**Threat-Risk Concepts**

Contents

[1 Threat-risk-conceptual-model 5](#_Toc483071310)

[1.1 Diagram: Conceptual Threat/Risk Model Diagrams 5](#_Toc483071311)

[2 Threat-risk-conceptual-model::Threat and Risk Specific Concepts 6](#_Toc483071312)

[2.1 Diagram: Threat and Risk Specific Concepts 7](#_Toc483071313)

[3 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::.Summary Diagrams 8](#_Toc483071314)

[3.1 Diagram: Entity Kinds 8](#_Toc483071315)

[4 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Accusations 9](#_Toc483071316)

[4.1 Diagram: Accusations 9](#_Toc483071317)

[5 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Campaigns 10](#_Toc483071318)

[5.1 Diagram: Campaign 10](#_Toc483071319)

[5.2 Diagram: Campaign Objectives 11](#_Toc483071320)

[5.3 Class Campaign 11](#_Toc483071321)

[6 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger 12](#_Toc483071322)

[6.1 Diagram: Danger 13](#_Toc483071323)

[6.2 Class Attack <<Role>> 14](#_Toc483071324)

[6.3 Class Indirect Threat <<Role>> 14](#_Toc483071325)

[6.4 Class Natural Threat <<Role>> 14](#_Toc483071326)

[6.5 Class Threat <<Role>> 14](#_Toc483071327)

[6.6 Class Unintentional Threat <<Role>> 15](#_Toc483071328)

[7 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger Sources 16](#_Toc483071329)

[7.1 Diagram: Danger Sources 16](#_Toc483071330)

[7.2 Class Accident <<Role>> 16](#_Toc483071331)

[7.3 Association Class Contribution to Danger <<Relationship>> 17](#_Toc483071332)

[7.4 Class Danger Source <<Role>> 17](#_Toc483071333)

[7.5 Class Dangerous Condition <<Role>> 17](#_Toc483071334)

[7.6 Class Dangerous Event <<Role>> 17](#_Toc483071335)

[7.7 Association Class Exploit of Vulnerability <<Relationship>> 18](#_Toc483071336)

[7.8 Class Objective to Disrupt 18](#_Toc483071337)

[7.9 Class Unwitting Participant <<Role>> 18](#_Toc483071338)

[8 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger Sources::Source of Danger Categories 19](#_Toc483071339)

[8.1 Diagram: Source of Danger Categories 19](#_Toc483071340)

[8.2 Class Biological Danger <<Category>> 20](#_Toc483071341)

[8.3 Class CBRN Danger <<Category>> 20](#_Toc483071342)

[8.4 Class Chemical Danger <<Category>> 20](#_Toc483071343)

[8.5 Class Civil Unrest Danger <<Category>> 20](#_Toc483071344)

[8.6 Class Criminal Danger <<Category>> 20](#_Toc483071345)

[8.7 Class Cyber Danger <<Category>> 20](#_Toc483071346)

[8.8 Class Fire Danger <<Category>> 20](#_Toc483071347)

[8.9 Class Geophysical Danger <<Category>> 20](#_Toc483071348)

[8.10 Class Loss of Control Danger <<Category>> 21](#_Toc483071349)

[8.11 Class Meteorological Danger <<Category>> 21](#_Toc483071350)

[8.12 Class Nuclear Danger <<Category>> 21](#_Toc483071351)

[8.13 Class Radiological Danger <<Category>> 21](#_Toc483071352)

[8.14 Class Safety Danger <<Category>> 21](#_Toc483071353)

[8.15 Class Security Danger <<Category>> 21](#_Toc483071354)

[8.16 Class Source of Danger Category <<Category>> 21](#_Toc483071355)

[8.17 Class Terrorism Danger <<Category>> 22](#_Toc483071356)

[8.18 Class War Danger <<Category>> 22](#_Toc483071357)

[9 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents 23](#_Toc483071358)

[9.1 Diagram: Incident 23](#_Toc483071359)

[9.2 Association Class Danger Leads to Incident <<Relationship>> 23](#_Toc483071360)

[9.3 Class Incident <<Role>> 24](#_Toc483071361)

[9.4 Class Witness <<Role>> 24](#_Toc483071362)

[9.5 Association Class Witnessing <<Relationship>> 24](#_Toc483071363)

[10 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents::Failure 26](#_Toc483071364)

[10.1 Diagram: Failure 26](#_Toc483071365)

[10.2 Class Failure 26](#_Toc483071366)

[11 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents::Failure Categories 27](#_Toc483071367)

[11.1 Diagram: Failure Categories 27](#_Toc483071368)

[11.2 Class Access Control Failure <<Category>> 27](#_Toc483071369)

[11.3 Class Control Failure <<Category>> 27](#_Toc483071370)

[11.4 Class Cyber System Failure <<Category>> 28](#_Toc483071371)

[11.5 Class Failure Category <<Category>> 28](#_Toc483071372)

[11.6 Class Industrial Control Failure <<Category>> 28](#_Toc483071373)

[11.7 Class Physical System Failure <<Category>> 28](#_Toc483071374)

[11.8 Class Process Failure <<Category>> 28](#_Toc483071375)

[11.9 Class System Failure <<Category>> 28](#_Toc483071376)

[12 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents::Impact Categories 29](#_Toc483071377)

[12.1 Diagram: Impact Categories 29](#_Toc483071378)

[12.2 Class Communications Impact <<Category>> 29](#_Toc483071379)

[12.3 Class Compliance Impact <<Category>> 30](#_Toc483071380)

[12.4 Class Control of Information Impact <<Category>> 30](#_Toc483071381)

[12.5 Class Decision-making Impact <<Category>> 30](#_Toc483071382)

[12.6 Class Disinformation Impact <<Category>> 30](#_Toc483071383)

[12.7 Class Electromagnetic Spectrum Impact <<Category>> 30](#_Toc483071384)

[12.8 Class Environmental Impact <<Category>> 30](#_Toc483071385)

[12.9 Class Financial Impact <<Category>> 30](#_Toc483071386)

[12.10 Class Health Impact <<Category>> 31](#_Toc483071387)

[12.11 Class Identity Spoof Impact <<Category>> 31](#_Toc483071388)

[12.12 Class Image Impact <<Category>> 31](#_Toc483071389)

[12.13 Class Impact Category <<Category>> 31](#_Toc483071390)

[12.14 Class Information Availability Impact <<Category>> 31](#_Toc483071391)

[12.15 Class Information Impact <<Category>> 31](#_Toc483071392)

[12.16 Class Infrastructure Impact <<Category>> 31](#_Toc483071393)

[12.17 Class Intellectual Property Impact <<Category>> 31](#_Toc483071394)

[12.18 Class Legal Impact <<Category>> 32](#_Toc483071395)

[12.19 Class Mission Impact <<Category>> 32](#_Toc483071396)

[12.20 Class Non-Technical Impact <<Category>> 32](#_Toc483071397)

[12.21 Class Safety Impact <<Category>> 32](#_Toc483071398)

[12.22 Class Transport Impact <<Category>> 32](#_Toc483071399)

[13 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents::Incident Response 33](#_Toc483071400)

[13.1 Diagram: Incident Response 33](#_Toc483071401)

[13.2 Class Incident Containment <<Role>> 33](#_Toc483071402)

[13.3 Class Incident Recovery <<Role>> 34](#_Toc483071403)

[13.4 Class Incident Response <<Role>> 34](#_Toc483071404)

[14 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Indicators 35](#_Toc483071405)

[14.1 Diagram: Indicator 36](#_Toc483071406)

[14.2 Diagram: Observability 37](#_Toc483071407)

[14.3 Diagram: Sighting 37](#_Toc483071408)

[14.4 Class Blacklist Indicator 37](#_Toc483071409)

[14.5 Class Indicator 38](#_Toc483071410)

[14.6 Class Indicator Pattern 38](#_Toc483071411)

[14.7 Class Indicator Watchlist 38](#_Toc483071412)

[14.8 Class Whitelist Indicator 38](#_Toc483071413)

[15 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk 39](#_Toc483071414)

[15.1 Diagram: Risk 39](#_Toc483071415)

[15.2 Diagram: Risk Metrics 40](#_Toc483071416)

[15.3 Diagram: Risk Objectives 41](#_Toc483071417)

[15.4 Association Class Impose Strategy <<Relationship>> 41](#_Toc483071418)

[15.5 Class Objective forSafety and Security 42](#_Toc483071419)

[15.6 Class Objective to Protect Assets 42](#_Toc483071420)

[15.7 Class Risk 42](#_Toc483071421)

[15.8 Class Risk Mitigation Strategy 42](#_Toc483071422)

[15.9 Class Risk Owner <<Role>> 43](#_Toc483071423)

[15.10 Class Risk Reduction Objective 43](#_Toc483071424)

[15.11 Association Class Risk To Resource <<Relationship>> 43](#_Toc483071425)

[15.12 Association Class Risk Topic <<Relationship>> 44](#_Toc483071426)

[15.13 Association Class Stakeholder Risk <<Relationship>> 45](#_Toc483071427)

[15.14 Class Threat Likelihood <<Quantity Kind>> 45](#_Toc483071428)

[15.15 Association Class Valuation of Asset <<Relationship>> 46](#_Toc483071429)

[15.16 Class Valued Asset <<Role>> 46](#_Toc483071430)

[15.16.1 Enumeration Likelihood Categories 46](#_Toc483071431)

[15.16.2 Enumeration Severity Categories 47](#_Toc483071432)

[16 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Risk Treatments 48](#_Toc483071433)

[16.1 Diagram: Risk Treatment 48](#_Toc483071434)

[16.2 Diagram: Safeguard Monitoring 49](#_Toc483071435)

[16.3 Class Accept Risk 49](#_Toc483071436)

[16.4 Association Class Assume Risk <<Relationship>> 49](#_Toc483071437)

[16.5 Class Avoid Danger 50](#_Toc483071438)

[16.6 Class Countermeasure <<Role>> 50](#_Toc483071439)

[16.7 Association Class Countermeasure for Strategy <<Relationship>> 50](#_Toc483071440)

[16.8 Association Class Countermeasure Mitigates <<Relationship>> 51](#_Toc483071441)

[16.9 Class Defensive Step 52](#_Toc483071442)

[16.10 Class Management Control 52](#_Toc483071443)

[16.11 Class Mitigation Actor <<Role>> 52](#_Toc483071444)

[16.12 Association Class Monitor <<Relationship>> 52](#_Toc483071445)

[16.13 Class Monitoring Control 52](#_Toc483071446)

[16.14 Class Operational Control 53](#_Toc483071447)

[16.15 Class Risk Agent <<Role>> 53](#_Toc483071448)

[16.16 Association Class Risk Treatment <<Relationship>> 53](#_Toc483071449)

[16.17 Class Risk Treatment Strategy 53](#_Toc483071450)

[16.18 Association Class Safeguarding <<Relationship>> 54](#_Toc483071451)

[16.19 Class Technical Control 54](#_Toc483071452)

[16.20 Class Transfer Risk 54](#_Toc483071453)

[17 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Threat Actors 55](#_Toc483071454)

[17.1 Diagram: Threat Actors 55](#_Toc483071455)

[17.2 Class Disrupt Stakeholder's Objective 56](#_Toc483071456)

[17.3 Class Disruptive Action <<Role>> 56](#_Toc483071457)

[17.4 Class Disruptive Step 56](#_Toc483071458)

[17.5 Association Class Perpetrate <<Relationship>> 56](#_Toc483071459)

[17.6 Class Threat Actor <<Role>> 57](#_Toc483071460)

[18 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Undesirable Situations 58](#_Toc483071461)

[18.1 Diagram: Undesirable Situations 59](#_Toc483071462)

[18.2 Class Harm 59](#_Toc483071463)

[18.3 Association Class Harms Victim <<Relationship>> 60](#_Toc483071464)

[18.4 Association Class Source of Harm <<Relationship>> 61](#_Toc483071465)

[18.5 Class Undesirable Condition <<Role>> 62](#_Toc483071466)

[18.6 Class Undesirable Event <<Role>> 62](#_Toc483071467)

[18.7 Class Undesirable Situation <<Role>> 62](#_Toc483071468)

[18.8 Class Victim <<Role>> 62](#_Toc483071469)

[19 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities 63](#_Toc483071470)

[19.1 Diagram: Vulnerability 63](#_Toc483071471)

[19.2 Diagram: Vulnerability Identifiers 64](#_Toc483071472)

[19.3 Class Physical Vulnerability 64](#_Toc483071473)

[19.4 Association Class Supporting Condition <<Relationship>> 64](#_Toc483071474)

[19.5 Class Vulnerability 65](#_Toc483071475)

[19.6 Class Vulnerability Identifier <<Value>> 65](#_Toc483071476)

[19.7 Class Vulnerability Metric <<Quantity Kind>> 65](#_Toc483071477)

[20 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Cyber Vulnerabilities 66](#_Toc483071478)

[20.1 Diagram: Cyber Vulnerability 66](#_Toc483071479)

[20.2 Class Communications Vulnerability 67](#_Toc483071480)

[20.3 Class CVE Identifier <<Value>> 67](#_Toc483071481)

[20.4 Class Cyber Vulnerability 67](#_Toc483071482)

[20.5 Class Information System Vulnerability 67](#_Toc483071483)

[20.6 Class Information Vulnerability 67](#_Toc483071484)

[20.7 Class OSVDB Identifier <<Value>> 67](#_Toc483071485)

[20.8 Class Software Vulnerability 67](#_Toc483071486)

[21 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Vulnerabilities::Vulnerability Vectors 69](#_Toc483071487)

[21.1 Diagram: Vulnerability Vectors 70](#_Toc483071488)

[21.2 Class CVSS Score <<Quantity Kind>> 71](#_Toc483071489)

[21.2.1 Enumeration Access Complexity 71](#_Toc483071490)

[21.2.2 Enumeration Access Vector 72](#_Toc483071491)

[21.2.3 Enumeration Authentication 72](#_Toc483071492)

[21.2.4 Enumeration Availability Impact 73](#_Toc483071493)

[21.2.5 Enumeration Collateral Damage Potential 73](#_Toc483071494)

[21.2.6 Enumeration Confidentiality Impact 74](#_Toc483071495)

[21.2.7 Enumeration Exploitability 74](#_Toc483071496)

[21.2.8 Enumeration Integrity Impact 75](#_Toc483071497)

[21.2.9 Enumeration Remediation Level 76](#_Toc483071498)

[21.2.10 Enumeration Report Confidence 76](#_Toc483071499)

[21.2.11 Enumeration Security Requirements 77](#_Toc483071500)

[21.2.12 Enumeration Target Distribution 77](#_Toc483071501)

[22 Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Weapons 79](#_Toc483071502)

[22.1 Diagram: Weapons 79](#_Toc483071503)

[22.2 Class Cyber Weapon <<Role>> 79](#_Toc483071504)

[22.3 Class Physical Weapon <<Role>> 79](#_Toc483071505)

[22.4 Class Weapon <<Role>> 80](#_Toc483071506)

[22.5 Association Class Weapon Leverages Vulnerability <<Relationship>> 80](#_Toc483071507)

# Threat-risk-conceptual-model

## Diagram: Conceptual Threat/Risk Model Diagrams



1. Conceptual Threat/Risk Model Diagrams

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

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

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

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](#_6b1b5bc2c02e97388502f44875bda1e8)
* [Risk](#_06bcfc4aa4414d36cb05ca997c4a0821)
* [Incident](#_b1d260370301e9c37b320e4c2c053faf)
* [Indicator](#_52ac381b3375b694d0d6cabc1d7c8b2a)
* [Vulnerability](#_6cf32abc6725e61497ee7c4fedec966c)

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

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

## Diagram: Threat and Risk Specific Concepts



1. Threat and Risk Specific Concepts

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

## Diagram: Entity Kinds



1. Entity Kinds

# Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Accusations

## Diagram: Accusations



1. Accusations

# 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.

## Diagram: Campaign



1. Campaign

## Diagram: Campaign Objectives



1. Campaign Objectives

## Class Campaign

Campaigns are ongoing work in an organized and active way toward a particular goal, typically a political, military, or social one. A campaign will typically have parts that are the specific activities of the campaign.  
A Military campaign is a series of military operations intended to achieve a particular objective, confined to a particular area, or involving a specified type of fighting.  
A campaign is also an objective for the activities supporting the campaign.

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

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

## Diagram: Danger



1. Danger

## Class Attack <<Role>>

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

Direct Supertypes

[Disruptive Action](#_1b064056002f89a4ba6f4565e08b4f3a), [Threat](#_3808bf8833da2fdb6f89d9e4ffa81146)

## Class Indirect Threat <<Role>>

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

Direct Supertypes

[Threat](#_3808bf8833da2fdb6f89d9e4ffa81146)

## Class Natural Threat <<Role>>

A threat from natural means.

Direct Supertypes

[Threat](#_3808bf8833da2fdb6f89d9e4ffa81146)

## Class Threat <<Role>>

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



1. Threat Detail

Direct Supertypes

[Dangerous Event](#_f2fa5e8341680da5e6e7a3cee51ee0a0)

## Class Unintentional Threat <<Role>>

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

Direct Supertypes

[Threat](#_3808bf8833da2fdb6f89d9e4ffa81146)

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

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

## Diagram: Danger Sources



1. Danger Sources

## Class Accident <<Role>>

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

Direct Supertypes

[Dangerous Event](#_f2fa5e8341680da5e6e7a3cee51ee0a0)

## Association Class Contribution to Danger <<Relationship>>

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



1. Contribution to Danger

Association Ends

contributor : [Danger Source](#_e92228f26631bd725a174bd1e0d187f6) [0..\*]



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

contributes to : [Undesirable Situation](#_4bdee0568b2f36e553f586b458dace32) [1..\*]



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

Attributes

likelihood



## Class Danger Source <<Role>>

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

## Class Dangerous Condition <<Role>>

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

Direct Supertypes

[Danger Source](#_e92228f26631bd725a174bd1e0d187f6), [Undesirable Condition](#_1e65602d4dd275cfb1ddaa86376c7fed)

## Class Dangerous Event <<Role>>

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

Direct Supertypes

[Danger Source](#_e92228f26631bd725a174bd1e0d187f6), [Undesirable Event](#_83770257a20b9ec56f996c13de27165d)

## Association Class Exploit of Vulnerability <<Relationship>>

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



1. Exploits Vulnerability

Association Ends

exploits : [Vulnerability](#_d936caf19626476c163d1b8384647aa0) [1..\*]



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

exploited by : [Danger Source](#_e92228f26631bd725a174bd1e0d187f6) [0..\*]



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

## Class Objective to Disrupt

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

## Class Unwitting Participant <<Role>>

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

Direct Supertypes

[Danger Source](#_e92228f26631bd725a174bd1e0d187f6)

# Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Danger Sources::Source of Danger Categories

## Diagram: Source of Danger Categories



1. Source of Danger Categories

## Class Biological Danger <<Category>>

Any danger from a biological source.

Direct Supertypes

[CBRN Danger](#_1b7fbbac749a99850f7fe96ac4bb6b8d)

## Class CBRN Danger <<Category>>

A Chemical, biological, radiological or nuclear danger.

Direct Supertypes

[Source of Danger Category](#_160715442680bb12abbe3b740c5facab)

## Class Chemical Danger <<Category>>

A danger from a chemical.

Direct Supertypes

[CBRN Danger](#_1b7fbbac749a99850f7fe96ac4bb6b8d)

## Class Civil Unrest Danger <<Category>>

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

Direct Supertypes

[Security Danger](#_a629b5862f5d42a8bc1b8f79b0f2f646)

## Class Criminal Danger <<Category>>

Danger from a criminal activity.

Direct Supertypes

[Security Danger](#_a629b5862f5d42a8bc1b8f79b0f2f646)

## Class Cyber Danger <<Category>>

Danger related to computer systems and networks.

Direct Supertypes

[Security Danger](#_a629b5862f5d42a8bc1b8f79b0f2f646)

## Class Fire Danger <<Category>>

Danger from fire

Direct Supertypes

[Source of Danger Category](#_160715442680bb12abbe3b740c5facab)

## Class Geophysical Danger <<Category>>

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

Direct Supertypes

[Source of Danger Category](#_160715442680bb12abbe3b740c5facab)

## Class Loss of Control Danger <<Category>>

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

Direct Supertypes

[Source of Danger Category](#_160715442680bb12abbe3b740c5facab)

## Class Meteorological Danger <<Category>>

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

Direct Supertypes

[Geophysical Danger](#_0ee55a33161552117f79fca2d73e574e)

## Class Nuclear Danger <<Category>>

Category of danger from a nuclear blast.

Direct Supertypes

[CBRN Danger](#_1b7fbbac749a99850f7fe96ac4bb6b8d)

## Class Radiological Danger <<Category>>

A categorization of danger from radiation.

Direct Supertypes

[CBRN Danger](#_1b7fbbac749a99850f7fe96ac4bb6b8d)

## Class Safety Danger <<Category>>

General emergency and public safety danger category. [CAP]

Direct Supertypes

[Source of Danger Category](#_160715442680bb12abbe3b740c5facab)

## Class Security Danger <<Category>>

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

Direct Supertypes

[Source of Danger Category](#_160715442680bb12abbe3b740c5facab)

## Class Source of Danger Category <<Category>>

A categorization of the source of dangers.

Direct Supertypes

[Danger Source](#_e92228f26631bd725a174bd1e0d187f6)

## Class Terrorism Danger <<Category>>

Category of danger from terrorism.

Direct Supertypes

[Security Danger](#_a629b5862f5d42a8bc1b8f79b0f2f646)

## Class War Danger <<Category>>

A Category of danger from acts of war.

Direct Supertypes

[Security Danger](#_a629b5862f5d42a8bc1b8f79b0f2f646)

# Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents

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

## Diagram: Incident



1. Incident

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

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



1. Cause of Incident

Direct Supertypes

[Contribution to Danger](#_b0b77eaf00ae3779a25865ff1f826f9d), [Dangerous Event](#_f2fa5e8341680da5e6e7a3cee51ee0a0)

Association Ends

leads to : [Incident](#_72703355926e6f9d23631bfd436b3d75) [0..\*]



Incident that is the result of a threat.

caused by : [Dangerous Event](#_f2fa5e8341680da5e6e7a3cee51ee0a0) [0..\*]



Cause of an incident.

## Class Incident <<Role>>

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

Direct Supertypes

[Dangerous Event](#_f2fa5e8341680da5e6e7a3cee51ee0a0)

## Class Witness <<Role>>

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

## Association Class Witnessing <<Relationship>>

Witnessing is the observation of an incident by a witness



1. Witnessing

Association Ends

witnesses : [Incident](#_72703355926e6f9d23631bfd436b3d75) [1..\*]



Incident observed by a witness.

witnessed by : [Witness](#_a29158762e9deaa170c39f468442f252) [0..\*]



Witnesses of an incident

# Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents::Failure

## Diagram: Failure



1. Failure

## Class Failure

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

Direct Supertypes

[Incident](#_72703355926e6f9d23631bfd436b3d75)

# Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents::Failure Categories

## Diagram: Failure Categories



1. Failure Categories

## Class Access Control Failure <<Category>>

Failure of permission controls to prevent unintended access.

Direct Supertypes

[Control Failure](#_d435d2a72c98c51f96c26a056cca4eb5)

## Class Control Failure <<Category>>

Failure of a policy or control process.

Direct Supertypes

[Failure Category](#_7f92c41b58c0056a267b8b5fbc000bd7)

## Class Cyber System Failure <<Category>>

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

Direct Supertypes

[System Failure](#_7af148db3cd6de3064b614dec120341a)

## Class Failure Category <<Category>>

A category of failure of a resource.

Direct Supertypes

[Failure](#_b40683e92bfe4e9d4ea7419f988b34c2)

## Class Industrial Control Failure <<Category>>

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

Direct Supertypes

[Cyber System Failure](#_159c67ab41f60cadc64b4e463ee4d104), [Physical System Failure](#_bc915b3e9f8fbd7965d14da551afd5a5)

## Class Physical System Failure <<Category>>

A category of danger of failure of any physical system.

Direct Supertypes

[System Failure](#_7af148db3cd6de3064b614dec120341a)

## Class Process Failure <<Category>>

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

Direct Supertypes

[Failure Category](#_7f92c41b58c0056a267b8b5fbc000bd7)

## Class System Failure <<Category>>

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

Direct Supertypes

[Failure Category](#_7f92c41b58c0056a267b8b5fbc000bd7)

# Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents::Impact Categories

## Diagram: Impact Categories



1. Impact Categories

## Class Communications Impact <<Category>>

Category of impact to the ability to communicate.

Direct Supertypes

[Information Impact](#_dedf5bede9319c2ebb81bd8f0e8aa42a)

## Class Compliance Impact <<Category>>

Impact on the ability to comply with policies.

Direct Supertypes

[Non-Technical Impact](#_4bffb09c727b56788e7de38a245db0cd)

## Class Control of Information Impact <<Category>>

Information becomes available to unauthorized actors (loss of confidentiality).

Direct Supertypes

[Information Impact](#_dedf5bede9319c2ebb81bd8f0e8aa42a)

## Class Decision-making Impact <<Category>>

Impact on the ability to make informed decisions.

Direct Supertypes

[Non-Technical Impact](#_4bffb09c727b56788e7de38a245db0cd)

## Class Disinformation Impact <<Category>>

Impact resulting from incorrect information.

Direct Supertypes

[Information Impact](#_dedf5bede9319c2ebb81bd8f0e8aa42a)

## Class Electromagnetic Spectrum Impact <<Category>>

Impact based on disruption in spectrum.

Direct Supertypes

[Impact Category](#_dee9f2345a1f910808f2263dfb689514)

## Class Environmental Impact <<Category>>

A danger to the environment.

Direct Supertypes

[Impact Category](#_dee9f2345a1f910808f2263dfb689514)

## Class Financial Impact <<Category>>

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

Direct Supertypes

[Impact Category](#_dee9f2345a1f910808f2263dfb689514)

## Class Health Impact <<Category>>

A category of danger to people's health.

Direct Supertypes

[Impact Category](#_dee9f2345a1f910808f2263dfb689514)

## Class Identity Spoof Impact <<Category>>

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

Direct Supertypes

[Disinformation Impact](#_1c7aba0f69325be4a8475e6515e816ed)

## Class Image Impact <<Category>>

Impact to how an entity is viewed by others.

Direct Supertypes

[Non-Technical Impact](#_4bffb09c727b56788e7de38a245db0cd)

## Class Impact Category <<Category>>

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

## Class Information Availability Impact <<Category>>

A category of danger impact where information becomes unavailable to the information owner.  
Availability: Ensuring timely and reliable access to and use of information.  
[NIST800]

Direct Supertypes

[Information Impact](#_dedf5bede9319c2ebb81bd8f0e8aa42a)

## Class Information Impact <<Category>>

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

Direct Supertypes

[Impact Category](#_dee9f2345a1f910808f2263dfb689514)

## Class Infrastructure Impact <<Category>>

Classification of impact to infrastructure such that it is not longer available to fulfill objectives.

Direct Supertypes

[Impact Category](#_dee9f2345a1f910808f2263dfb689514)

## Class Intellectual Property Impact <<Category>>

Category indicating a loss or compromise of intellectual property.

Direct Supertypes

[Non-Technical Impact](#_4bffb09c727b56788e7de38a245db0cd)

## Class Legal Impact <<Category>>

A categorization of impact to legal status or legal measures.

Direct Supertypes

[Non-Technical Impact](#_4bffb09c727b56788e7de38a245db0cd)

## Class Mission Impact <<Category>>

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

Direct Supertypes

[Impact Category](#_dee9f2345a1f910808f2263dfb689514)

## Class Non-Technical Impact <<Category>>

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

Direct Supertypes

[Impact Category](#_dee9f2345a1f910808f2263dfb689514)

## Class Safety Impact <<Category>>

Category of impact to the safety of a resource.

Direct Supertypes

[Non-Technical Impact](#_4bffb09c727b56788e7de38a245db0cd)

## Class Transport Impact <<Category>>

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

Direct Supertypes

[Impact Category](#_dee9f2345a1f910808f2263dfb689514)

# Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Incidents::Incident Response

## Diagram: Incident Response



1. Incident Response

Incident recovery is an incident response that restores the functionality of impacted resources and systems, including the removal of temporary containment measures.

## Class Incident Containment <<Role>>

Containment is an incident response that has two major goals: stopping the spread of the dangers causing the incident and preventing further harm. Containment includes the eradication of latent vulnerabilities of and infections to systems, such as the removal of malware.

Direct Supertypes

[Incident Response](#_0546b6cb684363d623353273263b40f5)

## Class Incident Recovery <<Role>>

Direct Supertypes

[Incident Response](#_0546b6cb684363d623353273263b40f5)

## Class Incident Response <<Role>>

Incident response is an activity to address and manage the scope and impact of an incident.

# 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.

## Diagram: Indicator



1. Indicator

## Diagram: Observability



1. Observability

## Diagram: Sighting



1. Sighting

## Class Blacklist Indicator

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

Direct Supertypes

[Indicator Watchlist](#_a3511bec5be4181aed91476c6b138095)

## Class Indicator

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

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

## Class Indicator Pattern

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

Direct Supertypes

[Indicator](#_0ea506f57adef61cfa374e799c7f4b3e)

## Class Indicator Watchlist

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

Direct Supertypes

[Indicator](#_0ea506f57adef61cfa374e799c7f4b3e)

## Class Whitelist Indicator

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

Direct Supertypes

[Indicator Watchlist](#_a3511bec5be4181aed91476c6b138095)

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

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

## Diagram: Risk



1. Risk

## Diagram: Risk Metrics



1. Risk Metrics

## Diagram: Risk Objectives



1. Risk Objectives

## Association Class Impose Strategy <<Relationship>>

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



1. Impose Strategy

Association Ends

imposes : [Risk Treatment Strategy](#_70807c15a257bc97a908d5f6b48d6c3d) [\*]



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

imposed by : [Risk Owner](#_3cfd42cf030efeac6a57064d1bb33318) [\*]



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

## Class Objective forSafety and Security

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

Direct Supertypes

[Risk Reduction Objective](#_776d60fce8516dacf9ec47f77bef3822)

## Class Objective to Protect Assets

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

Direct Supertypes

[Risk Reduction Objective](#_776d60fce8516dacf9ec47f77bef3822)

## Class Risk

[CNSSI 4009] Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of Event.  
[Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals', other organizations, and the Nation.]

## Class Risk Mitigation Strategy

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

Direct Supertypes

[Risk Treatment Strategy](#_70807c15a257bc97a908d5f6b48d6c3d)

## Class Risk Owner <<Role>>

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



1. Risk Owner

## Class Risk Reduction Objective

An objective of a risk owner to reduce risk.

## Association Class Risk To Resource <<Relationship>>

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



1. Risk To Resource

Association Ends

measures risk to : [Valued Asset](#_47ee5282957e27e87ceca3ae35620f9a) [1..\*]



Resources (aka assets) at risk.

has risk of harm : [Risk](#_6353799abeba2c8c30ac41459fde204f) [0..\*]



Potential risk to the subject resource.

## Association Class Risk Topic <<Relationship>>

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



1. Risk Topic

Association Ends

measures risk of : [Undesirable Situation](#_4bdee0568b2f36e553f586b458dace32) [1..\*]



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

may entail risk : [Risk](#_6353799abeba2c8c30ac41459fde204f) [0..\*]



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

## Association Class Stakeholder Risk <<Relationship>>

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



1. Stakeholder Risk

Association Ends

risk for : [Risk Owner](#_3cfd42cf030efeac6a57064d1bb33318) [1..\*]



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

has risk to objectives : [Risk](#_6353799abeba2c8c30ac41459fde204f) [1..\*]



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

Attributes

rank : [Integer](#_aeefbb09a8c456505ebb76cf8a103a03)



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

## Class Threat Likelihood <<Quantity Kind>>

A metric representing the likelihood of a threat occurring.

## Association Class Valuation of Asset <<Relationship>>

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

Association Ends

values : [Valued Asset](#_47ee5282957e27e87ceca3ae35620f9a) [\*]



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

supported by : [Objective to Protect Assets](#_9ebde53a1f70b354f94d28d6bc5313ff) [\*]



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

Attributes

sensitivity threshhold [0..1]



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

## Class Valued Asset <<Role>>

A system, organization, thing, process or person that is the direct concern of a stakeholder.  
[BMM] Asset: something of value owned by the enterprise

Attributes

replacement cost [0..1]



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

### Enumeration Likelihood Categories

A high-level scale of likelihood.

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

public enum Likelihood Categories

{Frequent, Probable, Occasional, Remote, Improbable}

Literals

Frequent



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

Probable



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

Occasional



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

Remote



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

Improbable



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

### Enumeration Severity Categories

A high-level scale of severity.

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

public enum Severity Categories

{Catastrophic, Critical, Marginal, Negligable}

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 mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.

Negligable



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

Known other enumerations

[Enumeration Likelihood Categories](#_2cbe30855e7c38eda8fd532436d545b8), [Enumeration Severity Categories](#_dbc10d4bb5d103ca01dfc9a56a55dca2)

Known other enumerations

[Enumeration Likelihood Categories](#_2cbe30855e7c38eda8fd532436d545b8), [Enumeration Severity Categories](#_dbc10d4bb5d103ca01dfc9a56a55dca2)

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

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

## Diagram: Risk Treatment



1. Risk Treatment

## Diagram: Safeguard Monitoring



1. Safeguard Monitoring

## Class Accept Risk

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

Direct Supertypes

[Risk Treatment Strategy](#_70807c15a257bc97a908d5f6b48d6c3d)

Attributes

risk level accepted



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

## Association Class Assume Risk <<Relationship>>

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



1. Assume Risk

Association Ends

transfer risk to : [Risk Agent](#_3dad71bdd97f208703b94ffa6e9fd693) [1..\*]



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

assumes risk from : [Transfer Risk](#_dcfb009f3ea89ca1b2bc5f2909bc3829) [1..\*]



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

## Class Avoid Danger

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

Direct Supertypes

[Risk Treatment Strategy](#_70807c15a257bc97a908d5f6b48d6c3d)

## Class Countermeasure <<Role>>

Countermeasure – actions, devices, procedures, techniques, or other measures that are designed to lower the likelihood of a threat scenario succeeding in its objectives, reduce the likely consequences of a threat scenario, or minimizing vulnerabilities that a threat scenario can exploit.  
Derived from [ISO 28001:2015], [ISO/IEC 2382:2015]  
  
Related concept: Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

## Association Class Countermeasure for Strategy <<Relationship>>

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



1. Countermeasure for Strategy

Association Ends

leverages countermeasure : [Countermeasure](#_27de7baab353145ea28cd16935bf947f) [1..\*]



Countermeasure which serves a risk mitigation strategy.

countermeasure for : [Risk Mitigation Strategy](#_4a31860e49ce04ad494ad84600b00364) [\*]



Mitigation strategy supported by a countermeasure.

## Association Class Countermeasure Mitigates <<Relationship>>

Undesirable situations mitigated by a countermeasure.



1. Countermeasure Mitigation

Association Ends

reduce harm via : [Countermeasure](#_27de7baab353145ea28cd16935bf947f) [\*]



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

mitigates : [Undesirable Situation](#_4bdee0568b2f36e553f586b458dace32) [1..\*]



Undesirable situation for which mitigation reduces the likelihood or impact.

## Class Defensive Step

A situation realizing a performance goal that is an objective to protect some valued asset.  
Derived from [Schweitzer 2013] Defense node

## Class Management Control

Derived from [NIST.IR.7298]: The security controls (i.e., safeguards or countermeasures) that focus on the management of risk and the management of information system security.  
SOURCE: SP 800-37; SP 800-53; SP 800-53A; FIPS 200

Direct Supertypes

[Countermeasure](#_27de7baab353145ea28cd16935bf947f)

## Class Mitigation Actor <<Role>>

Actor that performs a mitigation.

## Association Class Monitor <<Relationship>>

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



1. Monitor

Association Ends

watch based on : [Indicator](#_0ea506f57adef61cfa374e799c7f4b3e) [0..\*]



Indicators watched by the subject safeguard.

monitored by : [Monitoring Control](#_42a5d012e70fe684985bbcc8a0c4b4b5) [0..\*]



Activities monitoring an indicator using a monitoring safeguard.

## Class Monitoring Control

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

Direct Supertypes

[Operational Control](#_d62cdaff29d6a9151ff47cf9daa85ffd)

## Class Operational Control

[NIST.IR.7298] The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).  
SOURCE: SP 800-53; SP 800-37; FIPS 200

Direct Supertypes

[Countermeasure](#_27de7baab353145ea28cd16935bf947f)

## Class Risk Agent <<Role>>

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

Direct Supertypes

[Risk Owner](#_3cfd42cf030efeac6a57064d1bb33318)

## Association Class Risk Treatment <<Relationship>>

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



1. Risk Treatment

Association Ends

modifies risk : [Risk](#_6353799abeba2c8c30ac41459fde204f) [1..\*]



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

modified by : [Risk Treatment Strategy](#_70807c15a257bc97a908d5f6b48d6c3d) [0..\*]



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

## Class Risk Treatment Strategy

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

Attributes

degree of mitigation



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

## Association Class Safeguarding <<Relationship>>

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



1. Safeguarding

Association Ends

performs safeguard : [Operational Control](#_d62cdaff29d6a9151ff47cf9daa85ffd) [\*]



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

mitigated by : [Mitigation Actor](#_54ac2232a62cea44227bb2836a1a1334) [\*]



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

## Class Technical Control

Derived from [NIST.IR.7298]: The security controls (i.e., safeguards or countermeasures) that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.  
SOURCE: SP 800-53; SP 800-53A; SP 800-37; FIPS 200

Direct Supertypes

[Countermeasure](#_27de7baab353145ea28cd16935bf947f)

## Class Transfer Risk

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

Direct Supertypes

[Risk Treatment Strategy](#_70807c15a257bc97a908d5f6b48d6c3d)

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

## Diagram: Threat Actors



1. Threat Actors

## Class Disrupt Stakeholder's Objective

An action intended to harm the objectives of a stakeholder.

Direct Supertypes

[Disruptive Action](#_1b064056002f89a4ba6f4565e08b4f3a)

## Class Disruptive Action <<Role>>

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



1. Disruptive Actions

Direct Supertypes

[Dangerous Event](#_f2fa5e8341680da5e6e7a3cee51ee0a0)

## Class Disruptive Step

A situation realizing a performance goal that is an objective to disrupt some valued asset.  
Derived from [Schweitzer 2013] Attack node

## Association Class Perpetrate <<Relationship>>

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



1. Perpetrate

Direct Supertypes

[Contribution to Danger](#_b0b77eaf00ae3779a25865ff1f826f9d)

Association Ends

perpetrates : [Disruptive Action](#_1b064056002f89a4ba6f4565e08b4f3a) [\*]



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

perpetrator : [Threat Actor](#_a2021927a094afb50933eb829143a391) [1..\*]



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

## Class Threat Actor <<Role>>

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

Direct Supertypes

[Danger Source](#_e92228f26631bd725a174bd1e0d187f6)

# 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.

## Diagram: Undesirable Situations



1. Undesirable Situations

## Class Harm

Harm is a consequence of a situation that negatively impacts the objectives of stakeholders and therefore has negative desirability for those stakeholders.   
[Firesmith 2003] Harm is a negative impact associated with an asset. Harm is due to an accident when dealing with safety requirements, is due to an attack when dealing with security requirements, and may be due to both accidents and attacks when dealing with survivability requirements.   
[NIEM] Injury (More specific concept - Person specific).



1. Harm

Direct Supertypes

[Undesirable Situation](#_4bdee0568b2f36e553f586b458dace32)

## Association Class Harms Victim <<Relationship>>

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



1. Harms Victim

Association Ends

harms victim : [Victim](#_ebb283dc92a0ce409be895b1b9adf6e7) [\*]



Victim harmed by a situation.

victim of : [Undesirable Situation](#_4bdee0568b2f36e553f586b458dace32) [1..\*]



Situations for which the subject is a victim.

## Association Class Source of Harm <<Relationship>>

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



1. Harm Source

Association Ends

causes harm : [Harm](#_dc3f174a7d2e028c99d9ddf49c48c64f) [\*]



The harm to a resource caused by a undesirable situation.

harm from : [Undesirable Situation](#_4bdee0568b2f36e553f586b458dace32) [1..\*]



Situation which contributes to harm.

## Class Undesirable Condition <<Role>>

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

Direct Supertypes

[Undesirable Situation](#_4bdee0568b2f36e553f586b458dace32)

## Class Undesirable Event <<Role>>

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

Direct Supertypes

[Undesirable Situation](#_4bdee0568b2f36e553f586b458dace32)

## Class Undesirable Situation <<Role>>

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

Attributes

severity



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

## Class Victim <<Role>>

The role of any actor harmed by an incident.

Direct Supertypes

[Valued Asset](#_47ee5282957e27e87ceca3ae35620f9a)

# 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.

## Diagram: Vulnerability



1. Vulnerability

## Diagram: Vulnerability Identifiers



1. Vulnerability Identifiers

## Class Physical Vulnerability

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

Direct Supertypes

[Vulnerability](#_d936caf19626476c163d1b8384647aa0)

## Association Class Supporting Condition <<Relationship>>

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



1. Supporting Condition

Association Ends

condition for : [Undesirable Situation](#_4bdee0568b2f36e553f586b458dace32) [0..\*]



Incident or failure for which a vulnerability is a condition.

has condition : [Vulnerability](#_d936caf19626476c163d1b8384647aa0) [0..\*]



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

Attributes

required



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

## Class Vulnerability

A Vulnerability (of an object and a cause of failure, i.e. attack, natural cause, mistake, natural cause, accidental cause, or indirect) is the set of conditions under which an object fails under the particular cause of failure.  
This is consistent with NIST 800-30 (based on CNSSII 4009)  
Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Direct Supertypes

[Undesirable Condition](#_1e65602d4dd275cfb1ddaa86376c7fed)

Attributes

previously known : [Boolean](#_6119a00b0834641b9fe3f5ae9f58237f)



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

publicly known : [Boolean](#_6119a00b0834641b9fe3f5ae9f58237f)



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

score : [Vulnerability Metric](#_0255e9784e5af62b9441b7694cddbe80)



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

vector : [Vulnerability Vector](#_8b2a118b6c1323a86fe36c7eb129f9d9) [\*]



Factors influencing the subject vulnerabilitie's score.

## Class Vulnerability Identifier <<Value>>

An identifier for a vulnerability.

## Class Vulnerability Metric <<Quantity Kind>>

A metric representing the overall impact of a vulnerability.

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

## Diagram: Cyber Vulnerability



1. Cyber Vulnerability

## Class Communications Vulnerability

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

Direct Supertypes

[Cyber Vulnerability](#_7d4585c7408bb8f24ed25aed0548c471)

## Class CVE Identifier <<Value>>

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

Direct Supertypes

[Vulnerability Identifier](#_4860316d895463f3d07bcbfdf8d15257)

## Class Cyber Vulnerability

A vulnerability of any cyber related resource.

Direct Supertypes

[Vulnerability](#_d936caf19626476c163d1b8384647aa0)

## Class Information System Vulnerability

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

Direct Supertypes

[Cyber Vulnerability](#_7d4585c7408bb8f24ed25aed0548c471)

## Class Information Vulnerability

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

Direct Supertypes

[Cyber Vulnerability](#_7d4585c7408bb8f24ed25aed0548c471)

## Class OSVDB Identifier <<Value>>

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

Direct Supertypes

[Vulnerability Identifier](#_4860316d895463f3d07bcbfdf8d15257)

Attributes

value : [Integer](#_aeefbb09a8c456505ebb76cf8a103a03) [1]



Index into the OSVDB database.

## Class Software Vulnerability

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

Direct Supertypes

[Cyber Vulnerability](#_7d4585c7408bb8f24ed25aed0548c471)

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

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

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

## Diagram: Vulnerability Vectors



1. Vulnerability Vectors

## Class CVSS Score <<Quantity Kind>>

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

Direct Supertypes

[Vulnerability Metric](#_0255e9784e5af62b9441b7694cddbe80)

### 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.

Direct Known Superclasses

[Vulnerability Base Vector](#_196d76f570f8c2bd9cccd75b4f5ce514)

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

public enum Access Complexity

{High, Medium, Low}

Literals

High



Specialized access conditions exist. For example:

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

Medium



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

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

Low



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

examples:

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

### Enumeration Access Vector

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

Direct Known Superclasses

[Vulnerability Base Vector](#_196d76f570f8c2bd9cccd75b4f5ce514)

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

public enum Access Vector

{Local, Adjacent, Remote}

Literals

Local



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

Adjacent



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

Remote



A vulnerability that does not require physical or virtual proximity.  
[cvss] Network: A vulnerability exploitable with network access means the vulnerable software is bound to the network stack and the attacker does not require local network access or local access.  
Such a vulnerability is often termed “remotely exploitable”. An example of a network attack is an RPC buffer overflow.

### Enumeration Authentication

[CVSS] This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability. This metric does not gauge the strength or complexity of the authentication process, only that an attacker is required to provide credentials before an exploit may occur. The fewer authentication instances that are required, the higher the vulnerability score.  
It is important to note that the Authentication metric is different from Access Vector. Here, authentication requirements are considered once the system has already been accessed. Specifically, for locally exploitable vulnerabilities, this metric should only be set to “single” or “multiple” if authentication is needed beyond what is required to log into the system. An example of a locally exploitable vulnerability that requires authentication is one affecting a database engine listening on a Unix domain socket (or some other non-network interface). If the user must authenticate as a valid database user in order to exploit the vulnerability, then this metric should be set to “single.”

Direct Known Superclasses

[Vulnerability Base Vector](#_196d76f570f8c2bd9cccd75b4f5ce514)

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

public enum Authentication

{Multiple, Single, None}

Literals

Multiple



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

Single



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

None



Authentication is not required to access and exploit the vulnerability.

### Enumeration Availability Impact

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

Direct Known Superclasses

[Vulnerability Base Vector](#_196d76f570f8c2bd9cccd75b4f5ce514)

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

public enum Availability Impact

{None, Partial, Complete}

Literals

None



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

Partial



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

Complete



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

### Enumeration Collateral Damage Potential

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

Direct Known Superclasses

[Vulnerability Environmental Vector](#_ab1b10800dbf4458dc008d00f609c924)

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

public enum Collateral Damage Potential

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

Literals

None



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

Low



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

Low-Medium



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

Medium High



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

High



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

### Enumeration Confidentiality Impact

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

Direct Known Superclasses

[Vulnerability Base Vector](#_196d76f570f8c2bd9cccd75b4f5ce514)

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

public enum Confidentiality Impact

{None, Partial, Complete}

Literals

None



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

Partial



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

Complete



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

### Enumeration Exploitability

This metric measures the current state of exploit techniques or code availability. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability.   
Initially, real-world exploitation may only be theoretical. Publication of proof of concept code, functional exploit code, or sufficient technical details necessary to exploit the vulnerability may follow. Furthermore, the exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently. In severe cases, it may be delivered as the payload of a network-based worm or virus. The more easily a vulnerability can be exploited, the higher the vulnerability score.

Direct Known Superclasses

[Vulnerability Temporal Vector](#_e53dd5572fd3346fa73d5e5e4a87c50a)

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

public enum Exploitability

{Unproven, Proof of concept, Functional, High}

Literals

Unproven



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

Proof of concept



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

Functional



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

High



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

### Enumeration Integrity Impact

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

Direct Known Superclasses

[Vulnerability Base Vector](#_196d76f570f8c2bd9cccd75b4f5ce514)

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

public enum Integrity Impact

{None, Partial, Complete}

Literals

None



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

Partial



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

Complete



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

### Enumeration Remediation Level

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

Direct Known Superclasses

[Vulnerability Temporal Vector](#_e53dd5572fd3346fa73d5e5e4a87c50a)

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

public enum Remediation Level

{Offical Fix, Temporary Fix, Workaround, Unavailable}

Literals

Offical 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

### Enumeration Report Confidence

[CVSS] Confidence in a report.

Direct Known Superclasses

[Vulnerability Temporal Vector](#_e53dd5572fd3346fa73d5e5e4a87c50a)

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

public enum Report Confidence

{Unconfirmed, Uncorroborated, Confirmed}

Literals

Unconfirmed



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

Uncorroborated



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

Confirmed



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

### Enumeration Security Requirements

[CVSS] These metrics enable the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user’s organization, measured in terms of confidentiality, integrity, and availability. That is, if an IT asset supports a business function for which availability is most important, the analyst can assign a greater value to availability, relative to confidentiality and integrity. Each security requirement has three possible values: “low,” “medium,” or “high.” The full effect on the environmental score is determined by the corresponding base impact metrics. That is, these metrics modify the environmental score by reweighting the (base) confidentiality, integrity, and availability impact metrics. For example, the confidentiality impact (C) metric has increased weight if the confidentiality requirement (CR) is “high.” Likewise, the confidentiality impact metric has decreased weight if the confidentiality requirement is “low.” The confidentiality impact metric weighting is neutral if the confidentiality requirement is “medium.” This same logic is applied to the integrity and availability requirements.  
Note that the confidentiality requirement will not affect the environmental score if the (base) confidentiality impact is set to “none.” Also, increasing the confidentiality requirement from “medium” to “high” will not change the environmental score when the (base) impact metrics are set to “complete.”  
This is because the impact sub score (part of the base score that calculates impact) is already at a maximum value of 10.  
The greater the security requirement, the higher the score (remember that “medium” is considered the default).

Direct Known Superclasses

[Vulnerability Environmental Vector](#_ab1b10800dbf4458dc008d00f609c924)

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

public enum Security Requirements

{Low, Medium, High}

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)

### Enumeration Target Distribution

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

Direct Known Superclasses

[Vulnerability Environmental Vector](#_ab1b10800dbf4458dc008d00f609c924)

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

public enum Target Distribution

{None, Low, Medum, High}

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.

Medum



[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.

# Threat-risk-conceptual-model::Threat and Risk Specific Concepts::Weapons

## Diagram: Weapons



1. Weapons

## Class Cyber Weapon <<Role>>

A software weapon able to exploit the vulnerabilities of a cyber system.

Direct Supertypes

[Weapon](#_85732391519559b8da2839960274417a)

## Class Physical Weapon <<Role>>

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

Direct Supertypes

[Weapon](#_85732391519559b8da2839960274417a)

## Class Weapon <<Role>>

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

## Association Class Weapon Leverages Vulnerability <<Relationship>>

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



1. Weapon Leverages Vulnerability

Association Ends

leverages : [Vulnerability](#_d936caf19626476c163d1b8384647aa0) [0..\*]



Vulnerability that a weapon helps an actor take advantage of.

leveraged by : [Weapon](#_85732391519559b8da2839960274417a) [0..\*]



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