



DeepL

Subscribe to DeepL Pro to translate larger documents.
Visit www.DeepL.com/pro for more information.

Customizing risk analysis

Instructions



for the ISO/ISM perspective, 1.04.2023

verinice.

Table of contents

1. Introduction	1
2. Risk analysis in verinice.....	2
2.1. Introduction	2
2.2. Procedure in verinice	4
3. Customizing in the SNCA.xml.....	5
3.1. Effect of damage	5
3.1.1. Object: Process.....	5
3.1.2. Object: Asset.....	8
3.1.3. Parallel adjustment in the scope object.....	9
3.2. Probability of occurrence	13
3.2.1. Object: Weak point.....	13
3.2.2. Object: Threat	14
3.2.3. Object: Scenario.....	15
3.2.4. Parallel adjustment for the scope object	18
3.3. Risk reduction	19
3.3.1. Object: Control	19
4. Customizing the translations" in the ".properties" files	23
4.1. Effect of damage	23
4.1.1. Object: Process.....	24
4.1.2. Object: Asset.....	24
4.1.3. Scope object	24
4.1.4. Risk of acceptance.....	27
4.2. Probability of occurrence	27
4.2.1. Object: Threat	27
4.2.2. Object: Weak point.....	27
4.2.3. Object: Scenario.....	27
4.2.4. Placeholder texts in the scope (threat & vulnerability)	29
4.3. Risk reduction	30
5. Placeholder texts in verinice (result).....	31
6. Tracking in the reports (from V1.26).....	32
6.1. Customize dimensions of the risk matrix.....	32
6.2. Color threshold configuration	33
7. Special use cases.....	38
7.1. Customizing risk analysis with new class	38
8. Copyright	39



1. Introduction

The customization options in verinice are made possible by the dynamic data model without the need for programming. For detailed instructions on customizing, please refer to Chapter 12 of the verinice user documentation.

This guide first explains the structure and basic setup of the risk analysis in the ISM/ISO perspective using the risk matrix of a standard report. The aim is to give you an understanding of which risk parameters are required to carry out the risk analysis and which objects need to be adapted. In addition, specific sections are highlighted that need to be adjusted depending on the use case for correct customizing.



2. Risk analysis in verinice

2.1. Introduction

The risk management matrix in the reports represents a risk probability and impact matrix. It helps you to define and assign the probability of occurrence of a potential risk from the scenario object and the impact of the asset object on your company with regard to the protection goals of availability, integrity and confidentiality. This matrix also enables the risk categories to be evaluated, allowing critical and particularly significant risks to be prioritized. It is made up of two integral components: probability and impact, and provides an overview of the number of high, medium and low risks.

Three matrices for the three protection goals from the risk assessment report are shown below as examples:

Risikomatrix: Vertraulichkeit (ohne implementierte Controls)

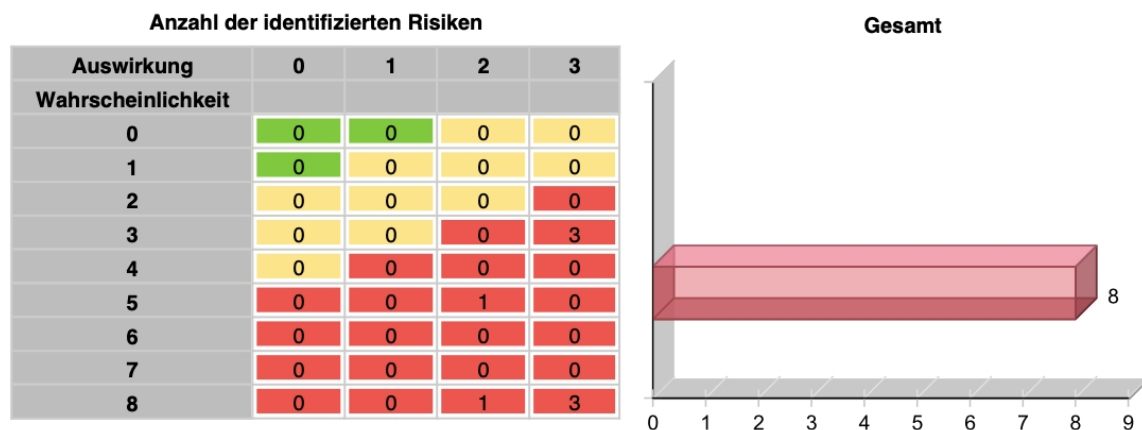


Figure 1: Extract from risk assessment report - risk matrix - confidentiality

Risikomatrix: Integrität (ohne implementierte Controls)

Anzahl der identifizierten Risiken			
Auswirkung	0	1	2
Wahrscheinlichkeit			
0	0	0	0
1	0	0	0
2	0	0	0
3	0	0	3
4	0	0	0
5	0	0	1
6	0	0	0
7	0	0	0
8	0	1	3

Die Tabelle zeigt die Anzahl der identifizierten Risiken und deren Schweregrad. Die Einstufung der Wahrscheinlichkeit und die Business-Impact-Klassifizierung folgt gesondert.

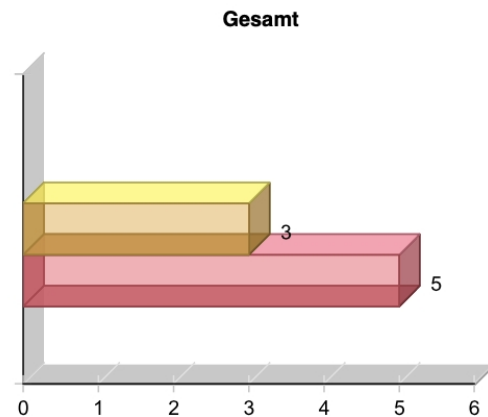


Figure 2: Extract from risk assessment report - risk matrix - integrity

Informations Risikomanagement Ergebnisse

SerNet
verinice.

Risikomatrix: Verfügbarkeit (ohne implementierte Controls)

Anzahl der identifizierten Risiken					
Auswirkung	0	1	2	3	4
Wahrscheinlichkeit					
0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	3
4	0	0	0	0	0
5	0	0	0	1	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	1	3

Die Tabelle zeigt die Anzahl der identifizierten Risiken und deren Schweregrad. Die Einstufung der Wahrscheinlichkeit und die Business-Impact-Klassifizierung folgt gesondert.

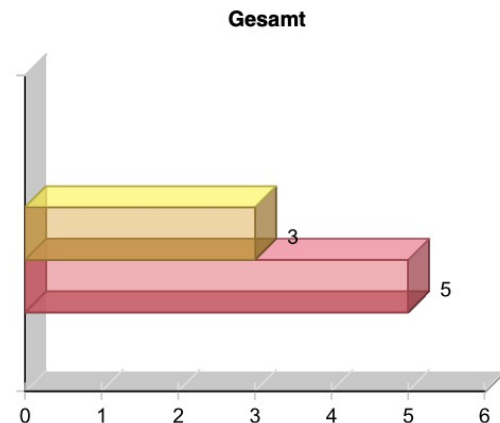


Figure 3: Extract from risk assessment report - risk matrix - availability

In most cases, it is recommended to work with the default values in order to minimize effort and avoid problems with reporting. However, if your company other risk parameters such as probability of occurrence (threat frequency, vulnerability levels) or business impact values and protection requirement categories, an alternative to customizing could be to carry out a mapping.

For a correct modification of the two risk components, it is important to understand how the risk value is calculated in verinice and how the risk analysis is carried out in verinice. The next chapter provides a detailed explanation of the risk analysis methodology in verinice.

2.2. Procedure in verinice

The risk analysis in verinice is carried out in several steps. First, the company's processes and assets are represented abstractly in the model view and a business impact analysis is carried out. These are then linked with each other and the business impact is derived from the higher-level process to the assets if necessary.

A vulnerability and a threat are then each to a risk scenario, or a new scenario object is created. The scenario is to an asset, depending on the asset for which the risk scenario represents a risk. An actual risk is only created through this link. The probability of occurrence of the scenario is then evaluated.

Once the assessments of the scenarios and assets have been completed, the risk analysis can be carried out in accordance with ISO/IEC 27005. The result shows that the risk value is made up of the sum of the probabilities of the scenarios and the business impact values. If several risk scenarios are linked to an asset, the two business impact values are added together and added to the probability.

The risk value is calculated using the following formula:

Formula for calculating the risk value:

Risk value = Probability of occurrence + Impact

The probability of occurrence is determined from the scenario object, w while the value for the effect comes from the asset object.

Controls can make a preventive contribution to minimizing risks. If a preventive measure or a control is linked to a risk scenario, this leads to a reduction in the probability of occurrence. If, on the other hand, a control is linked to an asset, it reduces the impact of damage and acts more as an emergency measure.

The modification of the probability of occurrence or impact by the control is defined under the control object. In around 80% of cases, the probability of the scenario is reduced by the control.

Once the risk analysis has been carried out, the result is under the corresponding asset. This result can be by creating a report.

3. Customizing in the SNCA.xml

Once you have decided which values you want to adjust, customizing by opening the SNCA.xml and properties files. The storage location of the SNCA.xml is specified in the verinice user documentation in chapter 12.

3.1. Effect of damage

The objects, processes and assets can be modified to adjust the impact of the damage.

3.1.1. Object: Process

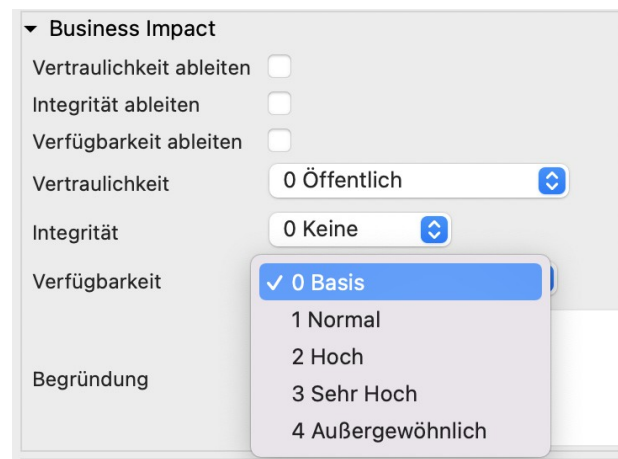


Figure 4 Business impact value for protection goal availability in the object process and asset

For the process object, you have the option of adjusting the value range or the business impact classes of the Business Impact Assessment (BIA). After this adjustment, you also store the corresponding values in the asset object.

The standard value range for the "Availability" protection target is 0-4.

Source code section from the SNCA.xml "Availability" protection objective for the process object

```
<huiproperty
  tags="Risk" id="process_value_availability"
  name="Availability"
  inputtype="numericoption" min="0" max="4">
  <depends option="process_value_method_availability"
value="0"/>
  <option
    id="process_value_availability_normal"
    name="0 Basic" value="0" />
  <option
    id="process_value_availability_high"
    name="1 Standard" value="1" />
  <option
```

```

        id="process_value_availability_very_high"
        name="2 Premium" value="2" />
    <option
        id="process_value_availability_very_high
        2" name="3 Enterprise" value="3" />
    <option
        id="process_value_availability_very_high
        3" name="4 Exceptional" value="4" />
    </huiproperty>
</huipropertygroup>

```

Figure 5: Business impact value for the integrity protection objective in the process and asset object

The standard value range for the "Integrity" protection target is 0-2.

Source code section from the SNCA.xml "Integrity" protection objective for the process object

```

<huiproperty
    tags="Risk" id="process_value_integrity"
    name="Integrity"
    inputtype="numericoption" min="0" max="2"
    value="0"/>
    <depends option="process_value_method_integrity"
    <option
        id="process_value_integrity_normal
        " name="0 None" value="0" />
    <option
        id="process_value_integrity_high"
        name="1 Normal" value="1" />
    <option
        id="process_value_integrity_very_high"
        name="2 High" value="2" />
    </huiproperty>

```


Figure 6: Business impact value for confidentiality protection objective in the process and asset object

The standard value range for the "Confidentiality" protection objective is 0-3.

Source code section from the SNCA.xml "Confidentiality" protection objective for process object

```
<huipropertygroup tags="Risk" id="process_value_group" name="Business Impact">

    <huiproperty
        tags="Risk"
        id="process_value_confidentiality"
        name="Confidentiality"
        inputtype="numericoption" min="0" max="3">
        <depends option="process_value_method_confidentiality"
value="0"/>

        <option
            id="process_value_confidentiality_normal"
            name="0 Public"
            value="0" />
        <option
            id="process_value_confidentiality_high"
            name="1 Company confidential"
            value="1" />
        <option
            id="process_value_confidentiality_very_high"
            name="2 Customer confidential"
            value="2" />
        <option
            id="process_value_confidentiality_very_high2"
            name="3 Sensitive"
            value="3" />

    </huiproperty>
```

3.1.2. Object: Asset

Source code section from the SNCA.xml "Confidentiality" protection objective for asset object

```
<huiproperty
    id="asset_value_confidentiality
    " name="Confidentiality"
    tags="Risk"
    inputtype="numericoption" min="0" max="3">
    <depends option="asset_value_method_confidentiality"
value="0"/>
    <option
        id="asset_value_confidentiality_normal"
        name="0 Public"
        value="0" />
    <option
        id="asset_value_confidentiality_high"
        name="1 Company confidential"
        value="1" />
    <option
        id="asset_value_confidentiality_very_high"
        name="2 Customer confidential"
        value="2" />
    <option
        id="asset_value_confidentiality_very_high2
        " name="3 Sensitive"
        value="3" />
</huiproperty>
```

Source code section from the SNCA.xml "Availability" protection objective for the asset object

```
<huiproperty
    id="asset_value_availability"
    tags="Risk"
    name="Availability"
    inputtype="numericoption" min="0" max="4">
    <depends option="asset_value_method_availability"
value="0"/>
    <option
        id="asset_value_availability_normal"
        name="0 Basic" value="0" />
    <option
        id="asset_value_availability_high"
        name="1 Standard" value="1" />
    <option
        id="asset_value_availability_very_high"
        name="2 Premium" value="2" />
```



```

        <option
            id="asset_value_availability_veryhigh2"
            name="3 Enterprise" value="3" />
        <option
            id="asset_value_availability_veryhigh3"
            name="4 Exceptional" value="4" />
    </huiproperty>

```

Source code section from the SNCA.xml "Integrity" protection objective for the asset object

```

<huiproperty
    id="asset_value_integrity"
    " tags="Risk"
    name="Integrity"
    inputtype="numericoption" min="0" max="2">
    <depends option="asset_value_method_integrity" value="0"/>
    <option
        id="asset_value_integrity_normal"
        name="0 None" value="0" />
    <option
        id="asset_value_integrity_high"
        name="1 Normal" value="1" />
    <option
        id="asset_value_integrity_very_high"
        name="2 High" value="2" />
</huiproperty>

```

3.1.3. Parallel adjustment in the scope object

If you have made changes to the business impact classification levels or definitions, you must also adjust these in the properties file under the scope object.

Source code section from the SNCA.xml for "Business Impact Classification" - Confidentiality protection objective for managing the placeholder text in verinice

```

<huipropertygroup name="Business impact classification"
id="org_classification" tags="Risk">
    <huiproperty name="Confidentiality"
id="org_class_asset_c" tags="Risk" inputtype="text" textrows="6">
        <defaultRule class="SimpleValue">
            <param id="org_class_asset_c_default">0 Public: No special
requirements.

1 External Use: Information for internal use and customers or partners.
Possible financial loss is between ? and ?, breach of legal requirements with
financial penalties is possible.

```



2 Internal Use: Information for internal use only. Financial loss between ? and ?. Breach of legal requirements could lead to high financial penalties. Personal injury could result by breach of confidentiality.

3 Sensitive: Possible financial loss higher than ? Breach of legal requirements could lead to prosecution and a prison sentence. Information loss could lead to serious injury or loss of life.

```
</param>
</defaultRule>
</huiproperty>
```

Source code section from the SNCA.xml for "Business Impact Classification" - Integrity protection objective for managing the placeholder text in verinice

```
<huiproperty name="Integrity" id="org_class_asset_i"
inputtype="text" textrows="6" tags="Risk">
  <defaultRule class="SimpleValue">
    <param id="org_class_asset_i_default">
```

0 None: Possible financial loss below ?

1 Normal: Possible financial loss between ? and ?. Breach of legal requirements could lead to financial penalties. Disclosure could result in personal injury.

2 High: Possible financial loss higher than ? Breach of legal requirements could lead to prison sentence. Disclosure could result in personal injury or death.

```
    </param>
  </defaultRule>
</huiproperty>
```

Source code section from the SNCA.xml for "Business Impact Classification" - Protection goal Availability for managing the placeholder text in verinice

```
<huiproperty name="Availability"
id="org_class_asset_a" inputtype="text" textrows="6"
tags="Risk">
  <defaultRule class="SimpleValue">
    <param id="org_class_asset_a_default">
```

0 Basic: Possible financial due to downtime loss below ? Recovery time objective (RTO) is higher than one week.

1 Normal: Possible financial loss due to downtime between ? and ?. RTO is lower than ?. Downtime could impair public image

2 High: Possible financial loss due to downtime between ? and ?. RTO is



than ? Downtime could impair public image or client relationship.

3 Very high: Possible financial loss due to downtime between ? and ?. RTO is lower than ?. Downtime could seriously impair public image or end client relationship.

4 Extraordinary: Special agreements with individual clients which do not fall into one of the above categories.

```
</param>
</defaultRule>
</huiproperty>
</huipropertygroup>
```

Risk Acceptance Value range

If you reduce or increase the value ranges of the protection goals through customizing, you must also adjust the value range in the Scope/Organization object accordingly. Using the default values for the risk analysis results in the following value ranges for risk acceptance for the three protection goals:

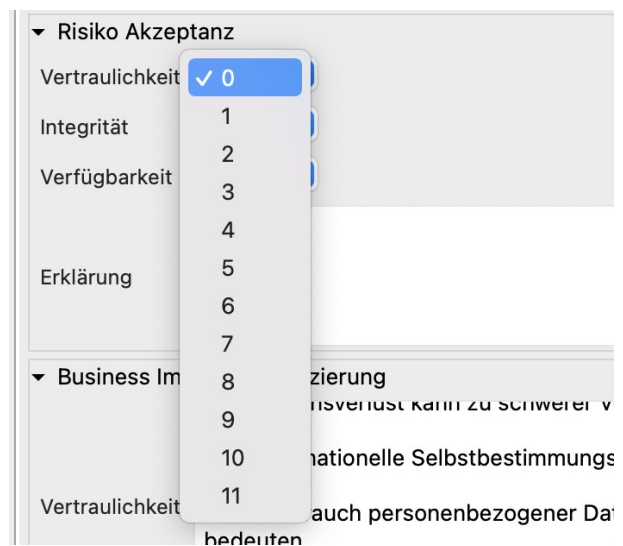


Figure 7: Risk acceptance value for confidentiality in verinice

- Confidentiality= 11,
 - because 8 (5 threat+ 3 vulnerability)+ 3 (number of business impact values for C)

▼ Risiko Akzeptanz

Vertraulichkeit 0

Integrität **✓ 0**

Verfügbarkeit 1

Erklärung 2

3

4

5

6

▼ Business Im zierung

7 isverlust kann zu schweren

8

9 nationale Selbstbestimmung

Vertraulichkeit 10 auch personenbezogener Da

Figure 8: Risk acceptance value for integrity in verinice

- Integrity= 10,
 - because $8 + (5 \text{ threat} + 3 \text{ vulnerability}) + 2$ (number of business impact values I)

▼ Risiko Akzeptanz

Vertraulichkeit 0

Integrität 0

Verfügbarkeit **✓ 0**

Erklärung 1

2

3

4

5

▼ Business Im zierung

6 isverlust kan

7

8 nationale Se

Vertraulichkeit 9 auch person

10

11 s bundeswei

12 möglicher fina

Figure 9: Risk acceptance value for availability in verinice

- Availability: Risk value= 12,
 - because $8 + (5 \text{ threat} + 3 \text{ vulnerability}) + 4$ (number of business impact values for A)

Source code section from the SNCA.xml in the scope object for risk acceptance values of the protection goals: Confidentiality, integrity and availability

```
<!-- risk analysis, ranges must match defined CIA levels+ scenario
probability -->
  <huipropertygroup name="Acceptable Risk Levels " id="org_riskgroup"
tags="Risk">
  <huiproperty
    name="Confidentiality" id="org_riskaccept_confid"
    inputtype="numericoption" min="0" max="11" tags="Risk"/>
  <huiproperty
    name="Integrity" id="org_riskaccept_integ"
    inputtype="numericoption" min="0" max="10" tags="Risk"/>
  <huiproperty
    name="Availability" id="org_riskaccept_avail"
    inputtype="numericoption" min="0" max="12" tags="Risk" />
  <huiproperty
    name="Explanation" id="org_riskaccept_expl" inputtype="text"
tags="Risk" />
</huipropertygroup>
```

3.2. Probability of occurrence

To modify the probability of occurrence, the threat and vulnerability objects are considered, as well as the resulting scenario in which the probability of occurrence specified. If no changes are made to these objects, you can skip the following chapter.

3.2.1. Object: Weak point

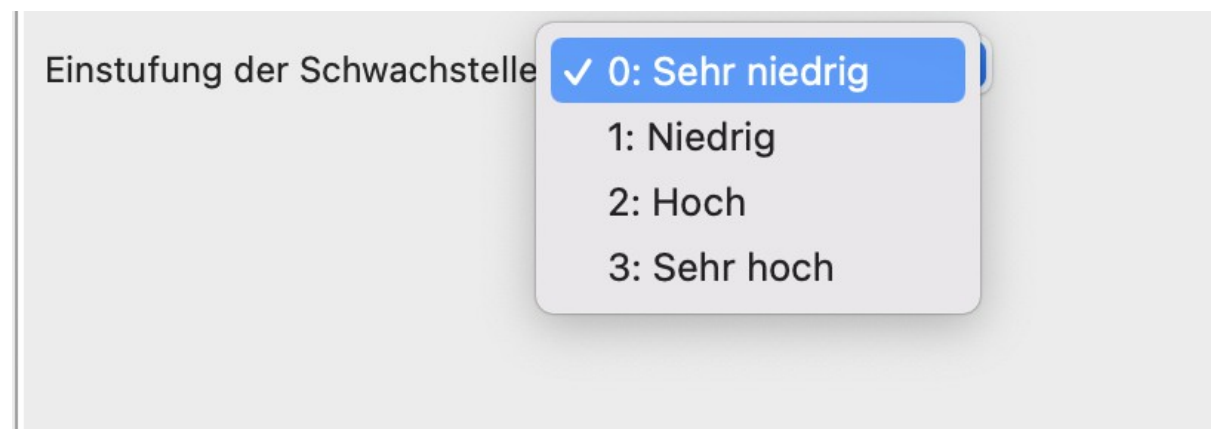


Figure 10: Vulnerability object with classification of the vulnerability in verinice

You have the option of adjusting the vulnerability levels according to your requirements. The default values for this are 0, 1, 2 and 3, where 0 stands for very low and 3 for very high.

Source code section from the SNCA.xml for vulnerability object

```
<huiproperty name="Ease of Exploitation " id="vulnerability_level"
inputtype="numericoption"
    min="0" max="3" defaultValue="0" tags="Risk">
    <option id="vulnerability_level_0" name="0: Very low" value="0"/>
    <option id="vulnerability_level_1" name="1: Low" value="1"/>
    <option id="vulnerability_level_2" name="2: High" value="2"/>
    <option id="vulnerability_level_3" name="3: Very High" value="3"/>
</huiproperty>
```

3.2.2. Object: Threat



Figure 11: Threat object with threat frequencies in verinice

You have the option of the threat frequency according to your needs. The default values for this are 0, 1, 2, ... to 5, where 0 stands for rarely and 5 for hourly.

Source code section from the SNCA.xml for threat object

```
<!-- Threat likelihood and impact, the higher of the two values will be used.
-->
    <huiproperty
        name="Threat Likelihood" id="threat_likelihood"
inputtype="numericoption" min="0" max="5" defaultValue="0" tags="Risk">
        <option id="threat_likelihood_0" name="Rare" value="0"/>
        <option id="threat_likelihood_1" name="Annually" value="1"/>
        <option id="threat_likelihood_2" name="Monthly" value="2"/>
        <option id="threat_likelihood_3" name="Weekly" value="3"/>
        <option id="threat_likelihood_4" name="Daily" value="4"/>
        <option id="threat_likelihood_5" name="Hourly" value="5"/>
    </huiproperty>
```


You have option to customize the following source code:

```
<!-- Optionally enable this to allow either likelihood or threat level
classification (or both): -->
    <huiproperty
        visible="false"
        name="Threat Impact" id="threat_impact" inputtype="numericoption"
min="0" max="5" tags="Risk">
        <option id="threat_impact_0" name="0: Very Low" value="0"/>
        <option id="threat_impact_1" name="1: Low" value="1"/>
        <option id="threat_impact_2" name="2: Medium" value="2"/>
        <option id="threat_impact_3" name="3: High" value="3"/>
        <option id="threat_impact_4" name="4: Very High" value="4"/>
        <option id="threat_impact_5" name="5: Catastrophic" value="5"/>
    </huiproperty>
</huientity>
```

3.2.3. Object: Scenario

▼ Wahrscheinlichkeit

Ableiten aus Bedr. / Schwachst.	<input type="checkbox"/>
Bedrohungshäufigkeit	2: Monatlich
Einstufung der Schwachstelle	1: Niedrig
Eintrittswahrscheinlichkeit	0: Weniger als 10%
Wahrscheinlichkeit mit implementierten (ja) Controls	0: Weniger als 10%
Wahrscheinlichkeit mit allen (ja, nein, teilw., unb., n.a.) Controls	0: Weniger als 10%
Wahrscheinlichkeit ohne n.a (ja, nein, teilw., unb.) Controls	0: Weniger als 10%

Figure 12: Probability calculation in the scenario object

In the same way, you must make the adjustments to the values for the vulnerability and threat in the scenario object.

Source code section from the SNCA.xml for scenario object for threat frequency

```
<huiproperty
    name="Threat Likelihood" id="incscen_threat_likelihood"
inputtype="numericoption" min="0" max="5" defaultValue="2"
tags="Risk">
    <depends option="incscen_likelihoodmethod" value="0"/>
    <option id="incscen_threat_likelihood_0" name="Rare"
value="0"/>
    <option id="incscen_threat_likelihood_1" name="Annually"
value="1"/>
```



```

        value="2"/>
        <option id="incscen_threat_likelihood_2" name="Monthly"
value="3"/>
        <option id="incscen_threat_likelihood_3" name="Weekly"
value="4"/>
        <option id="incscen_threat_likelihood_4" name="Daily"
value="5"/>
        <option id="incscen_threat_likelihood_5" name="Hourly"
value="5"/>
    </huiproperty>

```

Source code section from the SNCA.xml for scenario object for vulnerability classification

```

        <huiproperty name="Vulnerability exploitation"
id="incscen_vuln_level" inputtype="numericoption"
        min="0" max="3" defaultValue="1"
        tags="Risk">
        <depends option="incscen_likelihoodmethod" value="0"/>
        <option id="incscen_vuln_level_0" name="0: Very low"
value="0"/>
        <option id="incscen_vuln_level_1" name="1: Low" value="1"/>
        <option id="incscen_vuln_level_2" name="2: High" value="2"/>
        <option id="incscen_vuln_level_3" name="3: Very High"
value="3"/>
    </huiproperty>

```

Optionally, it is possible to adjust the probability of occurrence, which is calculated as a percentage and is grayed out by default in verinice.

Source code section from the SNCA.xml for scenario object for probability of occurrence

```

    <!-- Risk analysis, range has to match min to max sum possible from threat +
vulnerability -->
        <huiproperty
            tags="Risk"
            name="Probability of scenario occurring"
id="incscen_likelihood"
            inputtype="numericoption" min="0" max="8" editable="false"
            tooltip="Probability as determined by possible
combination
of threat and vulnerability, the lowest being a rarely occurring threat (less
than once a year) meeting a barely exploitable vulnerability. The highest
combination is an hourly occurring threat meeting an easily exploitable
vulnerability. Probability is scaled between those limits."
        >
            <option id="incscen_likely_0" name="0: Less than 10%"
value="0" />
            <option id="incscen_likely_1" name="1: 20%" value="1" />
            <option id="incscen_likely_2" name="2: 30%" value="2" />

```



```

        <option id="incscen_likely_3" name="3: 40%" value="3" />
        <option id="incscen_likely_4" name="4: 50%" value="4" />
        <option id="incscen_likely_5" name="5: 60%" value="5" />
        <option id="incscen_likely_6" name="6: 70%" value="6" />
        <option id="incscen_likely_7" name="7: 80%" value="7" />
        <option id="incscen_likely_8" name="8: 90% and higher"
value="8" />
    </huiproperty>

```

Source code section from the SNCA.xml for scenario object for probability with implemented (yes) controls

```

    <huiproperty tags="Risk"
id="incscen_likelihood_wcontrol" name="Probability with
implemented controls "
    inputtype="numericoption" min="0" max="8" editable="false">
        <option id="incscen_likelyc_0" name="0: Less than 10%"
value="0" />
        <option id="incscen_likelyc_1" name="1: 20%" value="1" />
        <option id="incscen_likelyc_2" name="2: 30%" value="2" />
        <option id="incscen_likelyc_3" name="3: 40%" value="3" />
        <option id="incscen_likelyc_4" name="4: 50%" value="4" />
        <option id="incscen_likelyc_5" name="5: 60%" value="5" />
        <option id="incscen_likelyc_6" name="6: 70%" value="6" />
        <option id="incscen_likelyc_7" name="7: 80%" value="7" />
        <option id="incscen_likelyc_8" name="8: 90% and higher"
value="8" />
    </huiproperty>

```

Source code section from the SNCA.xml for scenario object for probability with all controls

```

    <huiproperty id="incscen_likelihood_wplancontrol"
name="Probability with planned controls "
    inputtype="numericoption" min="0" max="8" editable="false"
tags="Risk">
        <option id="incscen_likelypc_0" name="0: Less than 10%"
value="0" />
        <option id="incscen_likelypc_1" name="1: 20%" value="1" />
        <option id="incscen_likelypc_2" name="2: 30%" value="2" />
        <option id="incscen_likelypc_3" name="3: 40%" value="3" />
        <option id="incscen_likelypc_4" name="4: 50%" value="4" />
        <option id="incscen_likelypc_5" name="5: 60%" value="5" />
        <option id="incscen_likelypc_6" name="6: 70%" value="6" />
        <option id="incscen_likelypc_7" name="7: 80%" value="7" />
        <option id="incscen_likelypc_8" name="8: 90% and higher"
value="8" />
    </huiproperty>

```

Source code section from the SNCA.xml for scenario object for probability without n.a. controls

```
<huiproperty id="incscen_likelihoood_without_na_control"
name="Probability without N.A. controls "
inputtype="numericoption" min="0" max="8" editable="false"
tags="Risk">
    <option id="incscen_likelynac_0" name="0: Less than 10%"
value="0" />
    <option id="incscen_likelynac_1" name="1: 20%" value="1" />
    <option id="incscen_likelynac_2" name="2: 30%" value="2" />
    <option id="incscen_likelynac_3" name="3: 40%" value="3" />
    <option id="incscen_likelynac_4" name="4: 50%" value="4" />
    <option id="incscen_likelynac_5" name="5: 60%" value="5" />
    <option id="incscen_likelynac_6" name="6: 70%" value="6" />
    <option id="incscen_likelynac_7" name="7: 80%" value="7" />
    <option id="incscen_likelynac_8" name="8: 90% and higher"
value="8" />
</huiproperty>
```

3.2.4. Parallel adjustment for the scope object

If you have made changes to the values or definitions in the Vulnerability and Threat objects, you must also adjust these in the properties file under the Scope object.

Source code section from the SNCA.xml for "Vulnerability"

```
<huipropertygroup id="org_vuln_class" name="Vulnerability classification"
tags="Risk">
    <huiproperty name="Level" id="org_class_vuln"
inputtype="text" textrows="6" tags="Risk">
        <defaultRule class="SimpleValue">
            <param id="org_class_vuln_default">


0: Exploitation of the vulnerability requires a directed attack, highly special knowledge or skill and resources that are not ordinarily available to an attacker. Rare Natural events or technical failures of a large scale could trigger the vulnerability.



1: Exploitation of the vulnerability requires a directed attack by a determined attacker. Natural events or technical failures could affect the vulnerability.



2: Exploitation of the vulnerability could occur by an automated attack (i.e. scripted attacks) or any attacker even with limited capabilities. Natural events or technical failures could affect the vulnerability.



3: Exploitation of the vulnerability could occur randomly and is highly


```



likely. Even someone without bad intentions could trigger the vulnerability accidentally. Common events will almost certainly trigger the vulnerability.

```
</param>
</defaultRule>
</huiproperty>
</huipropertygroup>
```

Source code section from the SNCA.xml for "Threat"

```
<huipropertygroup id="org_threat_class" name="Threat
classification" tags="Risk">
  <huiproperty name="Likelihood" id="org_class_threat"
inputtype="text" textrows="6" tags="Risk">
    <defaultRule class="SimpleValue">
      <param id="org_class_threat_default">
```

Threats are classified by the likelihood of their occurrence as follows:

- 0 Rare
- 1 Annually
- 2 Monthly
- 3 Weekly
- 4 Daily
- 5 Hourly

```
      </param>
    </defaultRule>
  </huiproperty>
</huipropertygroup>
```

3.3. Risk reduction

After adjusting the value ranges of the changed protection target, you should note that you must customize the levels under the control level in the control object in order to take the risk reduction into account.

3.3.1. Object: Control



▼ Control-Level

Auswirkung hinsichtlich Vertraulichkeit

Auswirkung hinsichtlich Integrität

Auswirkung hinsichtlich Verfügbarkeit

Wahrscheinlichkeit des Szenarios

Erläuterung

Figure 13: Control level under control object in verinice

In the control object, depending on whether you have made changes to the business impact classification, the threat frequency or the vulnerability classification, you must adjust either the impact on confidentiality, availability and integrity (if the control is linked to an asset) or the impact on the probability of occurrence of the scenario (if the control linked to a scenario).

The following section is relevant if a scenario is linked to a control:

Source code section from the SNCA.xml in the control object for impact with regard to confidentiality

```
<!-- Risk analysis, values must match those defined for asset CIA
and scenario probability -->
<huipropertygroup name="Control Strength" id="control_effectivenessgroup"
tags="Risk">
  <huiproperty name="Impact on Confidentiality"
id="control_effectiveness_confidentiality"
tags="Risk"
  inputtype="numericoption" min="0" max="3">
    <option name="No effect" id="control_eff_conf_0"
value="0" />
    <option name="Reduces 1 level" id="control_eff_conf_1"
value="1" />
    <option name="Reduces 2 levels" id="control_eff_conf_2"
value="2" />
    <option name="Reduces completely" id="control_eff_conf_3"
value="3" />
  </huiproperty>
```

The following section is relevant if an asset is linked to a scenario, as the control can then modify the effect on the protection goals.

Source code section from the SNCA.xml in the control object for impact with regard to integrity

```
<huiproperty tags="Risk" name="Impact on Integrity"
id="control_effectiveness_integrity"
    inputtype="numericoption" min="0" max="2">
    <option name="No effect" id="control_eff_integ_0"
value="0" />
    <option name="Reduces 1 level" id="control_eff_integ_1"
value="1" />
    <option name="Reduces completely" id="control_eff_integ_2"
value="2" />
</huiproperty>
```

Source code section from the SNCA.xml in the control object for effect regarding availability

```
<huiproperty tags="Risk" name="Impact on Availability"
id="control_effectiveness_availability"
    inputtype="numericoption" min="0" max="4">
    <option name="No effect" id="control_eff_avail_0"
value="0" />
    <option name="Reduces 1 level" id="control_eff_avail_1"
value="1" />
    <option name="Reduces 2 levels" id="control_eff_avail_2"
value="2" />
    <option name="Reduces 3 levels" id="control_eff_avail_3"
value="3" />
    <option name="Reduces completely" id="control_eff_avail_4"
value="4" />
</huiproperty>
```

The following section is relevant if a scenario is linked to a control, because then the control the probability of occurrence. Source code section from the SNCA.xml in the control object for the probability of the scenario

```
<huiproperty tags="Risk" name="Probability of scenario"
id="control_eff_probability"
    inputtype="numericoption" min="0" max="8">
    <option name="No effect." id="control_eff_prob_0"
value="0" />
    <option name="Reduces 1 level" id="control_eff_prob_1"
value="1" />
    <option name="Reduces 2 levels" id="control_eff_prob_2"
value="2" />
    <option name="Reduces 3 levels" id="control_eff_prob_3"
value="3" />
    <option name="Reduces 4 levels" id="control_eff_prob_4"
value="4" />
```

```

value="4" />
      <option name="Reduces 5 levels" id="control_eff_prob_5"
value="5" />
      <option name="Reduces 6 levels" id="control_eff_prob_6"
value="6" />
      <option name="Reduces 7 levels" id="control_eff_prob_7"
value="7" />
      <option name="Reduces completely" id="control_eff_prob_8"
value="8" />
    </huiproperty>
    <huiproperty tags="Risk" name="Explanation"
id="control_effectiveness_explanation2" inputtype="text"/>

</huipropertygroup>

```


4. Customizing the translations" in the ".properties" files

After you have adjusted the value ranges of the risk parameters in the SNCA.xml as well as the display names and, if necessary, IDs, you should check the German properties file in the next step. This file lists all IDs with the corresponding translations or definitions that appear in the verinice user interface.

It is advisable to also record the changes you have made in the English properties file to ensure consistent customization.

When opening the scna-messages_en.properties file in an editor program search for the IDs for which you have edited the definition or the display name in the SNCA.xml and adjust the translations.

Errors during customization in the properties files can lead to standard reports not being output correctly or verinice or the information network being displayed in the "fallback" language. This is because the German language file could not be loaded correctly. Verinice reacts sensitively to possible errors, in particular incorrect or duplicate IDs in the language file can lead to problems. Special care should therefore be taken when making adjustments.

Below you will find excerpts from the German properties file in which you can adapt the translations of the IDs.



In the properties file, umlauts, the "sz", the euro sign and breaks are coded as follows:

```
# small umlaut-u: \u00FC #  
capital umlaut-u: \u00DC #  
small umlaut-a: \u00E4 #  
capital umlaut-a: \u00C4 #  
small umlaut-o: \u00F6 #  
capital umlaut-o: \u00D6 #  
sz: \u00DF  
# Euro: \u20AC  
  
Upheavals: .\n\n
```

4.1. Effect of damage

Below you can see an overview of the IDs for the individual objects that relevant in the context of the damage effect. You can rename these to change the display name in verinice.



4.1.1. Object: Process

Process

process_value_confidentiality_very_high2=3 Sensitive
process_value_availability_very_high2=3 Very high process_value_availability_very_high3=4 Similar to

process_value_confidentiality_normal=0 \u00D6public
process_value_confidentiality_high=1 External use
process_value_confidentiality_very_high=2 Internal use

process_value_integrity_normal=0 None
process_value_integrity_high=1 Normal
process_value_integrity_very_high=2 High
process_value_availability_normal=0 Basic
process_value_availability_high=1 Normal
process_value_availability_very_high=2 High

4.1.2. Object: Asset

Asset

(asset_value_confidentiality=Confidentiality)
asset_value_confidentiality_normal=0 \u00D6public
asset_value_confidentiality_high=1 External use
asset_value_confidentiality_very_high=2 Internal use
asset_value_confidentiality_very_high2=3 Confidential
(asset_value_integrity=Integrit\u00E4t)
asset_value_integrity_normal=0 None
asset_value_integrity_high=1 Normal asset_value_integrity_very_high=2 High (asset_value_availability=availability)
asset_value_availability_normal=0 Basic
asset_value_availability_high=1 Normal
asset_value_availability_very_high=2 High
asset_value_availability_very_high2=3 Very high
asset_value_availability_very_high3=4 Very high

4.1.3. Scope object

If you want to modify the texts in the scope object, the following excerpts are relevant for you:

Confidentiality

org_class_asset_c=Confidentiality



org_class_asset_c_default=0 Public\ : No special requirements confidentiality.\n\nNo damage is to be expected for those affected. \n\n1 Information for internal use and for customers / partners.\n\nM\u00F6possible financial loss between ??? and ???, breach of legal requirements or contractual terms with financial impact is possible.\n\nNo particular impairment of the right to informational self-determination is to be expected.\n\nA possible misuse of personal data has only a minor impact on the social position or economic circumstances of the person concerned.\n\nNo risk to reputation, no loss of trust to be expected.\n\n2 Internal use\n: Information exclusively for internal use.\n\nM\u00F6possible financial loss between ??? and ???.\nBreach of legal requirements or contractual conditions with high financial damage possible.\n\nBreach of trust can lead to personal injury.\n\nA significant impairment of the data subject's right to informational self-determination appears possible.\n\nData misuse can significantly impair the data subject's social position or economic circumstances.\n\nA significant loss of reputation or trust is to be expected. \n\n3 Confidential\ : M\u00F6ginal financial loss of more than ???.\n\nBreach of legal requirements may lead to criminal prosecution with a possible prison sentence.\n\nLoss of information may lead to serious injury to persons or loss of life.\n\nThe data subject's right to informational self-determination is seriously impaired or fundamentally threatened.\n\nMisuse of personal data can mean social or economic ruin for the data subject.\n\nWidespread (up to nationwide) or lasting loss of reputation or trust is conceivable.

Integrity

org_class_asset_i=Integrit\u00E4t
org_class_asset_i_default=0 None\ : Potential financial loss under ???.\n\nNo particular damage effects are to be expected for those affected.\n\n1 Normal\n: Potential financial loss between ??? and ????.\n\nBreach of legal requirements or contractual conditions with financial implications is possible.\n\nViolation\u00DF may lead to personal injury.\n\nImpairment of the individual's right to informational self-determination appears possible.\n\nA falsification or other modification of the data may impair the social position or economic circumstances of the data subject.\n\n2 High\n: Potential financial loss higher than ???.\n\nBreach of legal requirements can lead to imprisonment.\n\nViolation\u00DF can lead to personal injury or loss of life.\n\nThe informational Right to self-determination of the person concerned is significant or serious



The falsification or other modification of personal data can lead to serious disadvantages for the person concerned and may even social or economic ruin. A widespread loss of reputation or trust, possibly even loss of existence, is conceivable.

Availability

org_class_asset_a=availability
org_class_asset_a_default=0 Basis\ : M\u00F6gual financial loss due to a failure under ??? . RTO (Recovery Time Objective) greater than ??? week(s). \n\nNo time-critical procedures, no special requirements for availability or restoration availability and resilience. The recovery is subject to the general rules for data backup. \n\n1 Normal\ : M\u00F6gual financial loss due to a failure between ??? and ??? . RTO is below ??? . \n\nFailure can mean public image damage. \n\nNo particular impairment of the right to informational self-determination is to be expected. \n\nOnly minor effects on the social position or economic circumstances of the person concerned are to be expected. \n\n2 High\ : M\u00F6gual financial loss due to a failure between ??? and ??? . RTO is below ??? . \n\nLoss can mean damage the company's image or impairment of customer relationships. \n\nInterference with the right to informational self-determination appears possible. \n\nOnly minor effects on the social position or economic circumstances of the person concerned are to be expected. \n\n3 Very high\ : Potential financial loss due to a default between ??? and ??? . RTO is below ??? . \n\nLoss can mean serious damage the company's image or loss of a customer. \n\nA significant impairment of the right to informational self-determination is to be expected. \n\nthe extent that the data subject may be significantly impaired in his or her social position or economic circumstances. \n\nLoss of the data may in serious disadvantages for the data subject. \n\n4 Externally\ : Similar\ : Special agreements with individual customers who do not fall into one of the above categories. \n\nThe data subject's right to informational self-determination is seriously impaired or fundamentally threatened. \n\nThe data subject's right to informational self-determination is seriously impaired or fundamentally threatened. \n\nLoss of personal data can mean social or economic ruin for the data subject \n\nA complete loss of reputation or trust, possibly even of an existentially threatening nature, is conceivable.

Here you can adapt the texts accordingly to make the desired changes to the business impact classifications.



4.1.4. Risk of acceptance

Risk of acceptance

```
org_riskgroup=Risk acceptance
org_riskaccept_expl=Declaration
org_riskaccept_confid=Confidentiality
org_riskaccept_integ=Integrit\u00E4t
org_riskaccept_avail=Availability
```

4.2. Probability of occurrence

Below is an overview of the IDs for the individual objects that relevant for calculating the probability of occurrence. You can rename these to change the display name in verinice:

4.2.1. Object: Threat

Threat

```
threat_likelihood=threat_frequency
threat_likelihood_0=0: Rarely likelihood threat
threat threat_likelihood_1=1\: Annually
threat_likelihood_2=2: Monthly
threat_likelihood_3=3\: Weekly
threat_likelihood_4=4\: Daily
threat_likelihood_5=5\: Annually
```

4.2.2. Object: Weak point

Vulnerability

```
vulnerability_level=Classification of the vulnerability
vulnerability_level_0=0\: Very low
vulnerability_level_1=1\: Low
vulnerability_level_2=2\: High
vulnerability_level_3=3\: Very high
```

4.2.3. Object: Scenario

Scenario

```
incscen_likely_0=0: Less than 10%
incscen_likely_1=1: 20%
incscen_likely_2=2: 30%
incscen_likely_3=3: 40%
```



incscen_likely_4=4: 50%
incscen_likely_5=5: 60%
incscen_likely_6=6: 70%
incscen_likely_7=7: 80%
incscen_likely_8=8: 90% and higher
incscen_likelihood_tooltip=Likelihood defined as the combination of possible threat and vulnerability. The lowest value means a rare threat (assumed frequency less than once a year) that a minor vulnerability. The highest value indicates an infrequent threat that an easily exploitable vulnerability. The calculated probability value is scaled linearly between these extremes.

incscen_threat_likelihood=threat_frequency
incscen_threat_likelihood_0=0: Rarely
incscen_threat_likelihood_1=1: Annually
incscen_threat_likelihood_2=2: Monthly
incscen_threat_likelihood_3=3: Weekly
incscen_threat_likelihood_4=4: Daily
incscen_threat_likelihood_5=5: Hourly

incscen_vuln_level =Classification of the vulnerability
incscen_vuln_level_0=0: Very low
incscen_vuln_level_1=1: Low
incscen_vuln_level_2=2: High
incscen_vuln_level_3=3: Very high

incscen_likelihood_wcontrol =likelihood with implemented (yes)
Controls

incscen_likelyc_0=0: Less than 10%
incscen_likelyc_1=1: 20%
incscen_likelyc_2=2: 30%
incscen_likelyc_3=3: 40%
incscen_likelyc_4=4: 50%
incscen_likelyc_5=5: 60%
incscen_likelyc_6=6: 70%
incscen_likelyc_7=7: 80%
incscen_likelyc_8=8: 90% and more

incscen_likelihood_wplancontrol =likelihood with all (yes, no, partial, unb., n.a.) controls

incscen_likelypc_0=0: Less than 10%
incscen_likelypc_1=1: 20%
incscen_likelypc_2=2: 30%
incscen_likelypc_3=3: 40%
incscen_likelypc_4=4: 50%
incscen_likelypc_5=5: 60%



incscen_likelypc_6=6: 70%
incscen_likelypc_7=7: 80%
incscen_likelypc_8=8: 90% and more

incscen_likelihood_without_na_control=Likelihood without n.a (yes, no, partial, unb.) Controls

incscen_likelynac_0=0: Less than 10%
incscen_likelynac_8=8: 90% and more

4.2.4. Placeholder texts in the scope (threat & vulnerability)

Threats

org_threat_class=threats org_class_threat=frequency
org_class_threat_default=Threats are classified based on the expected frequency as follows:\n\n0 Rarely orgtest \n\n1 Yearly \n\n2 Monthly \n\n3 Weekly \n\n4 Daily\u00E4glich\n\n

Weak points

org_vuln_class=weaknesses
org_class_vuln=grade
org_class_vuln_default=0 Very Low\ : Exploitation of the vulnerability requires a directed attack, highly specialized knowledge or skills and resources not typically to an attacker. Rare natural events or technical failure of a large scale can exploit the vulnerability.\n\n1 Low\ : Exploitation of the vulnerability requires a directed attack by a determined attacker. Natural events or technical failure can exploit the vulnerability.\n\n2 High\ : The vulnerability can be exploited by an automated attack (e.g. scripted attacks) or by an attacker with limited capacity and skills. Natural events or technical failure can trigger the vulnerability.\n\n3 Very high\Exploitation of the vulnerability could happen accidentally and is very likely. Even someone without malicious intent could unintentionally exploit the vulnerability. Frequently occurring events would undoubtedly the vulnerability.

4.3. Risk reduction

Below is an overview of the IDs for the control object, which you can rename to change the display name in verinice: ===== Object: Control

Control

```
control_eff_conf_0=No effect
control_eff_conf_1=Modifies 1 level
control_eff_conf_2=Modified 2 levels
control_eff_conf_3=Modified full\u00E4ndig
control_eff_integ_0=No effect
control_eff_integ_1=Modified 1 level
control_eff_integ_2=Modified full\u00E4ndig
control_eff_avail_0=No effect
control_eff_avail_1=Modified 1 level
control_eff_avail_2=Modified 2    levels
control_eff_avail_3=Modified 3 levels
control_eff_avail_4=Modified full
control_eff_probability=Probability of the scenario
control_eff_prob_0=No effect control_eff_prob_1=Modified
1 level
control_eff_prob_2=Modifies 2 levels
control_eff_prob_3=Modifies 3 levels
control_eff_prob_4=Modifies 4 levels
control_eff_prob_5=Modifies 5 levels
control_eff_prob_6=Modified 6 levels
control_eff_prob_7=Modified 7 levels
control_eff_prob_8=Modified full
```

It is advisable to also add the IDs and translations in the English properties file, whereby the English translations should ideally be identical to the text from the SNCA.xml.



5. Placeholder texts in verinice (result)

In verinice, you can view the results in the placeholder texts for the business impact classification, threat, vulnerability and risk acceptance values under the "Scope" area. Figure 14 shows the verinice editor view, in which the protection requirement categories are displayed.

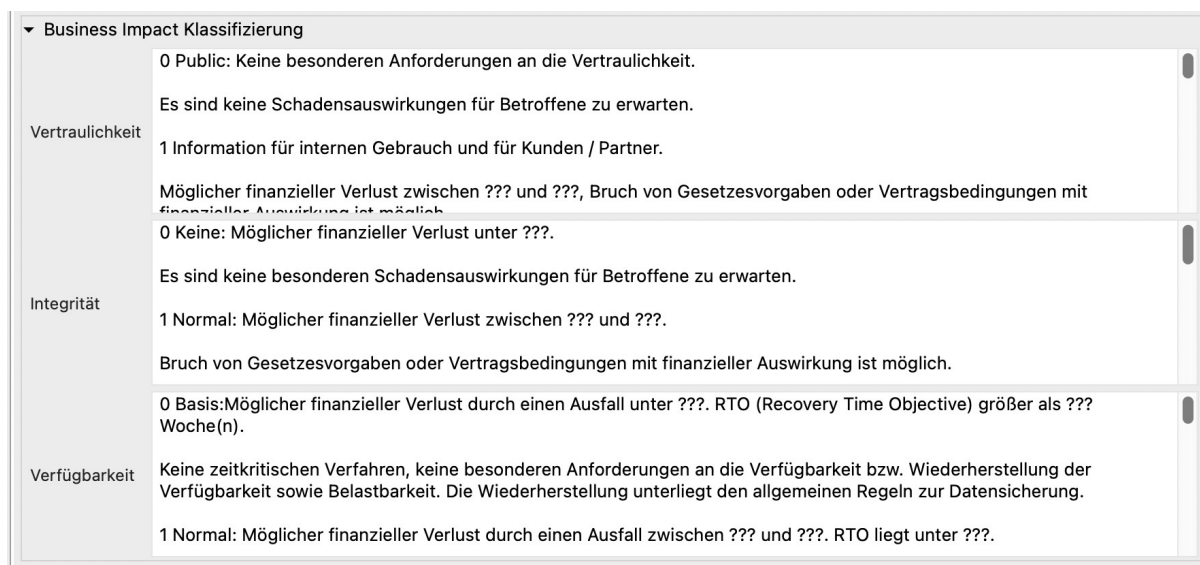


Figure 14: Business impact categories in the Scope/Organization object in verinice

The text adjustments made in the SNCA.xml or the properties files are now displayed in the verinice interface and in the generated reports. If you were to make these adjustments directly in the verinice interface, the change is not made centrally. In this case, you would have to repeat the adjustment manually each time you create a new information group.

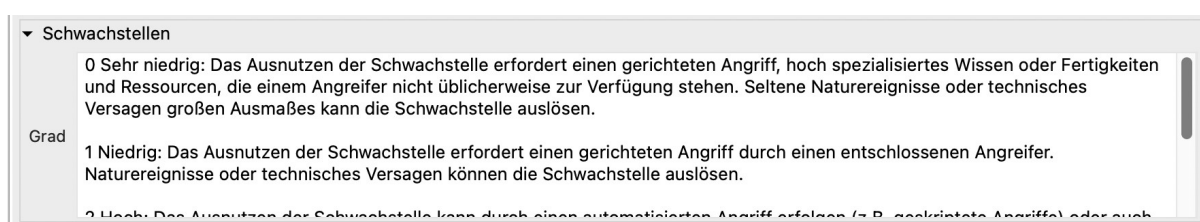


Figure 15: Classification of vulnerabilities in the Scope object in verinice

Figure 15 presents the section in the verinice editor view that shows the classification of the vulnerabilities.

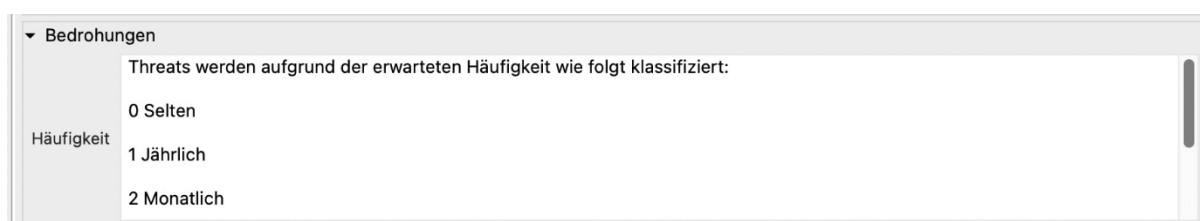


Figure 16: Threat frequency in scope in verinice

Figure 16 the section in the verinice editor view that displays the threat frequencies.

6. Tracking in the reports (from V1.26)

Three risk reports are available as standard in verinice: Risk assessment, risk treatment and risk calculation. If you make fundamental changes to the default values for the risk analysis, it is also necessary to adapt the reports. This ensures that the risk matrices are adapted according to your customizing.

The following explains how you can control the risk matrix and adapt it to your individual values. It is important to note that the reports are independent of the changes in the SNCA.xml. Therefore, every adjustment to the risk analysis also requires a corresponding adjustment to the reports.

6.1. Customizing the dimensions of the risk matrix

To the dimensions of the matrix, you must make changes in the following files:

Risk assessment report

- ism-riskmanagement_en.properties
- ism-riskmanagement.properties

Report risk treatment

- ism-risktreatment.properties
- ism-risktreatment_en.properties

To adjust the dimensions of the matrix, you should the values of the following attributes according to your desired number of levels. This will adjust the number of columns in the matrix accordingly:

```
risk_c_dim= 4  
risk_i_dim= 3  
risk_a_dim= 5  
risk_probability_dim 8 =
```

For each change, we recommend copying the properties files including the report from the remote_templates_remote folder and adding them to the local remote_templates_local folder. You can then make the changes locally and test them in verinice by running the report.

If you use verinice.PRO, you can easily exchange the new and old file via the report storage and store the updated report template centrally on the server. In the standalone version of verinice, you can simply keep the customized report in the local folder.



Risiko-Matrix: Vertraulichkeit

Anzahl identifizierter Risiken						
Auswirkung	0	1	2	3	4	5
Wahrscheinlichkeit						
0	0	0	0	1	0	0
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0

Die Tabelle zeigt die Anzahl der identifizierten Risiken und deren Schweregrade. Die Einstufung nach Eintrittswahrscheinlichkeit und Schadensauswirkung erfolgt weiter unten.

Figure 17: Confidentiality risk matrix - dimensions adjusted

The following figure serves as an example and shows how the dimensions for the x-axis (impact) and the y-axis (probability) have been modified. In this case, both dimensions have been changed to 6, and the resulting risk acceptance value is also 6.

6.2. Color threshold configuration

It is also possible to configure the color thresholds in the matrices. The defined risk acceptance value influences the color thresholds in the risk matrices. The red fields start according to the following formula:

Red (start)= Risk acceptance+ 1

The yellow fields end where the risk acceptance value is defined.

Yellow (end)= Risk acceptance

The following applies to the green area:

Green (end)= Risk acceptance - (XXX_correction_value+ 1)

This means that you can adjust the color threshold from green to yellow in the properties files:

This means that you can modify the color threshold from green to yellow in the properties files:

Risk assessment report

- ism-riskmanagement_en.properties
- ism-riskmanagement.properties



Report risk treatment

- ism-risktreatment.properties
- ism-risktreatment_en.properties

The following attribute **XXX_correction_value** must be adjusted by changing the value assigned to the ID:

- *XXX stands for the respective protection goal confidentiality, integrity,

availability #the color correction level for the grid

- integrity_correction_value= 3
- confidentiality_correction_value= 2
- availability_correction_value= 2

By setting this value, you determine how many yellow fields you would like to have in your matrix. This automatically results in the number of green fields. The red fields are defined by specifying the risk acceptance value.

The number 3 under **integrity_correction_value= 3** means, for example, that 4 yellow fields are counted upwards in the matrix for the "Integrity" protection objective, taking into account the following formula:

Default:

- $XXX_correction_value = \text{Number of yellow fields} - 1$

For each change made, we recommend copying the properties files including the report from the remote_templates_remote folder and adding them to the local remote_templates_local folder. In this way, you can implement the changes locally and test them in verinice by running the corresponding report.

One example:

Risk of acceptance= 6



Risk Matrix: Availability

Anzahl identifizierter Risiken					
Auswirkung	0	1	2	3	4
Wahrscheinlichkeit					
0	0	3	1	30	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0

Die Tabelle zeigt die Anzahl der identifizierten Risiken und deren Schweregrade. Die Einstufung nach Eintrittswahrscheinlichkeit und Schadensauswirkung erfolgt weiter unten.

Figure 18: Integrity risk matrix example XXX_correction_value = -1

XXX_correction_value= -1, means having 0 yellow fields in the matrix

Risk Matrix: Integrity

Anzahl identifizierter Risiken			
Auswirkung	0	1	2
Wahrscheinlichkeit			
0	1	4	29
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0

Die Tabelle zeigt die Anzahl der identifizierten Risiken und deren Schweregrade. Die Einstufung nach Eintrittswahrscheinlichkeit und Schadensauswirkung erfolgt weiter unten.

Figure 19: Risk matrix integrity Example XXX_correction_value = 0

XXX_correction_value= 0, means 1 yellow field in the matrix Result:

- Red(begin)=7
- yellow(end)=6
- green(end)=5

Risk Matrix: Availability

Anzahl identifizierter Risiken					
Auswirkung	0	1	2	3	4
Wahrscheinlichkeit					
0	0	3	1	30	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0

Die Tabelle zeigt die Anzahl der identifizierten Risiken und deren Schweregrade. Die Einstufung nach Eintrittswahrscheinlichkeit und Schadensauswirkung erfolgt weiter unten.

Figure 20: Risk matrix availability example XXX_correction_value = 1

XXX_correction_value= 1, means 2 yellow fields in the matrix Result:

- Red(begin)=7
- yellow(end)=6
- green(end)=4

Risk Matrix: Integrity

Anzahl identifizierter Risiken			
Auswirkung	0	1	2
Wahrscheinlichkeit			
0	1	4	29
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0

Die Tabelle zeigt die Anzahl der identifizierten Risiken und deren Schweregrade. Die Einstufung nach Eintrittswahrscheinlichkeit und Schadensauswirkung erfolgt weiter unten.

Figure 21: Integrity risk matrix example XXX_correction_value = 2

XXX_correction_value= 2, means having 3 yellow fields in the matrix Result:

- Red(begin)=7
- yellow(end)=6

- green(end)=3



7. Special use cases

7.1. Customizing risk analysis with new class

ATTENTION: If you add another class, such as data protection, to the protection goals, a risk matrix is not automatically generated for this in the report. You must also make adjustments at various points in the scope. For example, you should add a risk acceptance value for the new class under the root object.



8. Copyright

(c) 2023, SerNet GmbH. v.Designer by SerNet GmbH is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License. Based on a work at verinice.org. See <http://creativecommons.org/licenses/by-sa/3.0/> for details.

