Agiliance RiskVision™

Risk Calculations

December 2013

Contents

Agiliance Compliance and Risk Calculation

This document describes methods of compliance and risk score calculation used by the Agiliance System. Topics covered in this document include:

- Overview of the two different methods that the Agiliance system provides for calculating risk scores: simple risk (or gap analysis) and security risk.
- Description of the formulas used for simple risk score calculation.
- Description of the formulas used for security risk score calculation. For security risk score calculations, also describes how the input values of formula are obtained and used in the Agiliance System. This also includes options for aggregating risk score on an entity based on the propagation of risk using entity relationships.

Security risk calculation performed by the Agiliance System follows principles described in the Microsoft "Security Risk Management Guide" [Reference 1], also following common guidelines provided by NIST and other organizations. Interested users may refer to the references provided in this document for more detailed information.

The Enterprise or IT Risk Management risk score calculation is described, followed by an explanation of Risk Propagation.

Agiliance Compliance and Risk Calculation Overview

Using the Agiliance System, compliance provides a measure of how well an entity performs against some collection of controls that define conformance to a set of policy standards, best practices, laws, regulations, etc. Calculated risk provides a measure of the entities exposure and likelihood of loss or hazard typically based on factors such as the entity's business value or criticality and exposure or vulnerability to threats which may affect or cause damage to the entity. In addition, risk can often be separated into categories of threats, such as those that affect or impact the accountability or confidentiality, integrity, or availability of an entity (commonly referred to as CIA risk), which overall will add risk to an enterprise or business operation.

Using the Agiliance System, you can assign any collection of automated or manual controls (and subcontrols) to an individual entity or group of entities. For each control or subcontrol, the Agiliance System stores a score number (for example, 0 to 10) for how the entity scored for compliance or passing/failing the control test. (For surveys, individual question answers are mapped to a number.)

To determine the overall compliance of the entity based on a number of different controls and subcontrols, the Agiliance RiskVision system totals up the scores for each control result using the weighting factor applied to each control (Weighting is generally on a scale of 0 between 1). It then returns compliance score as a percentage (zero to 100%, where zero is complete noncompliance and 100% is complete compliance). In addition, percentage ranges are assigned to visual indicators such as low (red), medium (yellow), and high (green) so the Agiliance Console can display a visual indication of the entity's overall compliance.

Simple Risk Score Calculation

The first method of risk score calculation, referred to as "**simple risk**" (also gap analysis) only takes in account pass/fail results and weighting from assigned controls and subcontrols and then factors in the entity's criticality to produce a risk for the entity. You might typically use this type of scoring if you want to apply your own weight to controls to determine which factors most affect your enterprise or company's risk, rather than use standard threat/vulnerability mappings to controls to define risk.

To calculate the compliance score of subcontrol

`10*choicescore` - if subcontrol is answered with option 4, then the corresponding choicescore is 2.

To calculate the compliance score of control

`(Sum of Subcontrol weight) * (subcontrol compliance score)/ Sum of subcontrol weight)`

The following table provides an example of sample controls and compliance rating results and shows the associated compliance and simple risk score calculations for a specific entity.

Controls	Weight	Compliance Score - CS (0 to 10)	Normalized Compliance Score (CS x Weight)	Risk (10-CS)
Overall Compliance and Risk Scores			(.6 + .35) / (1 + .5) or .633 (63.3%)	
Control 1	1	NA	15/25 or .6 (60%)	NA
Subcontrol 1	1	8	8	2
Subcontrol 2	0.5	9	4.5	1
Subcontrol 3	0.5	3	1.5	7
Subcontrol 4	0.5	2	1	8
Control 2	.5	NA	14.0/20 or .7 (70%)	NA
Subcontrol 5	1	10	10	0
Subcontrol 6	.5	5	2.5	5
Subcontrol 7	.5	3	1.5	7

The risk scores shown in this table are calculated using the **simple risk** formula, that is, where weighting factors are applied to individual controls or subcontrols to determine their contribution to a combined risk score. In this case, organizations would weigh the value of controls based on their relative importance among several compliance objectives.

Note: Using the security risk formula, you can calculate risk taking in account other factors which include the entity's vulnerability and the exposure and likelihood this entity has to threats associated with this control. See the following section for more information on the security risk method of risk calculation.

In this example, an entity has two main controls applied, with each control having a number of subcontrols. From this example, you can see the rollup of compliance and

risk scores, first from the subcontrol to control level, and finally aggregated across all controls applied to an entity.

At the control level, the normalized compliance scores are calculated as:

```
Sum of the normalized scores for the subcontrols) / (sum of (10 X weight of each subcontrol))
```

The normalized score for a subcontrol is the raw control score times the weighting factor (typically any number between 0 and 1). So for Control #1, the calculation of the compliance score for its associated subcontrols is:

```
(8 + 4.5 + 1.5 + 1) / (10 + 5 + 5 + 5)
```

This results in a compliance value of:

```
.6  or 60%
```

Note that the score aggregation at the highest level takes in account different weighting factors applied to controls #1 and #2 (Control #1 has a weight of 1.0 and Control #2 has a weighting factor of .5), so in this case the normalized scores for Control #1 make a larger contribution to the overall compliance and risk scores calculated across results of both controls.

ERM/ITRM Risk Score Calculation

In general, the risk score is calculated using the following formula:

```
risk score = exposure value * likelihood
```

Note: Exposure is otherwise called as impact.

Risk score is in the range between 0 and 100, and asset criticality, exposure value, and likelihood are all ranged between 0 and 10.

Below are different kinds of risk scores in both ERM/ITRM projects. For all these scores, asset criticality is always the same one that is defined at entity level within asset classification.

- Inherent risk score
- Current risk score
- Residual risk score
- ALE (risk score in dollar amount, and it uses a different calculation)

A detailed explanation of each score follows:

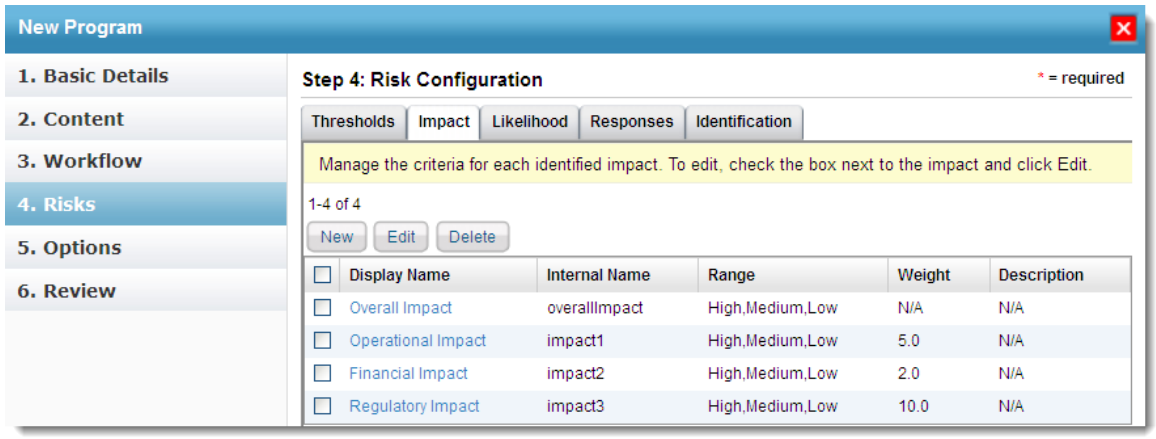
Inherent risk score

The exposure and likelihood values will get different user opnions and take the average or the middle value between highest or lowest, depending on the options set on each analysis.

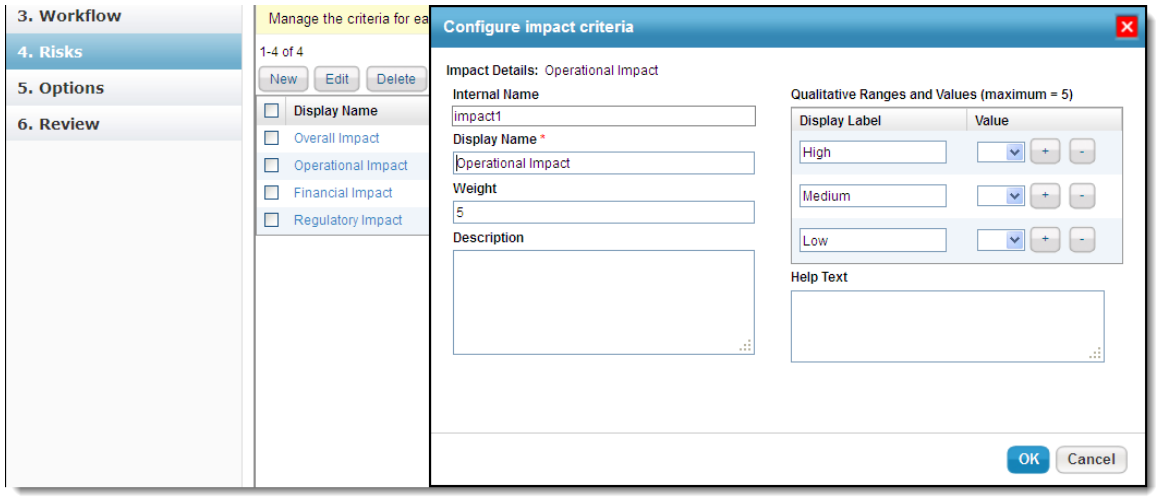
To calculate Inherent Risk Score

Impact: `sum of (ImpactWeight*Value) / sum of weights`

Likelihood: `sum of(LikelihoodWeight*Value) / sum of weights`



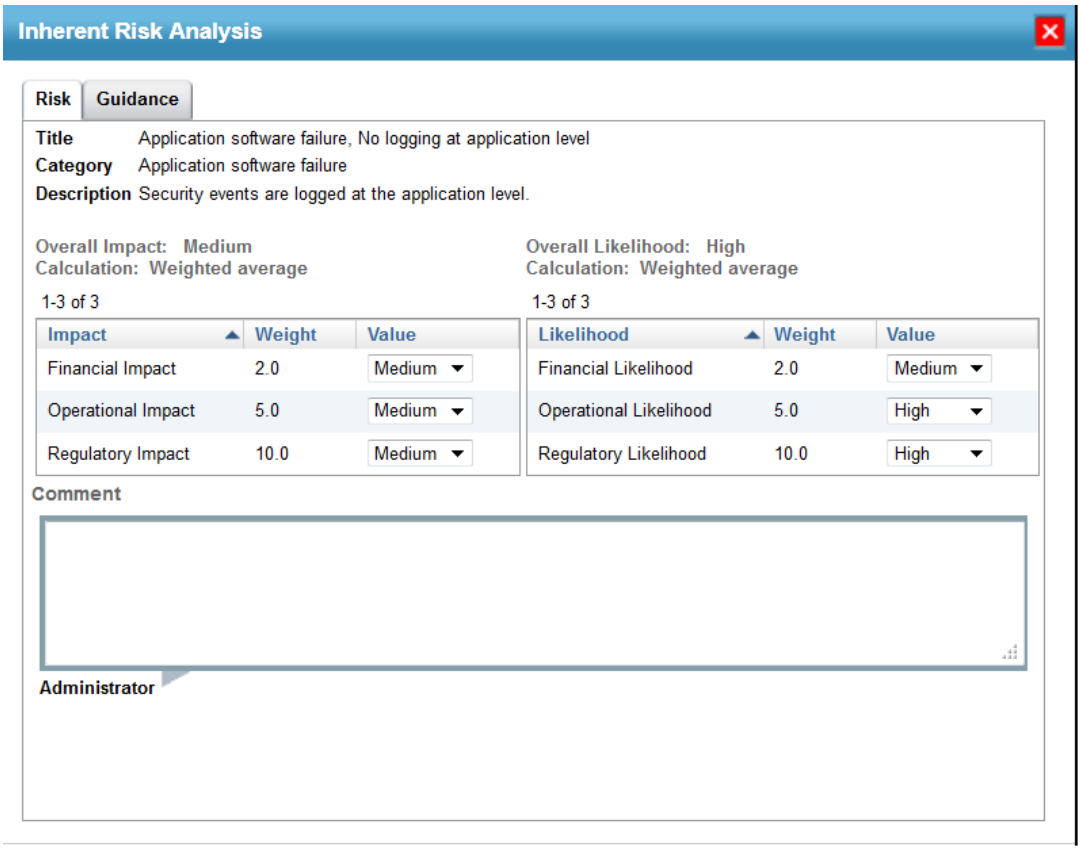
Note down the ranges of Operational, Financial and Regulatory impacts. Also, note down the weight's of the above impacts.



Click on the Operational, Financial and Regulatory impact's and note down the values for ranges (in the above window, they are High, Medium and Low)
The Custom defined ranges and custom defined values can also be used (through **ConfigureUI**).

Identify a Risk for the assessment in ERM

1 Select a particular Risk and click the "more actions" dropdown.
2 Select "Inherent Risk Analysis". The Inherent Risk Analysis window appears.

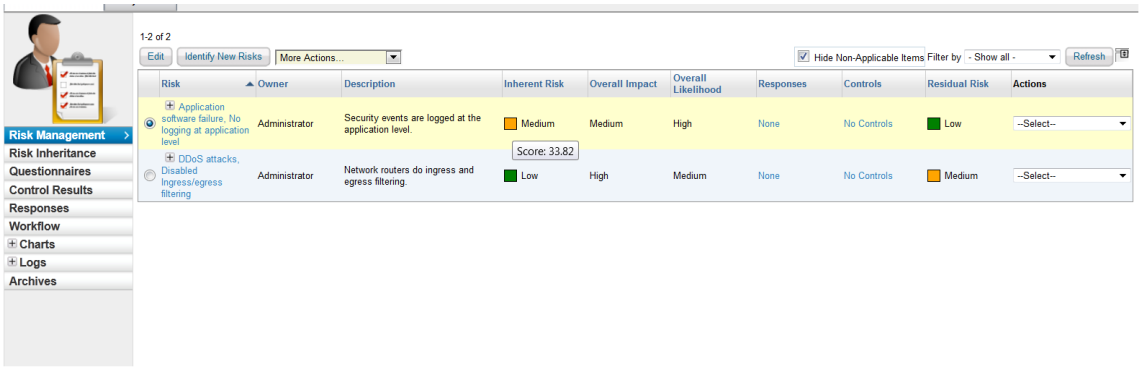


The Impact and Likelihood values are calculated as:

```
sum(ImpactWeight*Value) / sum of weights
sum(LikelihoodWeight*Value) / sum of weights
```

The values are:

```
Impact: ((2*5)+(5*5)+(10*5)) / 17 = 85 / 17 = 5
Likelihood: ((2*5)+(5*7)+(10*7)) = 115 / 17 = 6.76
```



Inherent Risk Value 33.82 is obtained as:

- In the previous page, results of Impact and Likelihood as 5 and 6.76 respectively
- `Inherent Risk = Impact * Likelihood = 5*6.76=33.8`

Average: take average from all opinions with best/worst cases.

Overall: take the middle value between highest and lowest.

Or users can choose NOT to use the opinions and provide values for the exposure/likelihood directly (override).

Instead of entering relative exposure values and likelihood, user may also decide to enter percentage and dollar values for likelihood and exposure (actually called impact in UI). In case of dollar value entered, we normalize the value using natural log e.g. highest $10000 and one risk has $100 as impact, the normalized exposure is

```
normalized exposure = 10 * ln(100) / ln(10000)
```

The highest dollar value is derived from the comparison all risks' impact dollar value, and the business cost of the entity.

Current risk score

The default Current Risk score formula is:

```
Current Risk score = Inherent Risk * (1-Risk Reduction Percentage)*(1-Control Protection Score)
```

Adding the `com.agiliance.web.risk.currentRisk.formula=2` property to the `agiliance.properties` file results in calculating the Current Risk score as:

```
Current Risk score = [(Inherent Risk – Residual Risk) * (1 – Control Protection score) * (1 – Risk Reduction score)] + Residual Risk
```

Average Risk Score = (Sum of Implemented Controls score) / (Total number of Implemented controls)

Control Protection Score = Average score – (0.75 * unimplemented control)/(total number of relevant controls)

The 0.75 value is based on the following property:
`com.agiliance.web.risk.protectionRiskScoreFactor`

If the Inherent Risk score is less than Residual Risk score, the default Current Risk score formula is applied even when the `com.agiliance.web.risk.currentRisk.formula` property is set to "`2`."

Residual risk score

Similar to inherent risk score, residual risk score is calculated based on users' input values of exposure and likelihood. Hence, use the average from worst and best cases.

Risk Propagation

Risk will propagate based on the predefined relationship (parent child for ERM) within an ERM project.

The direct for propagation is objective -> subprocess -> process. The real thing that matters is the asset hierarchy within the project.

And finally, all process level risk scores are aggregated to the project itself.

Security Risk Formula Calculation

Security risk scoring takes in account the threats and vulnerabilities addressed by assigned controls and calculates risk scores based on the weighting of the threat and vulnerability posed to individual entities. For security risk, the basic formula for calculating the risk score of an entity is:

```
Risk = Exposure x Criticality x Likelihood
```

where **exposure** is the extent of potential damage of a threat to an entity, **criticality** is the impact of an entity (using monetary business values and taking in account CIA factors such as confidentiality, integrity, and availability), and **likelihood** is the probability of a vulnerability to a threat being exploited.

Calculating security risk takes in account a couple of other factors:

```
Impact = Entity Criticality x Exposure Factor
```

Note:To populate the security risk score, use the following property in Agiliance.properties file.

```
com.agiliance.risk.security.enabled=true
```

Note: The risk calculated here is defined as the probability of realization of a threat due to vulnerability. If there is no vulnerability that can be exploited by a threat, then there is no risk for the particular threat.

Note: Information is based on values described in the Microsoft "*Security Risk Management Guide*" located at the following address:

http://www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/default.mspx

Determining Input for Risk Calculation on a Single Threat and Vulnerability Pair

As the risk formulae listed above, the risk calculation involves identifying the following information for entities:

1. Threat and vulnerability
2. Exposure of the threat
3. Likelihood of the vulnerability being exploited

Agiliance attempts to automate risk score calculation based on its knowledge of existing threats and vulnerabilities and its knowledge about an entity and corresponding input values such as policy compliance results, survey results, entity vulnerabilities, etc. (This means that the input values for risk score calculation are taken from already-acquired data.) However, authorized users may choose to overwrite the weight of these input values at any time to reflect their specific knowledge about a vulnerability that may be exploited by a threat for a particular entity.

Threat, Vulnerability, and Control Policy

Agiliance provides a library of many known threats, vulnerabilities, and controls. In addition, the library also provides mappings between threats, vulnerabilities, and controls, as shown in the examples included in Table B-1.

Table B-1. Threat, Vulnerability, and Control Policy Mapping

Threat	Vulnerability	Control policy	Default likelihood	Default exposure
Unauthorized network or system access	Unauthorized disclosure of confidential information	Handling of Confidential Data	4	4
Leaving sensitive documents exposed	Unauthorized disclosure of confidential information	Encryption	8	6

Note: Default likelihood and exposures in the library are actually separated into individual components of confidentiality exposure, integrity exposure and availability exposure.

Default likelihood and exposures in the library are actually separated into individual components of confidentiality exposure, integrity exposure and availability exposure. (We list a general exposure here for simplicity.) These mappings and default values are used in risk score calculations as described in following sections "Risk from policy violation."

The Agiliance Console provides a user interface for users to define new threats, new vulnerabilities, new controls and threat/vulnerability mappings, as well as to update default values for existing mappings.

Risk from Control Violations

For each entity, all executed controls, automated or manual (surveys), are included in the risk analysis based on the mappings shown in Table B-1.

Each policy execution (auto or manual) will result in a compliance level ranging between 0 and 10, where 0 means complete non-compliance and 10 means complete compliance. For risk calculations, an application-wide configuration value is used to determine if an entity is policy-compliant or non-compliant. The default value is 9, indicating that if a policy compliance result returned for an entity is less than 9, the entity is considered to be non-compliant.

The compliance result is aggregated at the control policy level to indicate the threat realization likelihood of the vulnerabilities mapped to the control policy. The compliance-result-to-likelihood relationship is established using the following formula:

```
Likelihood = ((10 – compliance level) * default likelihood)/10
```

So, a fully-compliant control policy will have a likelihood of 0 and a completely non-compliant policy will have the highest probability likelihood of 10, that is, the likelihood ranges from 0 to 10. This relationship follows calculation methods described in the Microsoft Security Risk Management Guide (Table B-2) and is supported by NIST's likelihood category as shown in Table B-3.

Table B-2. Likelihood defined by Microsoft Security Risk Management Guide

Likelihood Ranking consists of TWO parts	
Vulnerability Sum (Exposure attributes (select **one** value from below):	
High	5
Medium	3
Low	1
Likelihood value (1, 3, or 5)	Likelihood value
	+
Control Effectiveness (How effective are current controls? Yes - 0, No – 1)	
Is accountability defined and enforced effectively?	1,0
Is awareness communicated and followed effectively?	1,0
Are processes defined and practiced effectively?	1,0

Does existing technology or controls reduce threat effectively?	1,0
Are current audit practices sufficient to detect abuse or control deficiencies?	1,0
Sum of control attributes (0-5)	**Control effectiveness sum**

Table B-3. NIST Category of Likelihood

Likelihood Level	Description
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Note: See http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf for the NIST *Risk Management Guide for Information Technology Systems*.

The default exposure values from Table B-1 are used as exposure values for risk calculation.

Risk from Entity Vulnerabilities

An entity may also have associated vulnerabilities based on vulnerability scan results (using tools such Foundstone or Qualys) or vulnerabilities that are manually entered by users in the Agiliance Console. The Agiliance System and content library provides a mapping between these types of entity vulnerabilities and control rules. When entity vulnerabilities are created, the control rules that are mapped to the vulnerabilities are automatically assigned to the entity and marked as non-compliant. Then, these vulnerabilities will also be marked as "Auto-Resolved" under the entity.

Following the approach described in "Risk from Policy Violation," non-compliant controls will produce risks for the entity; however, users have the option to exclude certain vulnerabilities from risk calculation, on a per entity basis, by marking the vulnerabilities as "Ignored" under the entity's Compliance and Vulnerabilities tab.

Risk Score of an Entity

An entity might have hundreds of threats and vulnerabilities associated with it. Based on formulas described in the last section, "*Determining Input Values Used for Risk Calculation on a Single Threat and Vulnerability Pair*", the Agiliance System calculates risk score for each threat and vulnerability pair. Each risk score calculated for a single threat/vulnerability pair is in the range of 0 and 100 (with 0 indicating no risk and 100 indicating the highest risk).

At the entity level, users may choose to use the single highest risk score from all threat/vulnerability pairs to represent the risk score of the entity, or they can choose to add up risk scores from all individual threat/vulnerability pairs to represent the risk score of the entity as a sum value. (The final risk score for the entity has no limit, so may well exceed 100.)

If users choose to use the sum of individual risk scores, there is a cutoff value that users may specify to exclude risk contributions from individual threat/vulnerability whose risk score is below the cutoff value. The default cutoff value is 1.

Risk Score Propagation

Entities may have relationships with other entities. These relationships may be used for risk score propagation. For example, if entity A contains entity B, then the risk score from entity B should be reflected in the risk score of entity A.

The Agiliance System supports some well defined relationships such as:

Parent of (or **Child of**)

Owner of (or **Owned by**)

Consists of (or **Part of**)

Contains (or **Is inside**)

For (or **Has**)

Depends on (or **Needed by**)

Has access to (or **Can be accessed by**)

There is system-wide configuration available to allow users to choose which relationships should be used for risk propagation. The current risk propagation only supports values of 0 or 1, that is, risk is either fully propagated, or not at all. In future releases, the weight for each relationship may be specified and used to determine risk propagation.

After the risk score is propagated from a related entity, it will either be added to the total risk score of the entity (if risk score of the entity is configured to use the sum of all component risks), or compared with risk scores from other contributing items to select the highest risk value to represent the risk score of the entity (if risk score of the entity is configured to use the highest value among all component risk values).

References

[1] Microsoft, "Security Risk Management Guide"

http://www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/default.mspx

[2] Shon Harris, "How to conduct risk analysis":

http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1178862,00.html

[3] NIST, "Risk Management Guide for Information Technology Systems":

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[4] FIRST Forum, "A Complete Guide to the Common Vulnerability Scoring System (CVSS)":
http://www.first.org/cvss/cvss-guide.html.