is used to constrain other properties, such as on the ends of relationships, may be used to constraint pattern properties. Multiplicity constraints may also be used on the “ends” of connectors between pattern properties, to constraint the number of relationships (actual ground facts) that must exist between the pattern properties.

Setting the multiplicity constraint of a pattern property constrains it to have the specified set of values. If a <<Match>> is constrained, the pattern must match the constraint. If not a match, the pattern multiplicity will be satisfied by the rules engine. If, for any reason, this and other constraints cannot be satisfied the issue will be handled by the rules engine. The method for handling constraint violations is not specified.



**Figure 57. Example of setting multiplicity constraints on <<Match>>**

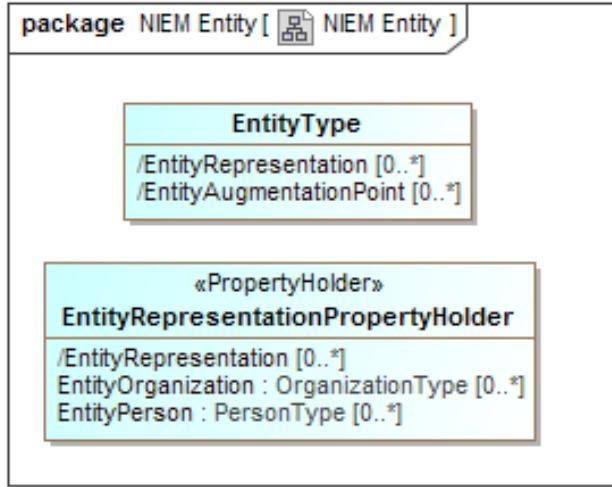
In the above example a SIMF Equivalent has exactly 2 <constrains> entities. This is the condition for matching the pattern. This matching pattern then maps the Equivalent constraint to a UML dependency stereotyped as <<Equivalent with>>.

Once these base patterns are mapped the two mapped entities will be mapped to the <supplier> and <target> of the UML dependency via a “List First” rule. The List First rule separates a list into its first and remaining elements.

### 12.3.8 Subsets of Pattern Elements

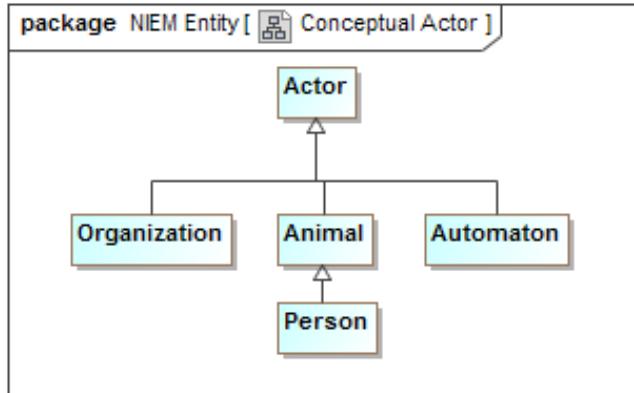
Conceptual models use sub classing, multiple inheritance, roles and phases to more accurately and intuitively represent the domain of interest. Many data technologies do not support these concepts and even if they did, would probably structure implementation classes differently. In other cases, there may be restrictions on the “extant” of what maps to what that require calculations or other constraints. To provide for these cases we use <<Subsets>> in mapping patterns. A subset defines another part (property) that holds a subset of the instances of the superset part, based on the type, relationship values and other constraints of the subset part.

To understand this feature we will first look at models for “Entity” and “Actor” in NIEM and the threat conceptual model, respectively.



**Figure 58 NIEM Entity Example**

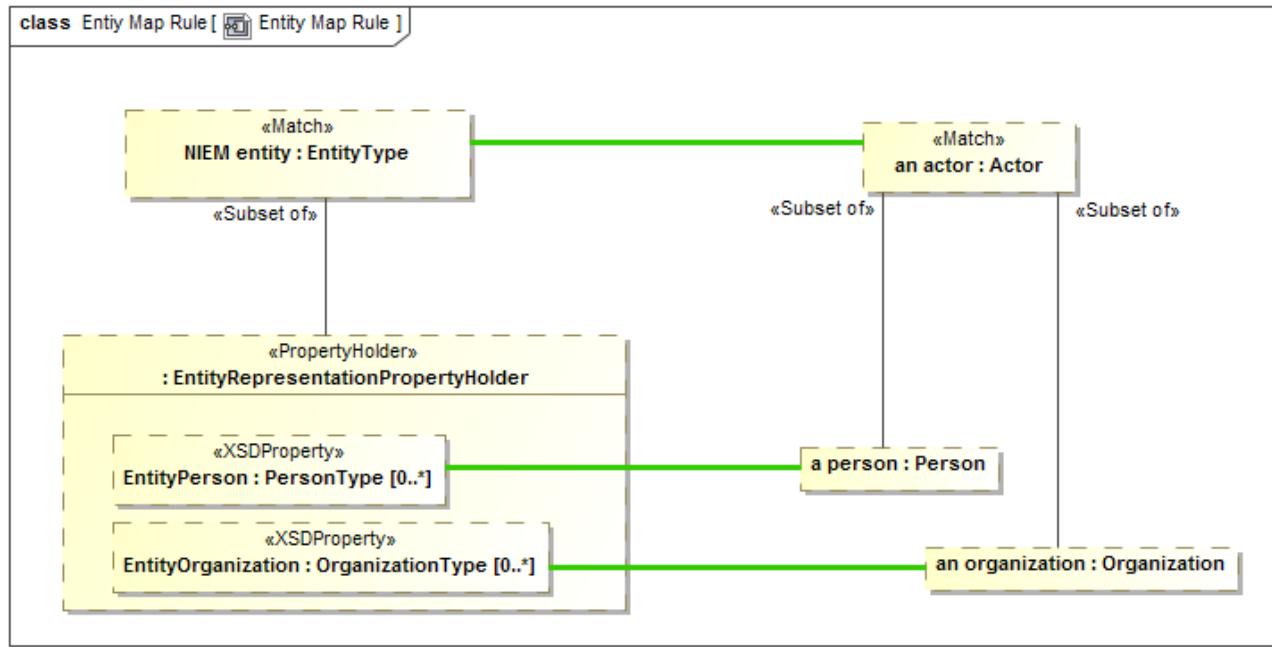
In NIEM, an “EntityType” has a “substitution group” property with properties that can be “EntityOrganization” or “EntityPerson” to allow the entity to represent one or the other. The general rules for mapping NIEM state that substitution groups are considered subtypes of the primary type.



**Figure 59 Conceptual Actor Example**

In the Threat conceptual model “Actor” is a Supertype of Organization and, indirectly person. It is also a Supertype of “Automaton”. An Automaton can’t be an actor in NIEM so it will not be mapped (However we could define a NIEM extension to allow this).

We want to map actors to NIEM entities, but see that they are very different “shapes”.



**Figure 60 Subset part example**

In the above example we see the actor - EntityType mapping. Notice “a person” of type “Person”. “a person” is defined to be a <<Subset of>> actor – that is every actor that is of type “Person” will populate the “a person” part. If an actor is not a Person, “a person” will be null. “a person” is then mapped to “EntityPerson”, a property of “Entity” by way of the substitution group (sorry that this gets into some NIEM substitution group details, but you probably get the basic idea).

Likewise, “an organization” will map to EntityOrganization iff “an actor” is an Organization. Note that if “an actor” is neither of these, it will not map to any NIEM property.

Note also that there could be other constraints on the subset parts, such as required relations or constraint expressions.

### 12.3.9 <<Pattern Element>> computations and constraints

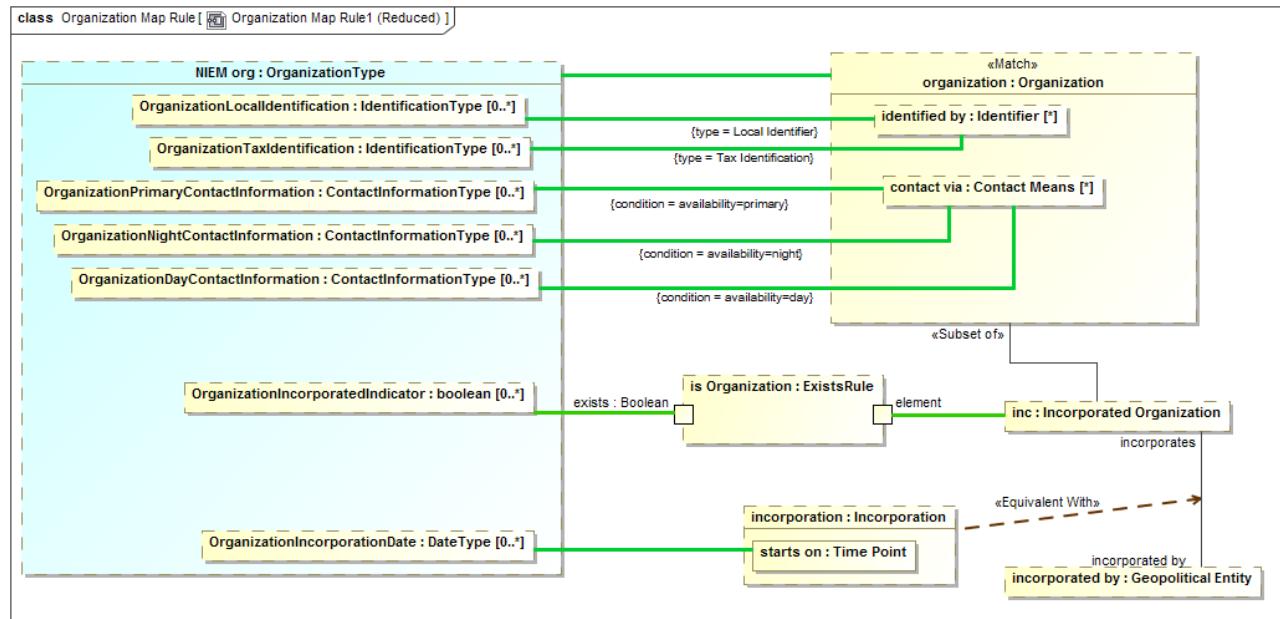


Figure 61 Map constraints example

To continue the tour of the primary mapping capabilities we will look at a subset of the “Organization” mapping.

Note the “type=” on two maps to “identified by”. In the conceptual model there are subtypes of identifiers. In NIEM there are special properties for some of these identifiers. The “type=” constraint on a map says that the map will be constrained to the type (on the specified end) of the actual instance matched the specified type. So “OrganizationLocalIdentification” will only map to “identified by” if the type of the identifier includes “Local Identifier”. Likewise, “OrganizationTaxIdentification” will only map to “identified by” if the type includes “Tax Identifier” (remembering that a SIMF concept instance can have multiple types). Likewise, the reverse is true; those properties will “assert” the type of the identifiers they reference.

On the maps to “contact via” we see “condition=”. Condition is a tag of <<Pattern Element>> that references a UML expression. The conditions referenced are properties of the association between an organization and “Contact Means”. The maps will be constrained to the “availability” property is set as indicated. Likewise, if an organization is being created, that property will be set by the same condition.

Note that “inc” is a subset of an organization only if it plays the role of an “Incorporated Organization”. In NIEM there is a Boolean set if the organization is incorporated. The “ExistsRule” is a computation rule (that is its implementation is outside the specification). But in this case ExistsRule’s behavior is defined – the exists Boolean will be true when the mapped “incorporated” has some value. This results in the NIEM “OrganizationIncorporatedIndicator” corresponding to the organization being incorporated.

If the organization is incorporated it will have an incorporation relationship to its incorporating body (incorporated by). That incorporation relationship will contain its date of incorporation, which is mapped to the NIEM property. In UML association classes have to be put into a structure like this in two pieces, the “line” and the “box”. Since both the line and the box represent the same “fact”, they are asserted to be equivalent – this is only required when association class properties need to be accessed and is required because UML has no way to show connectors as association classes.

The end result is that the more “flat” representation of an Organization in NIEM is mapped to the concept model.

### 12.3.10 <<Pattern Element>> strength

A connector between parts will both follow a relationship and assert that relationship. There are times when the “strength” of a rule implied by a connector needs to be more explicitly specified. The <strength> tag of <<Pattern Element>> allows different options for what is asserted by a connector. These are: match, assert, default and exists. The default is “assert”.

Definitions of each of these is in the reference section. In the following sections we will provide some examples. Note that strength=Match is the same as the <<Match>> stereotype and is not repeated here.

### 12.3.11 <<Pattern Element>> strength=Assert

Assert, the default, defines a pattern element. A pattern element operates in two modes: Pattern match and assertion.

When the <<Match>> elements match an existing situation the rule is considered to have “fired”. Properties and relationships of the matched elements, that are represented in the pattern as <<pattern elements>>, are “filled in” by following paths from the <<Match>> elements through properties and relationships to other pattern elements. Note that property elements may be null, contain a single element or contain sets of elements.

Once elements are matched and the properties and relationships followed, the <<Map>> rules “assert” that corresponding elements represent the same “facts”, perhaps in other forms or structures. Relationships between the elements, also represented as pattern elements, are then also asserted between the mapped elements. In this way the entire pattern on “both sides” (if it is a mapping pattern) is “made consistent”.

Strength=assert defines a pattern element as playing both roles – as a part of the pattern match “query” as well as what should be asserted within a pattern.

### 12.3.12 <<Pattern Element>> strength=Exists

In some cases it is required that we match a pattern but do not “assert” that some element or relationship exists, but if it does exist we need to apply some more rules. “Exists” will test for an element with creating it.

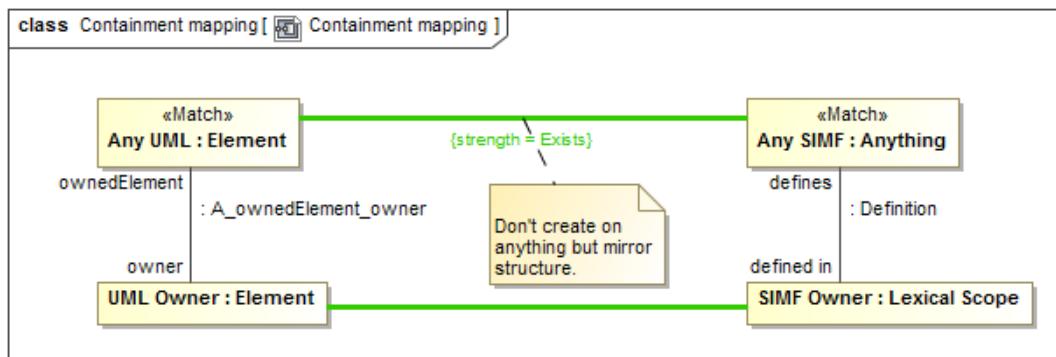
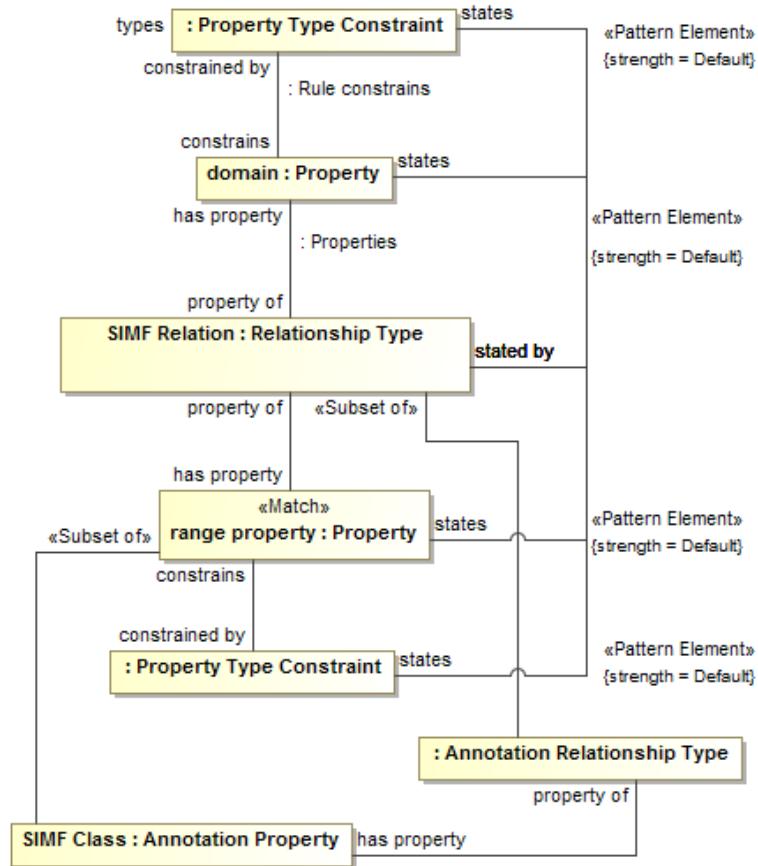


Figure 62 strength = Exists example

In mapping UML to SIMF we do not necessarily want to map every element. But where there are mappings we would like to make the ownership hierarchies match. A match of “Any UML” has a <<Map>> to <<Any SIMF>> but the <strength>> is specified as “Exists”. This means that they should be mapped if the elements exist but the mapping should not be asserted by this rule (it may be asserted by other rules). Where they do exist, the UML owner should be mapped to the SIMF owner.

### 12.3.13 <<Pattern Element>> strength=Default

Model information can come from multiple sources, model organizations and rules. There are times where a pattern element should be a default, asserted only if no other source is asserting the same element.



**Figure 63 strength = Default example**

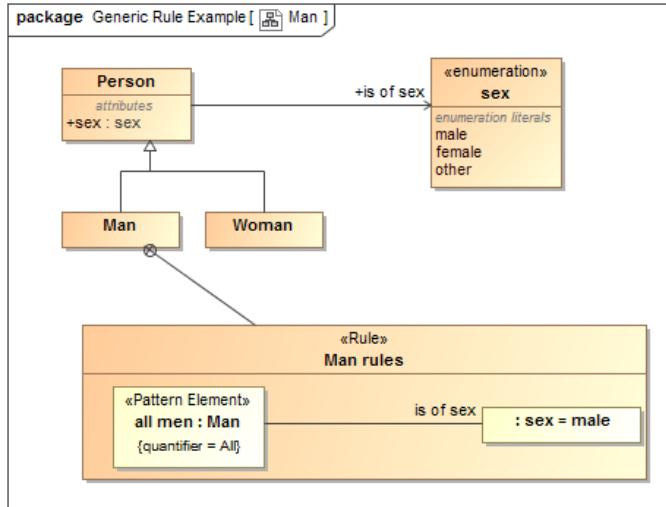
In the above fragment we see several states/stated by connectors that have strength=Default. What is intended is that “states” (which defines model organization) will be asserted by this rule only if the value is not asserted by some other rule.

### 12.3.14 <<Pattern Element>> quantifier

There are times when we need to define generic rules, not specific to a mapping or populate rule variables based on the entire extent of a type, or some constrained subset of the extent. In logic this is done with “quantifiers”. A <<Pattern Element>> may have a <quantifier> tag that specifies the content of a pattern property based on the extent of its type.

The quantifier can have values of: None, There Exists, Exactly One, Some, Most, All or Match. Note the close correspondence of quantifiers with those in predicate logics (with some extension). Definitions of each of these is in the reference section.

The quantified properties may then be used as the ends of relationships, making assertions about the set of quantified things.



**Figure 64 Generic Rule Using Quantifiers**

In the above example we assert the fact that “all men <is of sex> Male” in a <<Rule>> called “Man rules”. This rule is owned by (and therefor in the context of), the class “Man”.

The pattern element named “all men” has a type of “Man” and a quantifier=All. This means that the element will be “filled” with all men, statements made in this rule will apply to all men. We then have a connector typed <is of sex> to “Male”. This asserts that all men are male.

Note that quantified elements can also have connectors to other quantified elements, so we could say things like “all men like Most tools” or “John likes all supermodels living in New York”.

Note that how rules are resolved is implementation specific. Some “inference” systems may create new facts while others may check that certain facts are correct.

### 12.3.15 <<Pattern Element>> explicit

Most elements are mapped regardless of their source – explicitly asserted in a model or derived based on rules. There are times where only explicitly asserted elements need be mapped. In this case the element is marked with the <explicit> tag as TRUE.

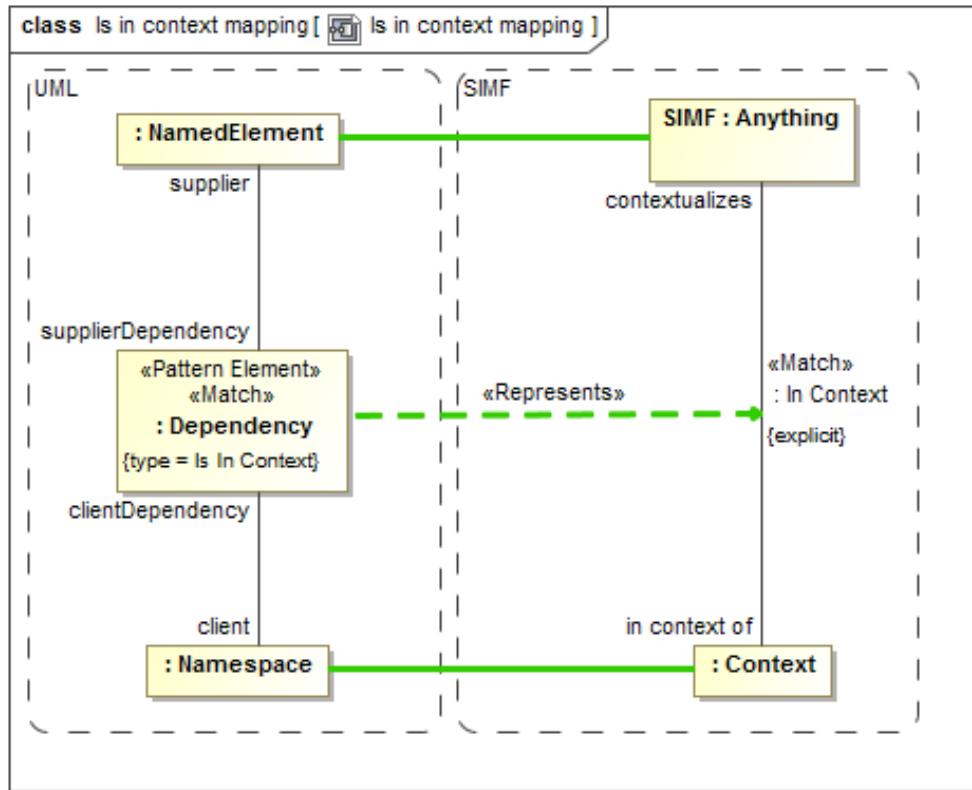


Figure 65 Example of "explicit" pattern elements

The above example shows that the “in context of” relationship in SIMF should only be mapped to UML if it is explicitly asserted.

### 12.3.16 Property Chains

Rules may also be used within a conceptual or logical model, an example being the “property chain” concept from OWL which allows a “path” through properties to be equivalent to another property.

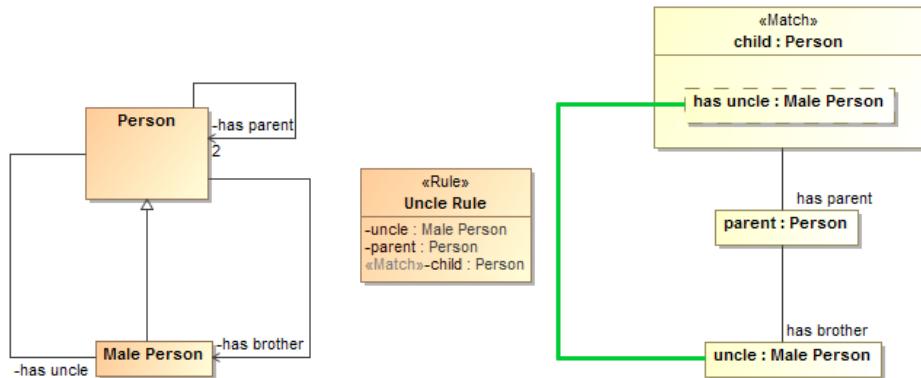
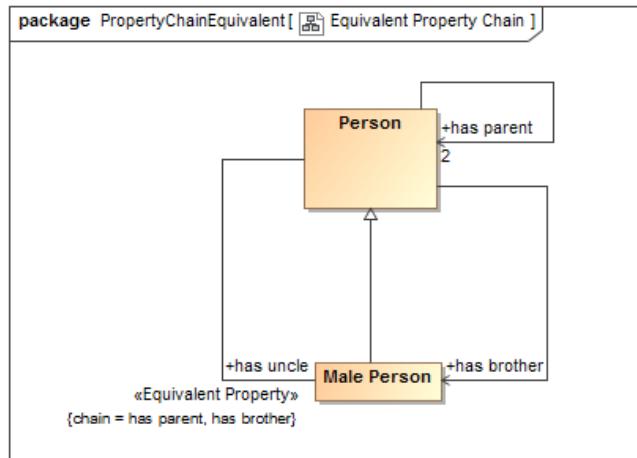


Figure 66 Property Chain Example

In this example we see a simple model of a person with parents and male people that can be brothers or uncles. The “Uncle Rule” states that the “path” through “has parent” to “has brother” <>Map>>s to “has uncle”.

The above is one way to specify a chain, another would be with the <chain> tag of an <<Equivalent Property>> which is more compact but less powerful.

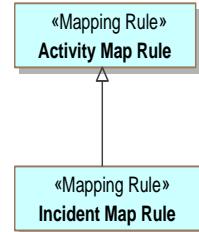


**Figure 67 Property Chain as Equivalent Property**

The above example says the same thing as the property chain rule, using the more compact <chain> tag of <<Equivalent Property>>

### 12.3.17 Pattern Precedence

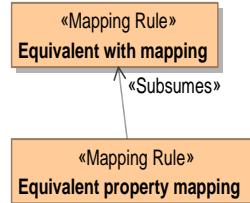
It is possible for more than one pattern to match for the same set of values. The general rule is that all patterns that match will execute. Where this may produce redundant elements a pattern may either subtype or subsume another. Where a pattern subtypes another and the more specific pattern matches, the more specific pattern will include the rules of the more general pattern.



**Figure 68. Example of Pattern Generalization**

An incident is a kind of activity. The incident rules subtypes and subsumes that activity map. An activity that is an incident will use the incident map rules as well as the sub-rules defined within activity.

Where a pattern uses a <<Subsumes>> dependency, if the <supplier> pattern matches it will prevent the <target> pattern from executing for the same set of values.

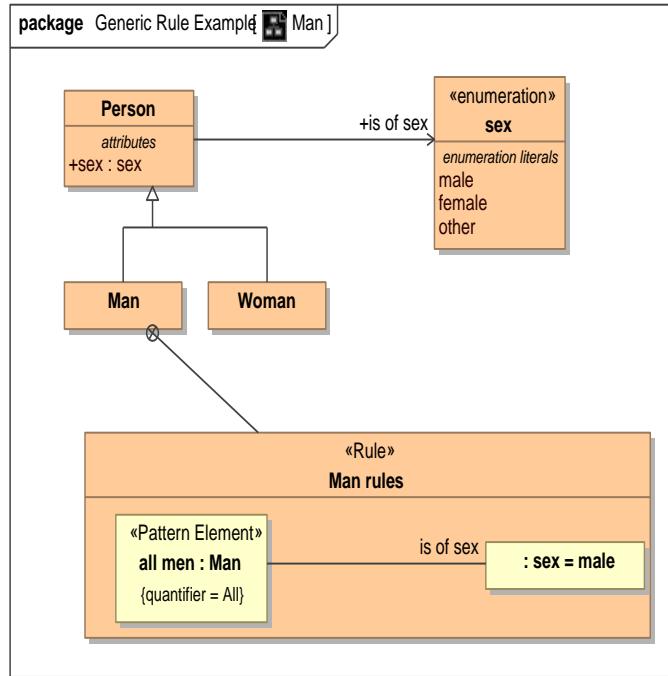


**Figure 69. Example of Rule Subsumption**

Using “Equivalent With” is more general but >Equivalent Property” more compact. If equivalence can be expressed with “Equivalent Property” it subsumes “Equivalent With”.

### 12.3.18 Generic Rules

Most of our examples have used mapping rules. Rules are also generic patterns that can be asserted to hold within some context. Generic rules generally use quantifiers rather than <<Match>> but can be stated either way. A quantifier defines a pattern property that contains a set of instances defined by the property type. The quantifier specifies how many instances will be in the set from none to all.



**Figure 70. Generic Rule Example**

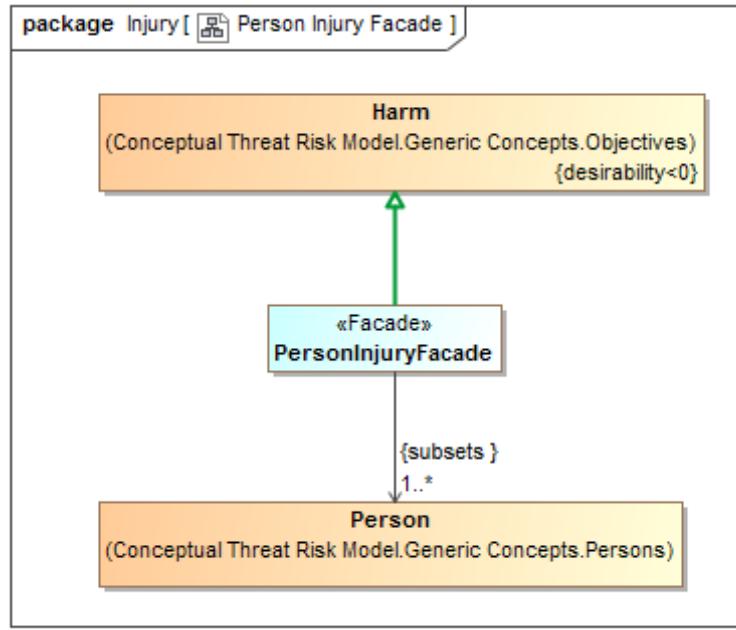
Figure 47 provides an example of a generic <<Rule>>. The rule states that as part of the definition of the class Man, the “Man rule” applies which says that all men <is of sex> male. The Pattern element “all men” has “quantifier = All” which is really what makes it represent all men, not the name. “all men” then has a relationship to a constant “sex = male” (the default value of a property is considered its value). The result is the “assertion” that all men will have the same sex.

Note that more than one property may be quantified, for example we could say “All men like at least one supermodel” by quantifying “a supermodel” with “quantifier = There exists” and creating a connector “likes” between them. Options for quantifiers are: None, There Exists, Exactly One, Some, Most, All. Note that for an interpretation in first order logic, There Exists, Some and Most are the same, even if they may have an intuitive distinction. In other logics concepts like “Most” may offer a default.

### 12.3.19 Facades and Representation Computations

In some cases, it is desirable to have mapping rules as “reusable pieces” that can provide a “Face” to a model that fits better for one or more mapping rules. There is also the case where these rules fall outside of the expressive power of mapping rules and are best done in calculations (program code or fUML models).

Facades provide for making a new “face” of either a conceptual model or data model element. A Façade is a class with additional properties and/or relations that can be derived from the element it represents. Either mapping rules or computations are then used to “populate” the façade or map the façade back to what it represents. The façade implementation keeps the façade properties consistent as any connector implies change in a property value.

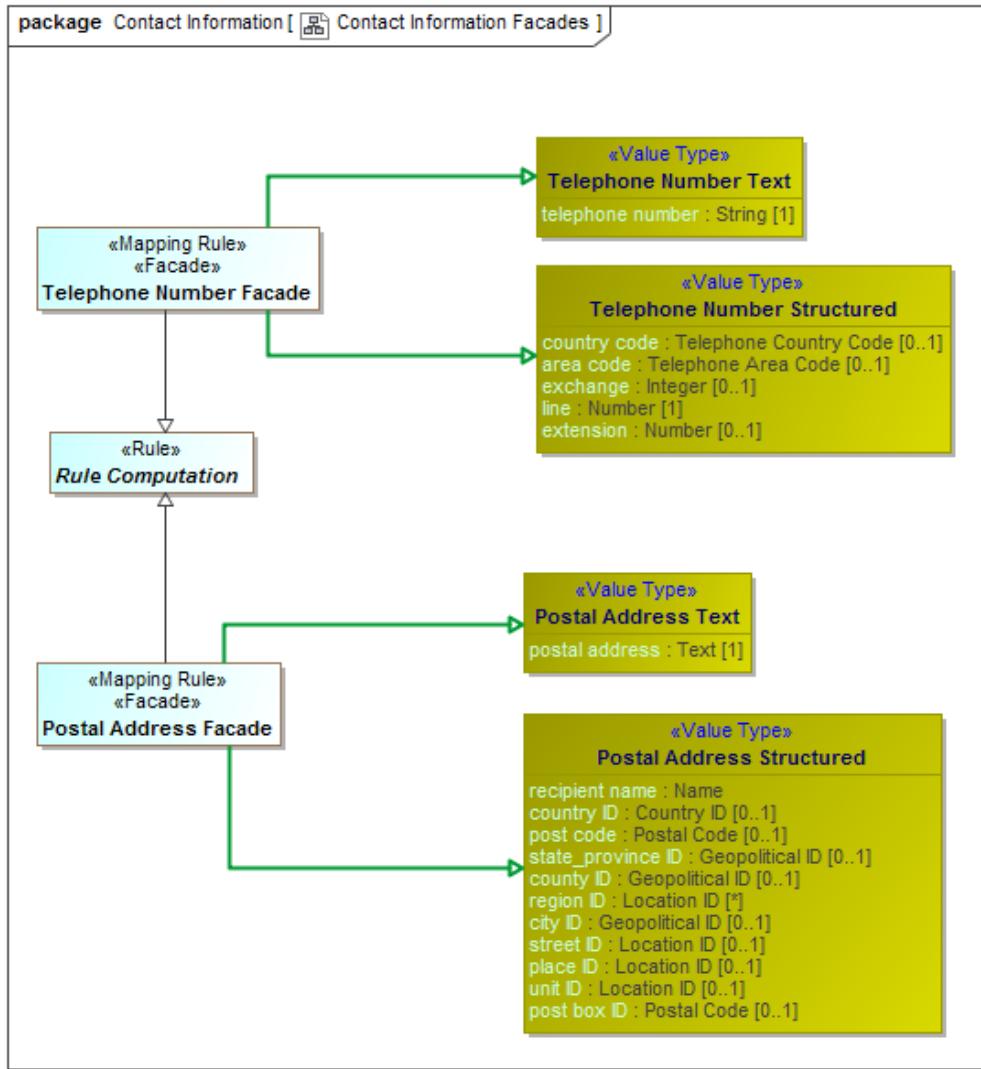


**Figure 71 Facade Example**

The “PersonalInjuryFacade” above represents the concept of “Harm” but only where the harm impacts a Person. In NIEM, injury is only considered relative to a person – so this façade provides such a “View” of the conceptual model, harm restricted to personal injury. In this case no additional representation rule is required, but such a façade could also define new properties or associations that would be populated in the same way as a data model.

Note that in this case the <<Represents>> relation is applied to a generalization to assert that “PersonalInjuryFacade” includes all of the features of “Harm” and is also a representation of it.

Facades can also use “Computations” or Representation Rules to define their properties.



**Figure 72 Computation Facade Examples**

In the above example both a telephone number façade and address façade are “computed” based on combining both a structured and unstructured representation of telephone numbers and addresses. The specific computation is external to the specification and defined by implementations. These implementations could be implemented in any language, including “ALF”, the executable language of UML.

The mapping engine is responsible for implementation of computation behavior and should update a computed Façade whenever any of its elements changes (some implementations may group such changes in a transaction).

In summary, facades and computations provide for reusability and extensibility of mappings.

## 12.4 SIMF Profile::SIMF Rules Profile Reference

The SIMF rules profile defines the way to model rules and mapping within and between data sources via a conceptual model.

### 12.4.1 Diagram SIMF Rules Profile

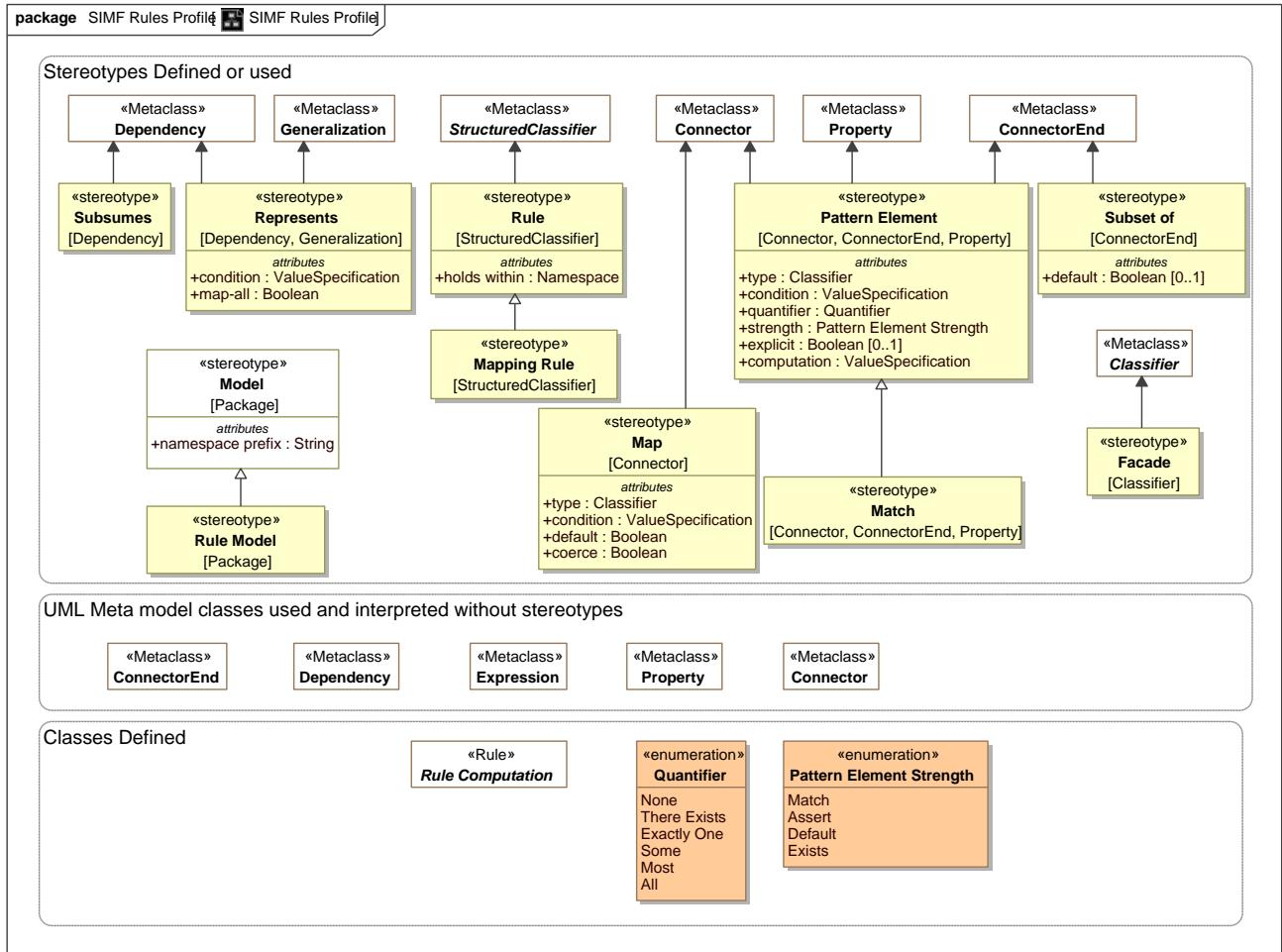


Figure 73 SIMF Rules Profile

Computation computes a value for the mapping end based on the expression applied to the mapped property or relationship.

Where computation is used inverse mapping is not specified - any inverse mapping is implementation specific.

### 12.4.2 Stereotype Facade

<<Facade>> defines a classifier as being a view of (facade of) one or more other classifiers. Facades usually define additional properties that match some external view of a conceptual model element.

A facade will represent the classifier for which it is a facade. A Facade will use one of two methods to relate the facade properties to the conceptual Model:

- \* <> using the facade.
- \* Applying the <> stereotype and Subclassing "Representation Computation"

#### *Base Classes*

- *Classifier*

### **12.4.3 Stereotype Map**

<> defines an equality rule between two properties in a <> - they must represent the same information, perhaps using different representations.

Maps should be drawn <from> the representation <to> the more conceptual.

<> may be used between models, as is common for a <> or within one model to equate different representations for the same thing (e.g., property paths).

#### *Base Classes*

- *Connector*

#### *Tag Definitions*

##### ○ **coerce : Boolean**

Where <coerce> has a value of TRUE a map rule will be evaluated even if the <from> is not type compatible with the <to> type.

Where <coerce> is FALSE or unstated a map rule will be evaluated only if the <from> is type compatible with the <to> type.

Type compatible shall be defined as one of: Being the same type, <from> being a subtype of <to> (as defined by a type generalization rule), <from> being a representation of <to> (as defined by a representation rule).

Representation rules applied to a supertype apply to a subtype.

##### ○ **condition : ValueSpecification**

<condition> is an expression that must be true for the map rule to hold.

##### ○ **default : Boolean**

<default> is true if the map should be enforced only if no other maps apply.

##### ○ **type : Classifier**

<type> is a restriction on the type of a property or relation that a map represents. One "side" of the map connector must have this type.

#### 12.4.4 Stereotype Mapping Rule

<<Mapping Rule>> defines a pattern structure described by a structured classifier that shows how both "sides" of a representation (conceptual and logical) are related. Each "side" must match, including any traversals through structures defined with properties and connectors. Such traversals are links which may also have filters to more precisely define the pattern.

The pattern is described using structured classifier properties and connectors.

The mapping engine ensures that the patterns match, bidirectionally.

##### *Base Classes*

- *StructuredClassifier*

##### *Direct Supertypes*

- *Rule*

#### 12.4.5 Stereotype Match

Match specifies an element in a structure that must match a model element for the pattern to match. The match is the starting point for the pattern from which all paths are computed.

<<Match>> is a shortcut for <<Pattern Element>> strength=Match

##### *Base Classes*

- *Connector*
- *ConnectorEnd*
- *Property*

##### *Direct Supertypes*

- *Pattern Element*

#### 12.4.6 Stereotype Pattern Element

<<Pattern element>> further defines a connector, connector end or property within a pattern based on the tag values.

Note that the UML default value may be used to set the initial value of a pattern element.

##### *Base Classes*

- *Connector*
- *ConnectorEnd*
- *Property*

##### *Tag Definitions*

- ◊ **computation : ValueSpecification**

<computation> computes a value for the pattern element based on the expression.

Where computation is used inverse mapping is not specified - any inverse mapping is implementation specific.

- **condition : ValueSpecification**

<condition> states a condition that must be true within the scope of the pattern element. This can be used for pattern matching, setting values or restriction of paths.

- **explicit : Boolean [0..1]**

If <explicit> is true, the pattern element must be explicitly asserted as the indicated type, not derived or inferred from a supertype or super property.

- **quantifier : Quantifier**

A property that defines a quantification within a pattern. The quantifier defines the set of things that will populate the pattern property for all instances of the pattern.

Quantifiers operate over the type of a pattern element and define a set or subset that corresponds to the extend of the pattern elements type.

e.g. for all people p: People is the context and P is the quantified property. In SIMF the quantified property would typically be named <quantifier> <type>. So the above quantified property would be named "all people". The quantified property will be asserted to have the quantified type.

- **strength : Pattern Element Strength**

<strength> defines the behavior of an element with respect to a pattern - how it impacts the selection, evaluation or assertion of the pattern.

- **type : Classifier**

<type> is a restriction on the type of a property or relation that a pattern element represents.

#### **12.4.7 Enumeration Pattern Element Strength**

Pattern Element Strength defines a set of options for the mapping behavior of a pattern element.

*Literals:*

○ **Assert**

*The element will be asserted as required for a valid pattern. Assert is the default.*

○ **Default**

*The element will be asserted only if no other values are asserted within the pattern or as pre-existing assertions.*

○ **Exists**

*Existing element that will be used to compute other values but does not otherwise impact the pattern.*

○ **Match**

*Match is used in query and mapping patterns, all elements of the classified type that match the pattern are selected as instances of the pattern.*

*Match may be considered a qualified "All". Match does not assert the existence of something, it determines the existence of a pattern match such that other assertions may be made.*

*Relationships between properties with <quantifier>=Match must hold between the matched properties for the pattern to match.*

#### 12.4.8 Enumeration Quantifier

The set of quantifiers for pattern variables. Quantifiers operate over the type of a pattern element and define a set or subset that corresponds to the extend of the pattern elements type.

*Literals:*

○ **All**

*The universal quantifier - the quantified property is a stand-in for all elements of the extent of the quantified type*

○ **Exactly One**

*The existential quantifier limited to exactly one of a potentially larger set*

○ **Most**

*A stratified existential quantifier with a default for a "typical" value - example: <Most> people have 2 arms.*

*For logics that do not support "most", most may be interpreted as "There Exists".*

○ **None**

*A quantifier where no instance of the type may fill the role. E.g. "there may not exist".*

○ **Some**

*A stratified existential quantifier for a common values - example: <Some> people like computers.*

*For logics that do not support "some", some may be interpreted as "There Exists".*

○ **There Exists**

*The existential quantifier - at least one element must exist.*

#### 12.4.9 Stereotype Represents

<<Represents>> is an assertion that the source type or feature provides a more concrete way to represent the target type or feature. Represents may be used within conceptual models or from a physical model to a conceptual model.

- A representation that is a dependency or realization makes no assumption that the types are substitutable.
- A representation that is a generalization is substitutable for what it represents.

#### *Base Classes*

- *Dependency*
- *Generalization*

#### *Tag Definitions*

◊ **condition : ValueSpecification**

<condition> is an expression that must be true for the source to represent the target.

◊ **map-all : Boolean**

<map-all> implies a direct mapping between instances of the types in both directions.

<map all> is equivalent to a mapping with a rule mapping properties of each type but is lower precedence than other mappings - if types have a more specific map it will apply first.

### **12.4.10 Stereotype Rule**

<<Rule>> defines a pattern that must hold true for the context of the rule.

The pattern is described using structured classifier properties and connectors.

A rule is a pattern structure described by a structured classifier that shows how elements are related. Each mapped element must match, including any traversals through structures defined with properties and connectors. Such traversals are links which may also have filters to more precisely define the pattern. The mapping engine ensures that the patterns match, bidirectionally.

#### *Base Classes*

- *StructuredClassifier*

#### *Tag Definitions*

◊ **holds within : Namespace**

<holds within> is the context in which a rule is asserted (required to be true). Anything contextualized by the context is subject to the proposition.

If not stated the rule is asserted by its owner.

### **12.4.11 Stereotype Rule Model**

A <<Rule Model>> defines a package as containing rule specifications and asserts those rules to be true.

#### *Base Classes*

- *Package*

#### *Direct Supertypes*

- *Model*

### 12.4.12 Stereotype Subset of

In a pattern or mapping rule, <Subset of> defines a pattern property that represents a subset of another property. The subset may be constrained by a more specific type, expressions, values or required cardinalities.

Subset stereotypes the end of a connector that is the superset.

#### *Base Classes*

- *ConnectorEnd*

#### *Tag Definitions*

- ◊ **default : Boolean [0..1]**

True if the subset should be populated only if no other subsets have been populated.

### 12.4.13 Stereotype Subsumes

<<Subsumes>> is a dependency between rules. When a rule subsumes another the subsumed rule will not apply (fire). if the <subsumed by> rules applies (fires).

Where rules are also patterns, a rule may specialize another which will subsume the specialized rule as well as include the generalized rule parts as parts of the specialized rule.

#### *Base Classes*

- *Dependency*

## 12.5 SIMF Profile::SIMF Computation Rules

Computation rules define mappings that are implemented via external methods. As such the implementation is defined by implementations, not the specification.

## 12.5.1 Diagram SIMF Computation Rules

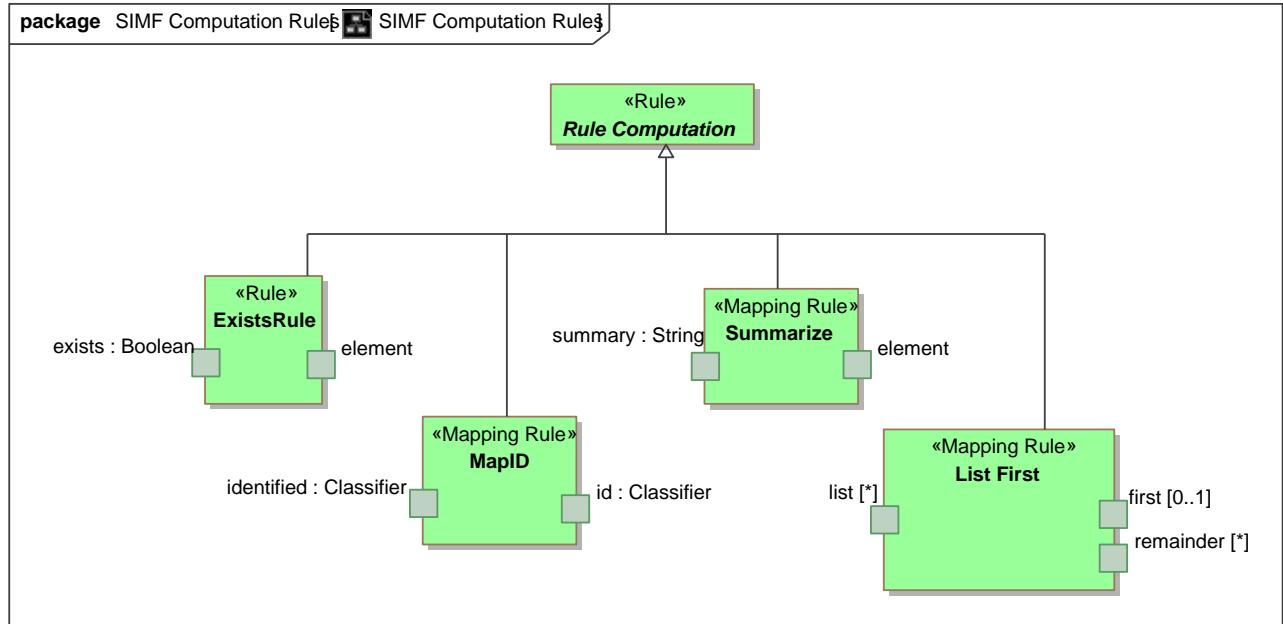


Figure 74 SIMF Computation Rules

## 12.5.2 Class ExistsRule

<<Exists Rule>> is a rule to map the existence of an <element> to a boolean.

<exists> is true iff <element> is not null.

### *Direct Supertypes*

- **Rule Computation**

### *Attributes*

exists : Boolean

exists : Boolean

## 12.5.3 Class List First

The <List First> rules will take the <list> property and place the first element into<first>. If <list> is empty, <first> will be empty.

If there are more <list> elements than 1, all remaining elements are placed as a set in <remainder>.

If <list> is an un-ordered set the order will be indeterminate but repeatable.

<<List First>> is bidirectional and will compute <list> by appending <first> and <remainder>.

Note that this will act like a LISP CDR/CAR pair

### *Direct Supertypes*

- *Rule Computation*

#### *Attributes*

☐ first [0..1]

☐ list [\*]

☐ remainder [\*]

### 12.5.4 Class MapID

<<MapID>> is a rule where the source is an ID and the target is a class, maps **an instance of the ID** to an instance of the class.

#### *Direct Supertypes*

- *Rule Computation*

#### *Attributes*

☐ id : [Classifier](#)

☐ identified : [Classifier](#)

### 12.5.5 Class Rule Computation

<<Rule Computation>> is an abstract supertype for a facade that includes external implementation. The implementation is outside of this specification.

### 12.5.6 Class Summarize

<<Summarize>> is a rule that produces a natural language description of an element. Summarize may not be bi-directional and is expected to have information loss.

<summary> is a summary of <element>.

Content of summary is implementation specific.

#### *Direct Supertypes*

- *Rule Computation*

#### *Attributes*

☐ element

☐ summary : [String](#)

# 13 Concept Index

- Abbreviated Name, 65
- Ability, 125
- Absorbed Dose (Radiation), 89
- Abuse Resource, 254
- Acceleration, 90
- Accept Risk, 275
- Access Complexity, 225
- Access Control Failure, 238
- Access Identifier, 204
- Access Point, 217
- Access Vector, 226
  - achieved by, 118
  - achieves, 190, 191
  - achieves end state, 161
- Acre, 99
- Action On Entity, 81
- Activity, 82
- Activity Map Rule, 320
- Actor, 54
- Actor Association, 129
  - acts on information, 71
- Actual Entity, 56
- Actual Occurrence, 120
- Actual Situation, 121
- Actual State, 121
- ActualObservableFacade, 297
- Address Map Rule, 325
  - address of, 142
- Adjacent, 226
  - affected by, 61
- AffectedAssetFacade, 298
  - affects, 82
- affords, 157
- All, 79
- All Actions, 254
- allowed by, 286
- allows, 294
- Alter Ability, 125
  - alters, 125
- altitude, 182
- Amount of Substance, 90
- Ampere, 99
- AND Condition, 137
- Angle, 90
- Animal, 168
- Anything, 56
- Area, 90
  - area code, 146
- Area Map Rule, 342
  - asserted by, 152, 211
- Asserting Policy, 151
  - asserts, 151, 152
  - assessed by, 133
- Assessed Entity, 133
  - assesses, 134
- Assessment Activity, 134
- Assessment Map Rule, 323
  - assessment of, 134
- Assessment Report, 134
  - assessment score, 134
- associate, 62, 129
  - associated with, 62, 129
- assumes risk from, 193
- Attack, 284
  - attack target, 285
- attests to, 163

Authentication, 226  
Authority, 152  
Automated Control, 152  
Automated Entity, 152  
automates, 152, 153  
Automaton, 172  
availability, 140  
Availability Impact, 227  
Avoid Danger, 271  
Becquerel (Bq), 100  
Benefit, 187  
Benefit Metric, 86  
Biological Danger, 239  
birth date, 169  
Blacklist Indicator, 263  
bound values, 78  
Boundary, 218  
bounded by, 178  
Bounded Topology, 178  
bounds, 218  
bounds region, 181  
call sign, 144  
Campaign, 234  
Candela, 100  
Capability, 135  
Capture Resource, 254  
Catastrophic, 280  
Categorization, 58  
categorized by, 57, 58, 78  
categorizes, 58, 77  
Category, 58  
Causality Rule, 113  
Cause and Effect, 116  
Cause of Incident, 258  
caused by, 117, 118, 259  
causes, 117, 118  
causes harm, 287  
CBRN Danger, 239  
Celsius, 100  
changes control of, 154  
channel, 144  
Chemical Danger, 239  
city ID, 143  
Civil Unrest Danger, 239  
Close Information, 254  
Collateral Damage Potential, 228  
collection of, 276  
Color, 91  
communicates via, 173  
Communicating Device, 173  
Communications Network, 173  
Communications Security Level, 140  
Communications Vulnerability, 291  
Complete, 228, 229, 230  
Compliance Impact, 239  
component of, 218, 219  
Composite Condition, 137  
Computer Control System, 153  
Computer System, 174  
Concentration, 91  
Concentration (amount of substance), 91  
Concentration (Mass), 91  
Concentration (Volume), 91  
Concentration Percent, 100  
condition, 77, 115  
condition for, 294  
conditional causes, 114, 118  
conditionally caused by, 114, 118  
Confidence, 71  
confidence metric, 71  
Confidence Metric, 86  
Confidentiality Impact, 228  
Confirmed, 231  
constrains, 115, 211

Constraint, 114  
Contact Availability, 147  
contact for, 140, 141  
Contact Information, 140  
Contact Information Mapping Rule, 326  
Contact Means, 140  
Contact Purpose, 147  
contact via, 140, 141  
Contactable, 141  
contains information, 174  
contains object, 75  
Context, 58  
Context Type, 59  
Contextualization, 59  
contextualizes, 59  
contributes to, 250  
contributor, 287  
Control, 153  
Control Action, 154  
Control Failure, 240  
Controlled Entity, 154  
Controlling Actor, 154  
Conveyance, 174  
Coordinate, 179  
Coordinate Map Rule, 342  
coordinate system, 179  
Coordinate System, 179  
Coulomb/kilogram (C/kg)., 100  
Count, 86, 92  
Countermeasure, 271  
countermeasure for, 272  
Country, 129  
country code, 146  
country ID, 143  
Country ID, 129  
county ID, 143  
Course of Action, 160  
Course Of Action Rule, 161  
Create Entity, 155  
Create Information, 254  
creates, 155  
creates process instance, 82  
Credential, 163  
Criminal Danger, 240  
Critical, 280  
Cubic Feet, 101  
Cubic Inch, 101  
Cubic Meter, 101  
Cup (US), 101  
Curie (Ci), 101  
Currency, 92  
Currency Benefit Metric, 86  
current height, 169  
Current Situation, 121  
current weight, 169  
Custodian, 155  
Custody, 155  
CVE Identifier, 291  
CVSS Score, 225  
Cyber Danger, 240  
Cyber System Failure, 240  
Cyber Vulnerability, 292  
Cyber Weapon, 165  
Damage, 254  
Damage Resource, 255  
Danger Category, 240  
Danger Impact, 285  
Danger Source, 249  
day, 147  
Day, 101  
death date, 169  
Decision-making Impact, 240  
defined by, 57  
defines, 72

defines identifier, 67  
degree of affect, 190  
degree of modification, 273  
degree of satisfaction, 211  
Degrees, 102  
Delete Information, 255  
DeliveryPoint, 315  
depends on, 215  
described by, 57, 287  
describes, 72  
designates location, 180  
desirability, 190  
desirability for, 193  
Desirability Metric, 188  
desirability of, 193  
Destroy Entity, 156  
destroys, 156  
Device, 174  
device address, 176  
Diminish Ability, 126  
direction, 182  
Disinformation Impact, 241  
Disrupt Objective, 250  
Disrupt Process, 255  
Disruptive Action, 250  
disrupts, 250  
distance, 182  
document capable, 141  
Dose Equivalent (Radiation), 92  
Electric Current, 92  
Electric Potential, 93  
Electromagnetic Spectrum Impact, 241  
electronic address, 142, 146  
Electronic Contact, 141  
elevation, 183  
Email Address, 142  
emergency, 147  
enabled by, 55  
enables, 125  
enacted by, 83, 121  
enacts, 82  
ends on, 118  
Energy, 93  
Enhance Ability, 126  
Enterprise, 166  
enters into, 218  
enters through, 218, 255  
Entity, 60  
Entiy Map Rule, 330  
Entry Action, 255  
Environmental Impact, 241  
evening, 147  
Exactly One, 78  
Exceed Capacity, 256  
exchange, 146  
executed by, 74  
executes, 174  
Exit Action, 256  
exit through, 256  
Exploitability, 229  
exploits, 216  
ExploitTargetFacade, 298  
Expression, 114  
Expression Language, 114  
expression text, 115  
extension, 146  
Facilitator, 126  
Facility, 208  
Facility Map Rule, 343  
Fahrenheit, 102  
Failure, 259  
Failure Category, 241  
fax capable, 141  
Female, 171

Financial Identifier, 205  
Financial Impact, 241  
Fire Danger, 242  
Fluid Ounce (US), 102  
Foot, 102  
Force, 93  
Frequency, 93  
Frequent, 279  
from location, 182  
Functional, 230  
Gallon (Imperial), 102  
Gallon (US), 103  
Generalization, 62  
generalizes, 58, 62  
Geophysical Danger, 242  
Geopolitical Entity, 129  
Geopolitical ID, 130  
Geopolitical Region, 179  
given name, 207  
governs region, 130, 132  
Gram, 103  
Gray (Gy), 103  
happens after, 118, 119  
happens before, 118, 119  
happens during, 118  
Harm, 188  
harm from, 189  
harmed by, 215, 285  
harms, 285, 287  
harms victim, 287  
has ability to, 56, 136  
has ability to influence, 125  
has address, 181  
has assessment, 133  
has authority over, 152, 159  
has boundary, 219  
has capable performer, 83, 136  
has child organization, 199  
has communications address, 173  
has component, 218, 219  
has condition, 259  
has confidence, 61  
has control over, 153, 154  
has control system, 152, 153  
has coordinate, 181  
has credential, 125  
has custodial action, 157  
has custody of, 155  
has failed resource, 259  
has failure, 215  
has impact, 118  
has indicator, 61  
has leader, 156, 199  
has location designation, 181  
has member, 199  
has metadata, 61  
has name, 61  
has nodes, 173  
has objective, 193, 250  
has objective to, 251  
has observation, 61  
has opening, 218  
has parent organization, 199  
has part, 61  
has permission to perform, 56, 202  
has portal, 219  
has property, 77  
has resident, 209  
has risk, 215, 277, 278  
has rule, 59  
has scope, 264  
has sighting, 121, 264  
has source, 190  
has state, 61

has temporal part, 118  
has topology, 181  
has value, 78  
has value binding, 119  
has vulnerability, 215  
Health Impact, 242  
height, 175  
Hertz, 103  
High, 88, 225, 228, 230, 232, 233  
Horsepower, 104  
hosts, 209  
Hour, 104  
Identification, 66  
Identification Map Rule, 333  
identified by, 61, 66  
Identifier, 66  
identifies, 66  
Identity Provider, 163  
Identity Theft, 242  
Image Impact, 242  
Impact, 189  
Impact Category, 243  
impact measure, 190  
impacted by, 61  
impacts, 61  
importance, 192  
imposed by, 273  
imposes, 277  
Improbable, 280  
in context of, 57, 59  
in network, 141  
in object, 72  
in the custody of, 156  
Inability to Communicate Impact, 243  
Inch, 104  
Incident, 259  
Incident Map Rule, 334  
incorporated by, 130, 131  
Incorporated Organization, 130  
incorporates, 130, 131  
Incorporation, 130  
indicated by, 122, 263  
indicates, 263, 264  
Indication, 263  
Indicator, 264  
Indicator Pattern, 264  
Indicator Watchlist, 265  
Indirect Threat, 285  
Industrial Control Failure, 243  
influenced by, 125  
Information Action, 71  
Information Impact, 243  
Information Loss Impact, 243  
Information Object, 72  
Information Source, 72  
Information Store, 72  
Information System Vulnerability, 292  
Information Transfer, 73  
Information Vulnerability, 292  
Infrastructure Impact, 244  
initiates, 118, 161  
Injury Map Rule, 337  
Integrity Impact, 230  
Intellectual Property Impact, 244  
Internet Contact, 142  
Internet Contact Map Rule, 327  
Interrupt Process, 256  
invalid on, 163  
Invoke Process, 82  
involved in, 55, 62  
Involvement, 62  
involves, 62, 119  
is boundary part, 77  
is composite part, 77

is controlled by, 153, 154  
is evidence for, 266  
is governed by, 132, 179  
is in, 72  
is in risk Group, 277  
is objective of, 250  
is part of, 60  
is possessed by, 154, 159  
issued by, 163  
issues credential, 163  
Item, 175  
Item Map Rule, 339  
Joule, 104  
Kelvin, 104  
Kg per cubic meter, 105  
Kill Chain, 268  
Kill Chain Step, 268  
Kilogram, 105  
Kilogram per cubic meter, 105  
Kilometer, 105  
Kilometer per Hour, 105  
Kilowatt hour, 106  
latitude, 183  
Leader, 156  
Leadership, 156  
leads, 156  
leads to, 259, 282  
Legal Impact, 244  
length, 175  
Length, 93  
leveraged by, 294  
leverages countermeasure, 277  
License Identifier, 131  
likelihood, 84, 122, 264, 285  
Likelihood Categories, 279  
line, 146  
Liquid Volume, 106  
Local, 226  
Local Identifier, 131  
located person, 181, 206  
Location ID, 180  
Location Identifier, 180  
Location Map Rule, 344  
location of, 209  
location of person, 205, 206  
longitude, 183  
looses control, 157  
Lose Control, 157  
loses via, 181  
loss action, 155  
Loss of Control Danger, 244  
lost by, 153  
lost via, 153  
Low, 88, 226, 228, 232, 233  
Low-Medium, 228  
Luminosity, 94  
Luminous Intensity, 94  
made available by, 61  
magnitude, 87  
makes prediction, 213  
Male, 171  
Managed Actor Identifier, 131  
Managed Entity, 157  
Managed Identifier, 163  
Managed Item Identifier, 175  
Managed Person Identifier, 205  
manufactured by, 184  
Manufactured Thing, 184  
Manufacturer, 185  
manufactures, 185  
Map, 180  
Map Coordinate, 180  
Marginal, 280  
mass, 175

Mass, 94  
Mass Density, 95  
Match, 79  
matches, 118, 266  
may be performed by, 83, 202  
may perform information action, 74  
Means, 190  
Means to End, 190  
Measurement, 195  
measures risk of, 276  
measures risk to, 276  
Medium, 88, 225, 232  
Medium High, 228  
Medium, 233  
member of, 199  
Membership, 198  
Metadata, 73  
metadata about, 73  
metatype, 59  
Meteorological Danger, 244  
Meter, 106  
Meter per second squared, 106  
Metric, 86  
middle name, 207  
Mile, 106  
Miles per Hour, 107  
Millimeter, 107  
Millisecond, 107  
Minute, 107  
Mission Impact, 245  
Mission Objective, 199  
mitigated by, 273  
mitigates, 272  
Mitigation Actor, 272  
mobile, 141  
model property, 78  
modelElementID, 57  
Moderate, 88  
modified by, 276  
modifies risk, 273  
Modify Information, 256  
Modify Resource, 256  
Modus Operandi, 82  
Mole, 107  
Mole Per Cubic Meter, 108  
monitored by, 264  
Monitoring Safeguard, 272  
Most, 79  
moved via, 181  
Multiple, 227  
Name, 66  
Name Identifier, 67  
name part, 206  
name suffix, 207  
names, 66  
Namespace, 67  
Natural Language Text, 73  
Natural Threat, 285  
negate, 138  
negation, 264  
Negligable, 280  
net benefit, 188  
net desirability, 188  
net likelihood, 188  
net risk, 188  
net severity, 188  
network address, 174  
Network Identifier, 67  
Newton, 108  
night, 147  
Non Happening, 121  
None, 78, 227, 228, 229, 230, 233  
Non-Technical Impact, 245  
Nuclear Danger, 245

number observed, 196  
Object Management Group, Inc. (OMG), 23  
Objective, 191  
objective of, 192  
Observability, 195  
ObservablePatternFacade, 298  
Observation, 196  
Observation Tool, 196  
observed by, 121  
observed in, 196  
observed using, 196  
observer, 196  
Observer, 196  
observes, 196  
Obtain Control, 157  
obtained by, 153  
obtained via, 153  
obtains control, 158  
Occasional, 280  
Occurrence, 117  
occurs on, 118  
Offical Fix, 231  
official given name, 207  
OMG specifications, 23  
on map, 180  
Open Information, 257  
operates at, 55  
Opportunity, 192  
OR Condition, 138  
Organization, 199  
Organization Map Rule, 346  
OSVDB Identifier, 292  
other, 147  
Ounce-Mass (US), 108  
owned by, 158, 159  
Owner, 158  
Ownership, 158  
owns, 158  
Package, 74  
Partial, 227, 229, 230  
Pascal, 108  
Passport Identifier, 205  
Past Situation, 122  
Pattern, 77  
Pattern Property, 77  
PentaScale, 88  
performed by, 117  
Performer, 214  
performs, 55  
performs information action, 174  
performs mitigation, 272  
performs observation, 197  
Permission, 202  
perpetrates, 250  
perpetrator, 285  
Person, 205  
Person at location, 206  
Person Map Rule, 348  
Person Name, 206  
Person Name Map Rule, 349  
Person Structured Name, 206  
Person Textual Name, 207  
personal, 147  
PersonInjuryFacade, 316  
Physical Characteristic, 95  
Physical Entity, 169  
Physical Location, 181  
Physical Quantity Kind, 95  
physical sex, 169  
Physical System Failure, 245  
Physical Tool, 176  
Physical Vulnerability, 293  
Physical Weapon, 176  
physically contains, 170

physically within, 170  
Pint (US), 108  
Place, 208  
place ID, 143  
Plan, 83  
Point On Earth, 181  
Policy, 210  
possesses, 155, 159  
Possession, 158  
post box ID, 143  
post code, 143  
postal address, 144  
Postal Address, 142  
Postal Address Facade, 314  
Postal Address Structured, 142  
Postal Address Text, 143  
Postal Code, 144  
PostCodeBase, 315  
PostCodeSuffix, 315  
postulated by, 212  
Potential Situation, 122  
Pound-Force, 109  
Pound-Mass (Imperial), 109  
Pound-Mass (US lb), 109  
Power, 95  
predicted by, 122  
Prediction, 212  
Predictor, 213  
predicts, 212  
preferred identifier, 61  
Pressure, 95  
previously known, 293  
primary, 147  
Private Network Contact, 144  
Probability Metric, 87  
Probable, 280  
Process, 83  
Process Action, 83  
Process Failure, 245  
Program, 199  
Proof of concept, 229  
Property, 159  
Property Chains, 430  
property of, 78  
Protect Assets Objective, 275  
protected by, 215  
protects, 272  
provided to, 158  
provides access to, 125  
provides security level, 173  
provisioned by, 155  
PSI, 109  
publicly known, 293  
purpose, 140  
quantifier, 77  
Quantifier, 78  
Quantity Kind, 87  
Quart (US), 109  
Radians, 110  
Radiation Absorbed Dose (rad), 110  
Radiation Exposure, 96  
Radio Contact, 144  
Radio Map Rule, 328  
Radioactivity, 96  
Radiological Danger, 245  
rank, 278  
Read Information, 257  
realized by, 191, 192  
reciever, 220  
recipient name, 143  
recvied via, 56  
reduce harm via, 287  
Reference, 74  
reference URI, 74

referenced by credential, 164  
references identifier, 163  
region ID, 143  
Regional Authority, 131  
relates, 57  
Relative Coordinate, 182  
relative to, 182  
relocated by, 170  
relocates, 182  
Relocation, 182  
Remediation Level, 230  
Remote, 226, 280  
replacement cost, 278  
Report, 74  
Report Confidence, 231  
required to perform, 215  
requires, 83  
Residence, 209  
resides at, 205  
Resource, 215  
Resource Actions, 257  
Responsible Performer, 62  
restricted to, 115  
results in, 84  
Revision, 184  
revokes permission, 202  
Risk, 276  
risk for, 276, 278  
Risk Group, 276  
risk level accepted, 275  
Risk Mitigation Strategy, 276  
Risk Owner, 277  
Risk Topic, 277  
Risk Treatment Strategy, 272  
Roentgen (R), 110  
Roentgen Equivalent Man (REM), 110  
Role, 63  
Rule, 115  
Safeguard Activity, 273  
Safety Danger, 246  
Safety Impact, 246  
salutation, 206  
Scenario, 84  
score, 293  
Second, 111  
secondary, 147  
Security and Safety Objective, 277  
Security Danger, 246  
security level, 140  
Security Requirements, 232  
sender, 220  
sensitive to objective, 279  
sensitivity threshhold, 279  
sent via, 56  
severity, 286  
Severity Categories, 280  
Sex Kind, 170  
Sievert (Sv),, 111  
Sighting, 265  
Simple Identifier, 67  
Single, 227  
situated at, 119  
Situation, 117  
Social Network Contact, 144  
Social Security Number, 207  
Software, 74  
Software Vulnerability, 293  
Some, 79  
Source of Danger Category, 246  
sourced from, 61  
specializes, 58, 62  
Speed, 96  
Square Feet, 111  
Square Meter, 111

Stakeholder, 193  
Stakeholder Desirability, 193  
Stakeholder Risk, 278  
starts on, 118  
State, 119  
State Identifier, 132  
state of, 119  
state\_province ID, 143  
stated by, 75  
Statement, 75  
statement date and time, 75  
states, 72  
step, 117  
step in, 117  
STIX Campaign Rule, 299  
STIX Categories Rule, 300  
STIX Course Of Action Rule, 301  
STIX Incident Rule, 302  
STIX Indicator Rule, 303  
STIX Objective Rule, 304  
STIX Observable Rule, 305  
STIX Sighting Rule, 306  
STIX Statement Rule, 307  
STIX Threat Actor Rule, 308  
STIX TTP Rule, 309  
STIX Vocabulary Rule, 310  
STIX Vulnerability Rule, 311  
Stop Process, 257  
street ID, 143  
Structured Information Object, 75  
Subject of Rule, 211  
subject to, 61, 154, 159, 211  
Subject to Authority, 159  
Subsystem, 218, 219  
Summary Description, 75  
supported by, 279  
supports, 215  
surname, 207  
surname prefix, 207  
System, 219  
System Failure, 246  
taken from, 157  
Target Distribution, 232  
Tax Identification, 132  
Technical Identifier, 68  
Telecommunication Device, 176  
Telephone Area Code, 145  
Telephone Country Code, 145  
Telephone Map Rule, 329  
telephone number, 146  
Telephone Number, 145  
Telephone Number Facade, 315  
Telephone Number Structured, 145  
Telephone Number Text, 146  
Temperature, 96  
Temporary Fix, 231  
Terrorism Danger, 247  
text, 73  
Text Expression, 115  
Text Identifier, 68  
text message capable, 141  
There Exists, 78  
Threat, 281  
Threat Actor, 250  
Threat Likelihood, 278  
Threat Objective, 251  
Threat Report, 298  
Time, 96  
Time Order, 119  
Time Point, 87  
title, 206  
to location, 182  
Tool, 215  
Topological Point, 182

Topology, 183  
topology of, 183  
transaction id, 75  
Transfer, 220  
Transfer Control, 159  
transfer harm to, 273  
Transfer Risk, 273  
transferred by, 61  
transfers, 220  
Transport Impact, 247  
traversed using, 218  
trigger, 161  
TriScale, 88  
types, 58  
typographical conventions, 24  
Unavailable, 231  
Unconfirmed, 231  
Uncorroborated, 231  
Undesirable Event, 285  
Undesirable Situation, 286  
Undesirable State, 287  
Unintentional Threat, 287  
Unique Identifier, 68  
unique within, 66  
unit ID, 143  
Unproven, 229  
Unwitting Participant, 287  
URIIIdentifier, 69  
used by, 60, 196  
uses, 117  
valid on, 163  
value, 65, 67, 68, 69, 145, 292  
Value, 87  
Value Binding, 78  
value for, 78  
value within, 78  
Valued Asset, 278  
Valued Assets, 279  
values, 275, 279  
vector, 294  
version, 75  
Very High, 88  
Very Low, 88  
Victim, 288  
victim of, 288  
video capable, 142  
voice capable, 141  
Volt, 111  
Volume, 97  
Vulnerability, 293  
Vulnerability Identifier, 294  
Vulnerability Metric, 294  
vulnerability of, 294  
War Danger, 247  
watch based on, 272  
watched by, 61  
watches, 265  
Watt, 112  
Weapon, 216  
Website Contact, 146  
Whitelist Indicator, 267  
width, 175  
withdraws, 157  
Witness, 260  
witnessed by, 259  
witnesses, 260  
work, 147  
Workaround, 231  
World Geodetic System, 183  
XOR Condition, 138  
Yard, 112  
Year, 112