No labels

Establish PSS risk management

In this section, the parameters of a PSS risk management strategy of a Company / Business Unit that affect the TRA tool are discussed, i.e. adaptation of risk rating scales, risk level definitions including risk acceptance criteria and management responsibilities.

The parameters of the PSS risk management strategy are integrated in TRA tool. The result is a TRA tool that matches the PSS risk management strategy of the Company / Business Unit, see RM1.

The relevant parameters of the TRA method, which are the basis of risk rating, are the following:

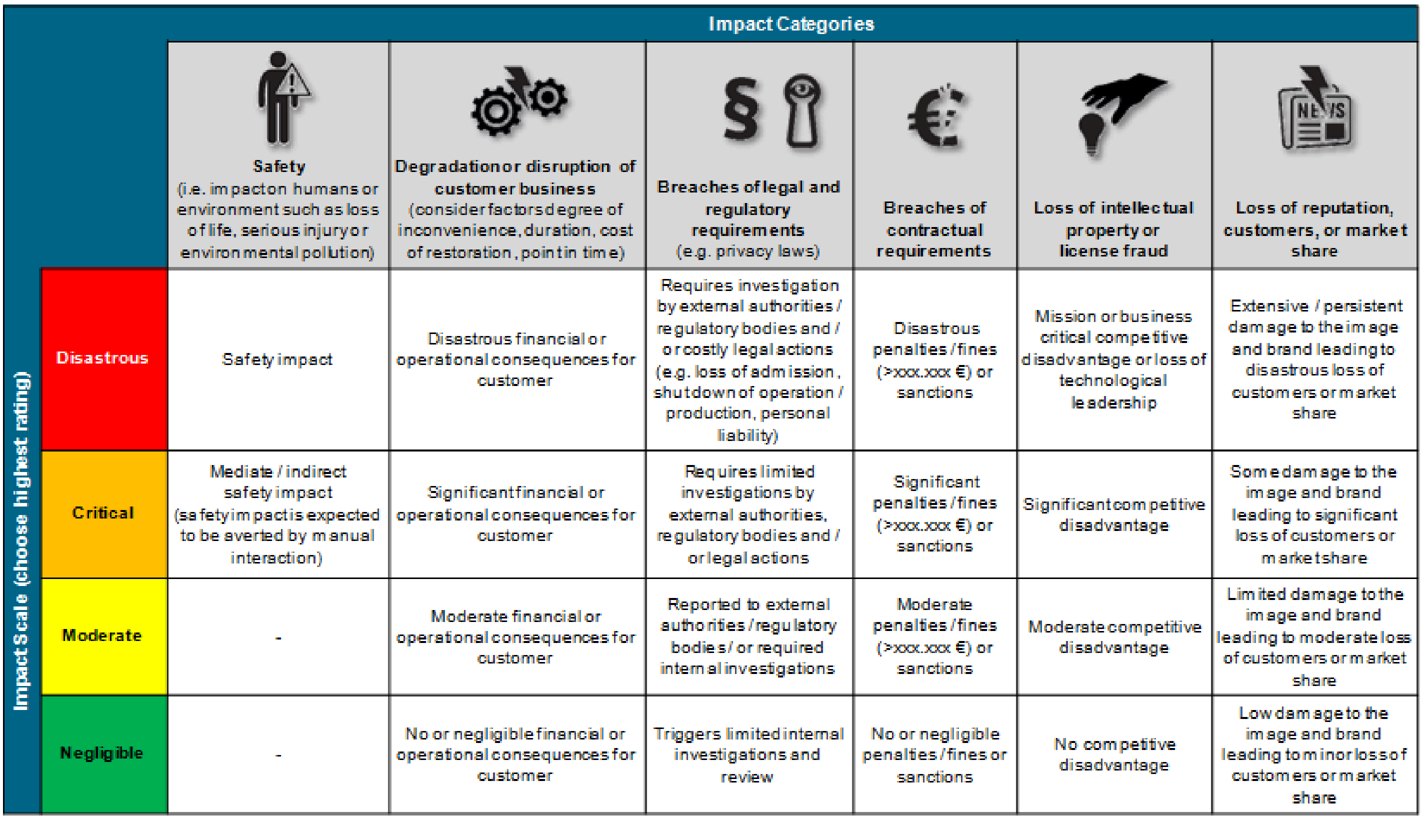
- *Impact rating scheme*
- *Likelihood rating scheme, consisting of two factors: exposures and exploitability/simplicity, and likelihood mapping table*
- *Risk rating mapping table for mapping likelihood and impact ratings to a risk level*
- *Risk level definition, including risk acceptance criteria associated with management responsibilities,*

These scales and mappings are an important part of the PSS risk management strategy (see OS1) of a Company / Business Unit, as they determine how threats are rated and handled. The PSS risk management strategy has to be decided by the Company / Business Unit management.

Furthermore, guidance for risk treatment options and tracking of risk treatment has to be provided for the organization.

Adaptation of impact rating scheme (Sheet ‚Impact')

The default impact rating scheme of the TRA tool, shown in Figure 2-1, has two axes. The first consists of impact categories, while the second axis defines the scale to rate the severity of impacts. Each cell in the impact rating scheme contains texts that provide indicators for selecting the appropriate impact level in a specific category.



		Impact Categories					
		Safety (i.e. impact on humans or environment such as loss of life, serious injury or environmental pollution)	**Degradation or disruption of customer business** (consider factors degree of inconvenience, duration, cost of restoration, point in time)	**Breaches of legal and regulatory requirements** (e.g. privacy laws)	**Breaches of contractual requirements**	**Loss of intellectual property or license fraud**	**Loss of reputation, customers, or market share**
Impact Scale (choose highest rating)	Disastrous	Safety impact	Disastrous financial or operational consequences for customer	Requires investigation by external authorities / regulatory bodies and / or costly legal actions (e.g. loss of admission, shutdown of operation / production, personal liability)	Disastrous penalties / fines (>xxx.xxx €) or sanctions	Mission or business critical competitive disadvantage or loss of technological leadership	Extensive / persistent damage to the image and brand leading to disastrous loss of customers or market share
	Critical	Mediate / indirect safety impact (safety impact is expected to be averted by manual interaction)	Significant financial or operational consequences for customer	Requires limited investigations by external authorities, regulatory bodies and / or legal actions	Significant penalties / fines (>xxx.xxx €) or sanctions	Significant competitive disadvantage	Some damage to the image and brand leading to significant loss of customers or market share
	Moderate	-	Moderate financial or operational consequences for customer	Reported to external authorities / regulatory bodies / or required internal investigations	Moderate penalties / fines (>xxx.xxx €) or sanctions	Moderate competitive disadvantage	Limited damage to the image and brand leading to moderate loss of customers or market share
	Negligible	-	No or negligible financial or operational consequences for customer	Triggers limited internal investigations and review	No or negligible penalties / fines or sanctions	No competitive disadvantage	Low damage to the image and brand leading to minor loss of customers or market share

Figure 2-1: Default impact rating scheme

The work team TRA agreed that the impact categories and the impact levels should be used uniformly across Siemens. However, the generic impact indicators should be made more specific for the business domains of a Company / Business Unit. More specific indicators help the TRA workshop participants in selecting an appropriate impact level, and hence support consistent impact rating in the Company / Business Unit.

The impact categories are derived from the impact categories of the Enterprise Risk Management (ERM) Risk Impact Matrix:

- Safety: If an attack that exploits a weakness in the system leads to loss of life, injuries or environmental damage, then Siemens business objectives are affected, as Siemens products or solutions are expected not to cause such hazards. (ERM Impact category 'Business Objectives')
- Degradation or disruption of customer business:The costs arising from attacks that stop the system or even lead to damage to the system highly depend on the type of customer business, and hence should be detailed. While such costs do not affect Siemens directly, nevertheless the Siemens business objectives are affected, if Siemens products and solutions fail to match customers' needs. (ERM Impact category 'Business Objectives')
- Breaches of legal and regulatory requirements:The legal and regulatory requirements that are relevant for the Company / Business Unit, together with the consequences of breaches, should be listed. E.g. for Healthcare, privacy laws apply, and the consequences are clearly defined. (ERM Impact category 'Regulatory Bodies')
- Breaches of contractual requirements: Financial figures appropriate for the Company / Business Unit should be applied. The financial figures could be taken from the ERM Risk Impact Scales of the Company / Business Unit, if this is considered appropriate. If the ERM figures are considered too high for project contexts, lower figures could be chosen. (ERM Impact category 'Financial')
- Loss of intellectual property or license fraud: If Siemens intellectual property is obtained by competitors, clearly business objectives are affected. Likewise, circumventing license mechanisms impairs business objectives. (ERM Impact category 'Business Objectives') If the intellectual property of the customer is obtained by competitors, following the argument of the category 'Degradation or disruption of customer business', the Siemens objectives are affected. Again, the level of impact highly depends on the type of customer business, and the impact indicators should be detailed.
- Loss of reputation, customers or market share: If incidents or vulnerabilities related to Siemens products or solutions are published or shared in domain-specific communities, the reputation of Siemens is damaged. (ERM Impact category 'Media') Indicators in an Company / Business Unit could refer to characteristics of communities and customer relationship.

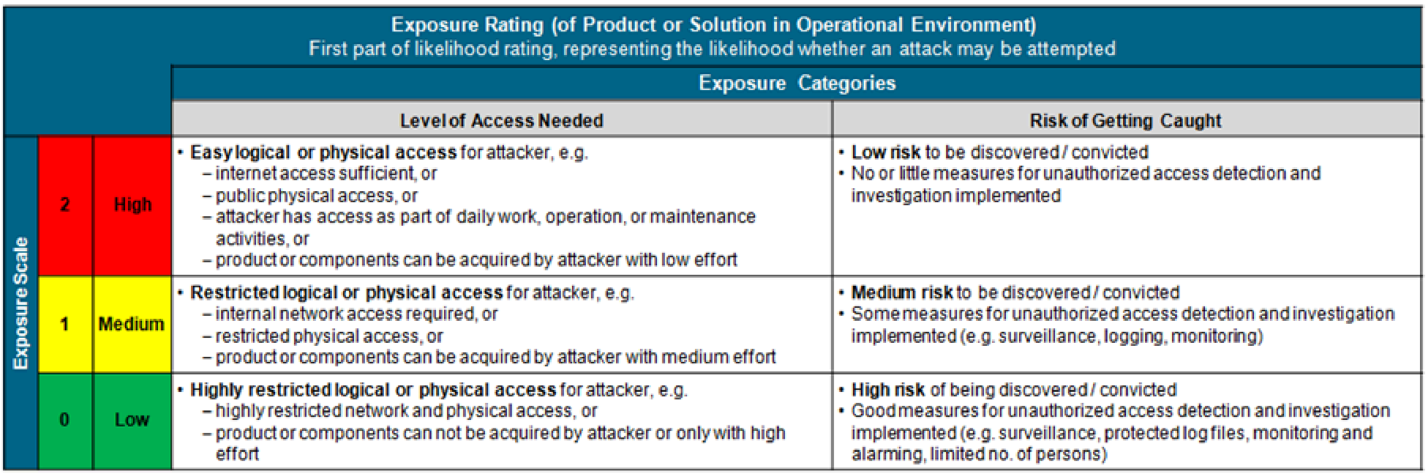
Note that the same impact rating scheme should be used for TRA and PSS Project Classification. So the adapted impact rating scheme for TRA (or a reference) has to be synchronized with PSS Project Classification Tool. In general further detailing is recommended, deleting parts needs a PSSC check.

Adaptation of likelihood rating scheme (Sheet ‚Likelihood')

The likelihood consists of two factors. First is the exposure, which defines whether an attack may be attempted by rating how much effort is needed to interact with the target (Figure 2-2). The second factor is the exploitability or simplicity, which represents the likelihood of an attempted attack to succeed (Figure 2-3). For a more detailed description of the likelihood rating factors see the section Rating Likelihood and Impact to Derive Risk of the TRA method description.

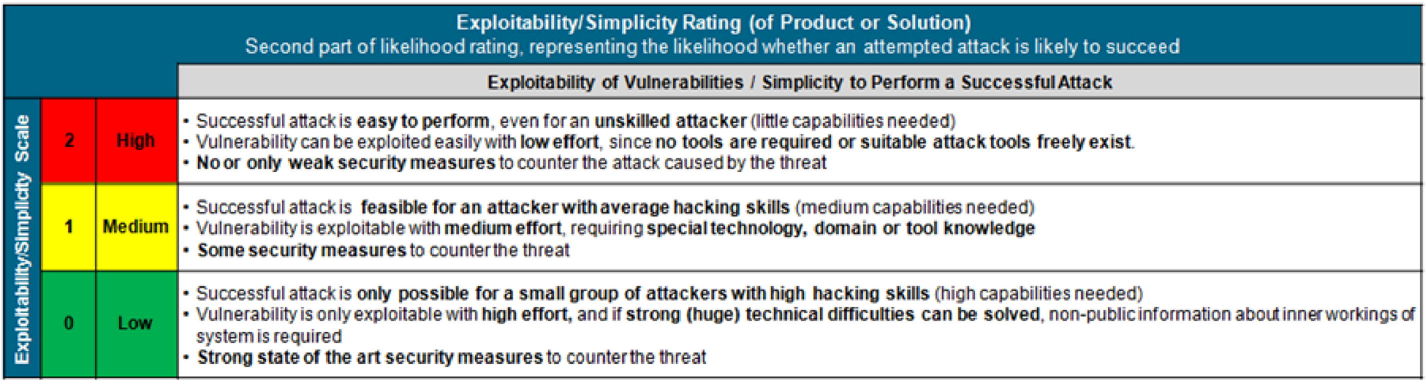
It is possible to detail the indicators in the likelihood scales, but the TRA work team does not see the need, and the benefits from using of the same likelihood rating scheme across Siemens should not be compromised without good reason. If a Company / Business Unit considers changes necessary, the TRA work team should check, and decide whether the likelihood rating scheme in the TRA tool should be updated.

The likelihood rating is derived from these two factors through a mapping table, shown in Figure 2-4. Again, the recommendation is not to change the likelihood mapping table.



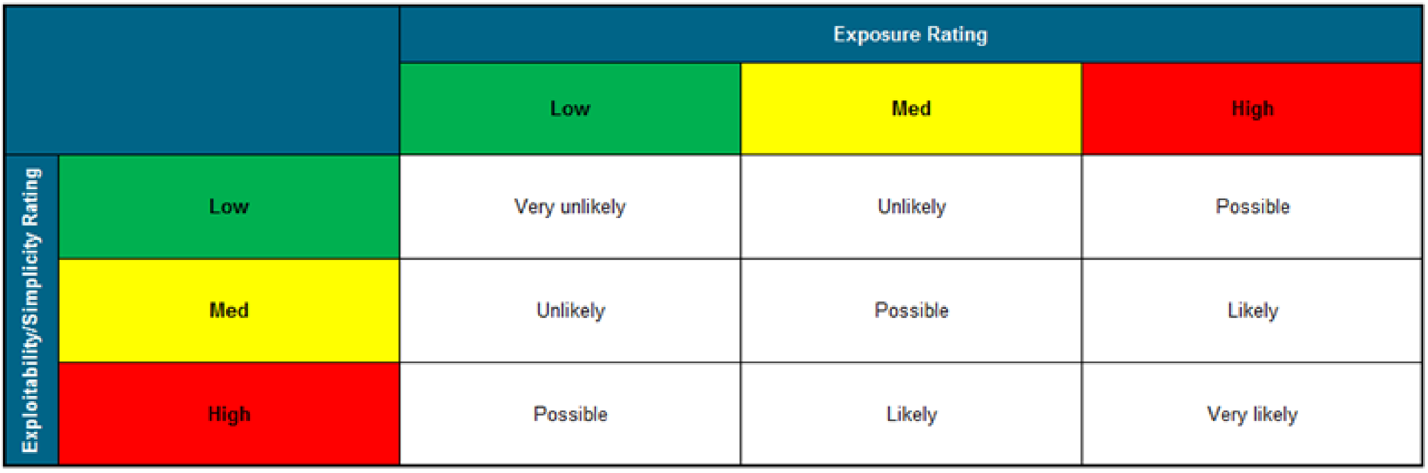
			Exposure Rating (of Product or Solution in Operational Environment) First part of likelihood rating, representing the likelihood whether an attack may be attempted	
			Exposure Categories	
			Level of Access Needed	Risk of Getting Caught
Exposure Scale	2	High	• **Easy logical or physical access** for attacker, e.g. – internet access sufficient, or – public physical access, or – attacker has access as part of daily work, operation, or maintenance activities, or – product or components can be acquired by attacker with low effort	• **Low risk** to be discovered / convicted • No or little measures for unauthorized access detection and investigation implemented
	1	Medium	• **Restricted logical or physical access** for attacker, e.g. – internal network access required, or – restricted physical access, or – product or components can be acquired by attacker with medium effort	• **Medium risk** to be discovered / convicted • Some measures for unauthorized access detection and investigation implemented (e.g. surveillance, logging, monitoring)
	0	Low	• **Highly restricted logical or physical access** for attacker, e.g. – highly restricted network and physical access, or – product or components can not be acquired by attacker or only with high effort	• **High risk** of being discovered / convicted • Good measures for unauthorized access detection and investigation implemented (e.g. surveillance, protected log files, monitoring and alarming, limited no. of persons)

Figure 2-2 Default exposure rating of the TRA method



			Exploitability/Simplicity Rating (of Product or Solution) Second part of likelihood rating, representing the likelihood whether an attempted attack is likely to succeed
			Exploitability of Vulnerabilities / Simplicity to Perform a Successful Attack
Exploitability/Simplicity Scale	2	High	• Successful attack is **easy to perform**, even for an **unskilled attacker** (little capabilities needed) • Vulnerability can be exploited easily with **low effort**, since **no tools are required or suitable attack tools freely exist**. • **No or only weak security measures** to counter the attack caused by the threat
	1	Medium	• Successful attack is **feasible for an attacker with average hacking skills** (medium capabilities needed) • Vulnerability is exploitable with **medium effort**, requiring **special technology, domain or tool knowledge** • **Some security measures** to counter the threat
	0	Low	• Successful attack is **only possible for a small group of attackers with high hacking skills** (high capabilities needed) • Vulnerability is only exploitable with **high effort,** and if **strong (huge) technical difficulties can be solved**, non-public information about inner workings of system is required • **Strong state of the art security measures** to counter the threat

Figure 2-3 Default exploitability/simplicity rating of the TRA method



		Exposure Rating		
		Low	Med	High
Exploitability/Simplicity Rating	Low	Very unlikely	Unlikely	Possible
	Med	Unlikely	Possible	Likely
	High	Possible	Likely	Very likely

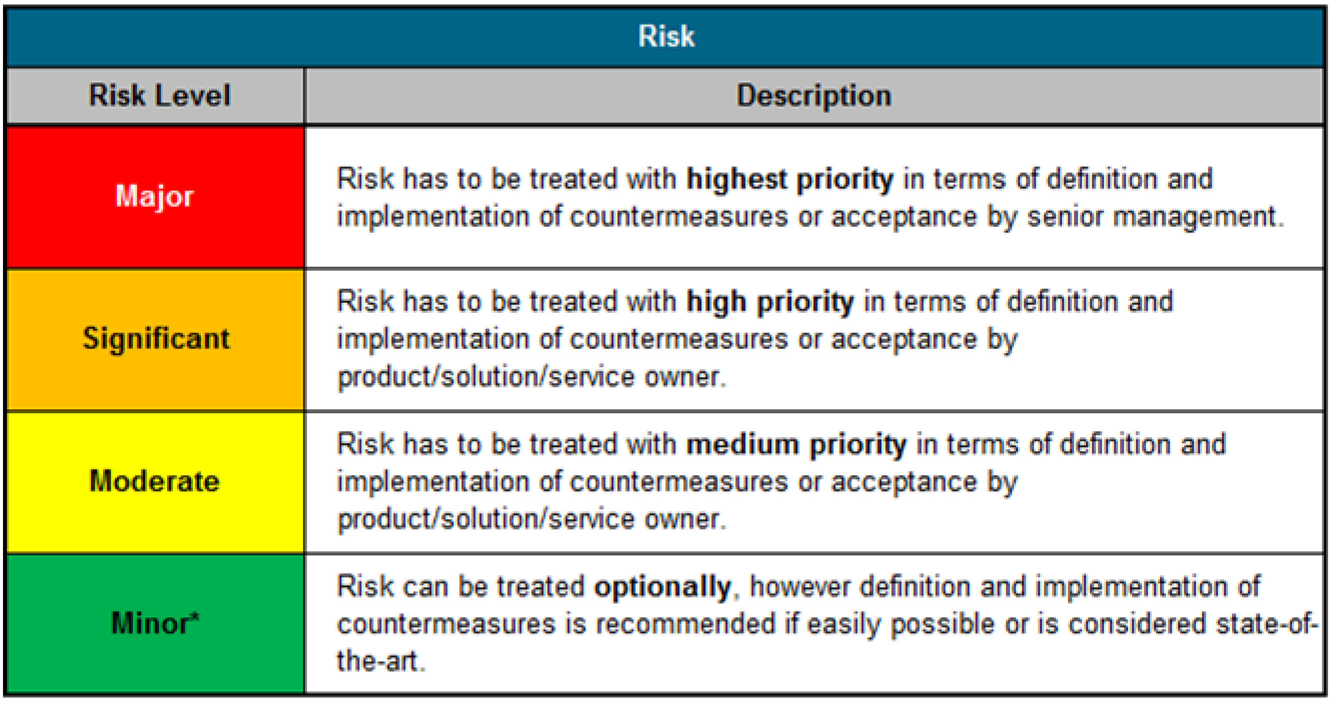
Figure 2-4 Default mapping of exposure and exploitability/simplicity to likelihood

Risk levels, management responsibilities and risk mapping table (Sheet ‚Risk')

The TRA method uses four risk levels, and provides default risk level descriptions (see Figure 2-6) that specify generically the priority with which to treat risks in the different risk levels. For example the description implies that a major risk has to be treated with highest priority or accepted by senior management

It is strongly recommended to adapt the definition of priorities to the needs of a Company / Business Unit, and also to link the different risk levels to management responsibilities.Typically a Company / Business Unit will have some priority scheme for requirements or change requests, and this could be a good starting point.

In the TRA tool, the risk levels can be found in the sheet 'Risk'.

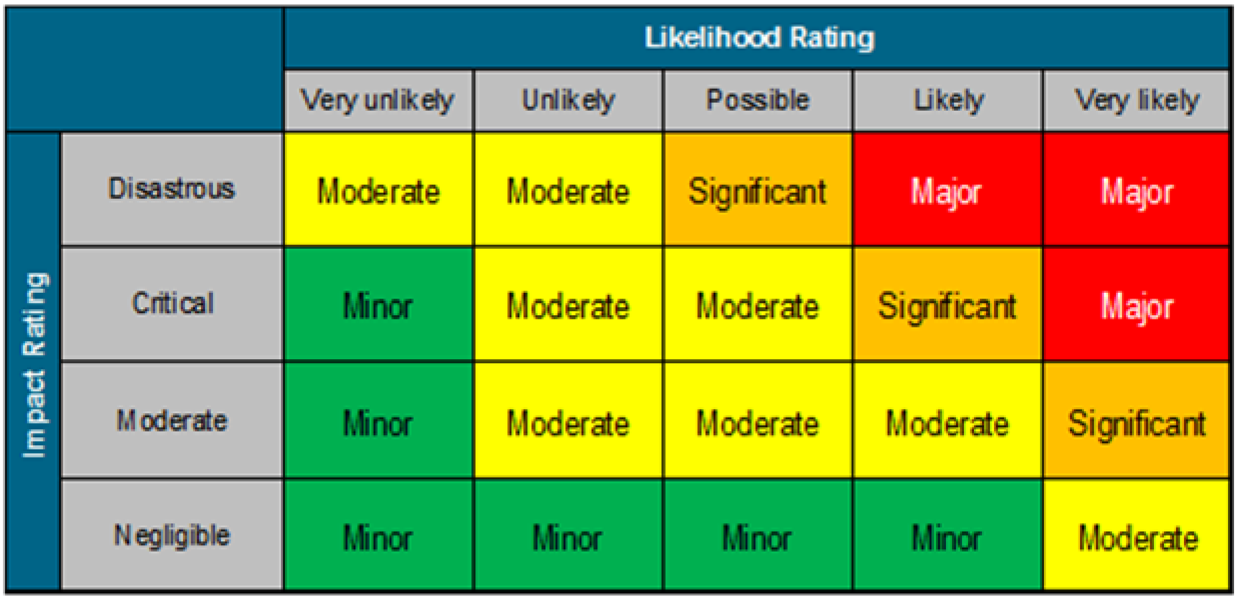


Risk	
Risk Level	Description
Major	Risk has to be treated with **highest priority** in terms of definition and implementation of countermeasures or acceptance by senior management.
Significant	Risk has to be treated with **high priority** in terms of definition and implementation of countermeasures or acceptance by product/solution/service owner.
Moderate	Risk has to be treated with **medium priority** in terms of definition and implementation of countermeasures or acceptance by product/solution/service owner.
Minor*	Risk can be treated **optionally**, however definition and implementation of countermeasures is recommended if easily possible or is considered state-of-the-art.

Figure 2-5 Default risk levels description of the TRA method

In the TRA, the identified threats are assigned a risk level through the mapping of likelihood rating and impact rating according to the risk rating mapping table. The default risk rating mapping table is shown in Figure 2-6. The risk mapping table can be adapted by the Company / Business Unit. For example the combination Critical / Very unlikely could be mapped to risk level Moderate instead of Minor, or the combination Moderate / Unlikely could be mapped to risk level Minor.

Like the other parameters of PSS risk management, the risk rating mapping table has to decided by management as part of the PSS strategy of a Company / Business Unit. Any changes of the default mapping table should be carefully considered.



		Likelihood Rating				
		Very unlikely	Unlikely	Possible	Likely	Very likely
Impact Rating	Disastrous	Moderate	Moderate	Significant	Major	Major
	Critical	Minor	Moderate	Moderate	Significant	Major
	Moderate	Minor	Moderate	Moderate	Moderate	Significant
	Negligible	Minor	Minor	Minor	Minor	Moderate

Figure 2-6 Risk rating mapping table

Specifying options for risk treatment

To perform a PSS TRA (workshop) is only one step of PSS risk management. After identifying threats and evaluating the level of resulting risks, the next step is risk treatment, in particular to determine measures against the threats so that the level of risks decreases. The overall goal is that after risk treatment there are no risks with high rating (e.g. Major or Significant).

The risk treatment options are listed in the PSS Guide requirement RM3. In a Company / Business Unit, the risk treatment options could be further specified. In particular, a detailed guideline on when customers should take over responsibility for risk mitigation should be provided.

The implementation of risk mitigation measures in the project has to be tracked, so that before the release, there is a clear picture which mitigation measures have been implemented. Only then it is clear which residual risks remain high (e.g. Major or Significant) and for which a decision on acceptance of remaining risks is required.

It is recommended to define upfront how treatment tracking and controlling should be done in a Company / Business Unit. Define clearly if the TRA tool has to be used for tracking or not. Alternatively, the tracking mechanisms of the Company / Business Unit for implementation of requirements and for handling change requests or defects can be used to get the state of risk treatment.

Tracking PSS risk mitigation and acceptance in the TRA tool

The TRA tool can be used to track PSS risk mitigation and acceptance, as explained in this section. Using the TRA tool provides a clear link of risk mitigation measures (aka derived requirements) to threats. It might be an option to feed output of the tracking mechanism into the tracking fields of the TRA tool.

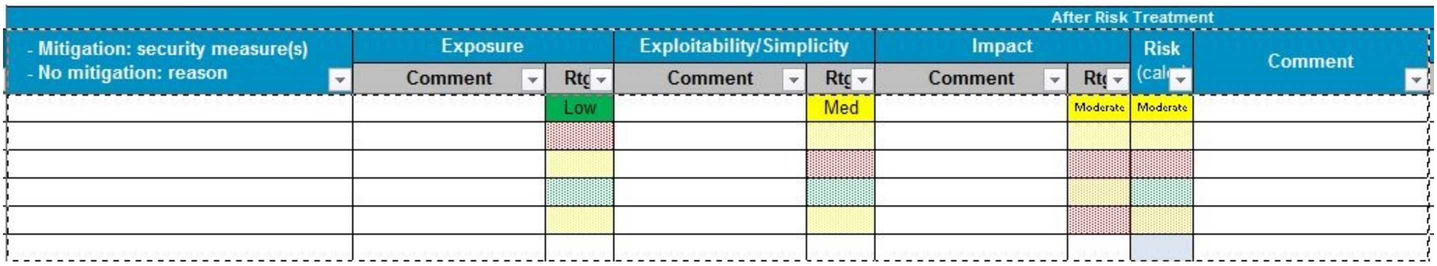
The risk treatment status could be used in milestone checklists, i.e. in the goals for a specific milestone. This could be in the form: "Mitigation measures (aka derived requirements) have been planned / implement / tested for all major and significant risks." For examples, see Recommendations for integrating PSS risk management into processes.

The TRA tools offers the possibility to calculate a risk treatment status on the basis of the following treatment information in order to track the treatment of each risk:

1. The *mitigating measures and the reduced risk level* after implementation of the mitigation measures, as shown in Figure 2-7.
   In the first column ('Mitigation: security measure(s), No mitigation: reason') a reference to the mitigation measure (e.g. ID of requirement or reference to design spec) should be listed. If no mitigation measure is planned for the risk, this also should be documented. For the next columns, the likelihood and impact of the threat after the measures have been implemented should be analyzed. The resulting new risk level is calculated automatically on the basis of the risk mapping table, and displayed in column 'Risk'. Note: the likelihood and impact rating is by default copied from left hand side of the Threat and Risk List sheet, and presented in shaded colors.
   If the chosen risk mitigation measure avoids the risk by removing the attack possibility, e.g. by removing an interface, then for the updated likelihood rating, the option 'Avoided' should be chosen, as shown in Figure 2-8.

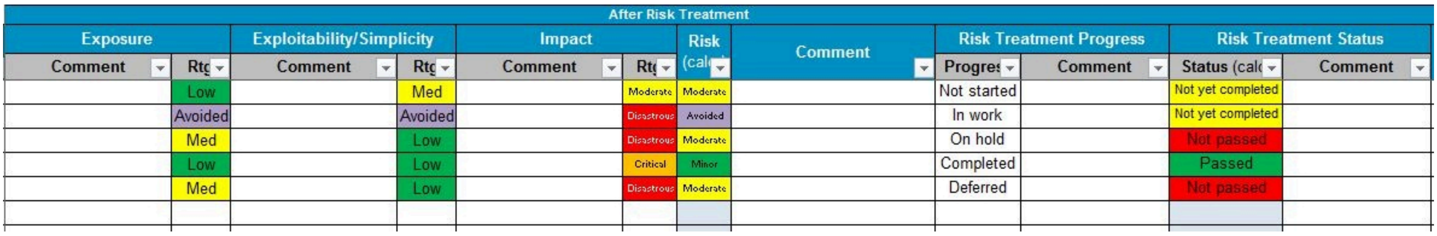
The *progress of implementation* is shown in Figure 2-8. In the column 'Progress', there is a drop-down list of options: 'Not started' / 'In work' / 'On hold' / 'Completed' (includes testing) / 'Deferred' (decision taken to defer the implementation).

2. The *risk treatment status* is displayed in column 'Status', as shown in Figure 2-8.



After Risk Treatment								
- Mitigation: security measure(s) - No mitigation: reason	Exposure		Exploitability/Simplicity		Impact		Risk (cal	Comment
	Comment	Rtg	Comment	Rtg	Comment	Rtg		
		Low		Med		Moderate	Moderate	

Figure 2-7 Documentation of mitigation measures and evaluation of the updated risk level in the TRA tool



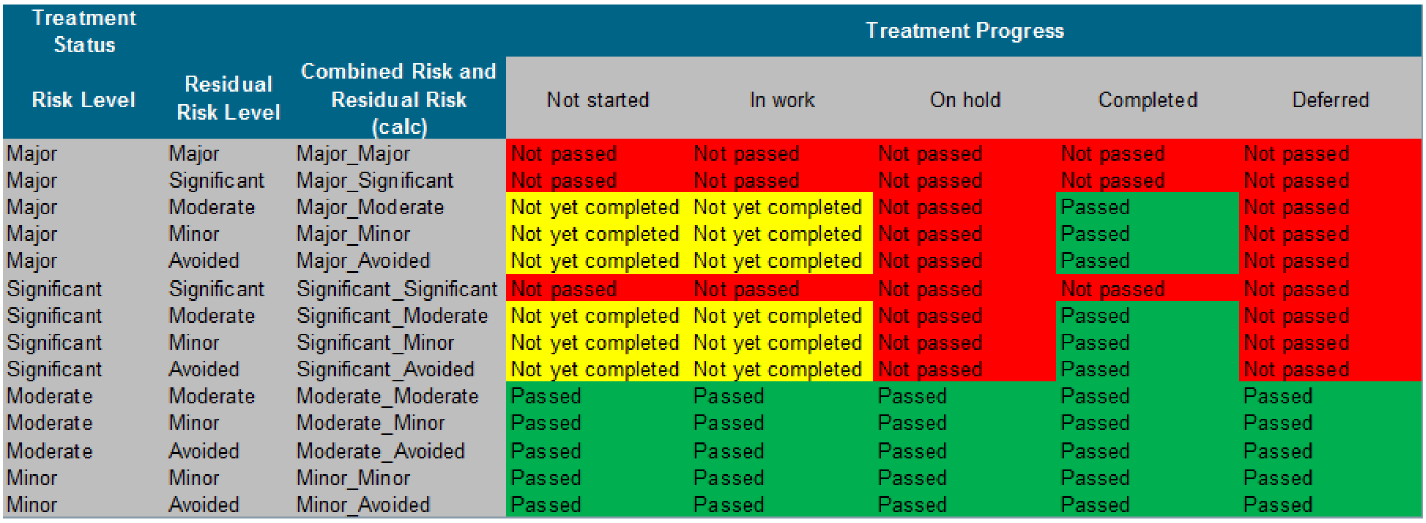
After Risk Treatment												
Exposure		Exploitability/Simplicity		Impact		Risk (cal	Comment	Risk Treatment Progress		Risk Treatment Status	
Comment	Rtg	Comment	Rtg	Comment	Rt			Progres	Comment	Status (calc	Comment
	Low		Med		Moderate	Moderate		Not started		Not yet completed	
	Avoided		Avoided		Disastrous	Avoided		In work		Not yet completed	
	Med		Low		Disastrous	Moderate		On hold		Not passed	
	Low		Low		Critical	Minor		Completed		Passed	
	Med		Low		Disastrous	Moderate		Deferred		Not passed	

Figure 2-8 Calculation of risk treatment status in the TRA tool

The risk treatment status is calculated according to a mapping table. The default mapping is shown in Figure 2-9. The factors that determine the risk treatment status are: The risk level that was determined in the TRA workshop, the risk level after implementation of mitigation measures and the treatment status. The status can take the following values: Passed / Not yet completed / Not passed.

The mapping table can be adjusted for the Company / Business Unit.

⚠ Note that the mapping table has to be consistent with the definition of risk levels: If it has been decided that major and significant risks have to be treated, then the mapping table has to map threats with a rating 'Major' for which the mitigation measures have not been completed to the status 'Not passed'.



Treatment Status			Treatment Progress				
Risk Level	Residual Risk Level	Combined Risk and Residual Risk (calc)	Not started	In work	On hold	Completed	Deferred
Major	Major	Major_Major	Not passed	Not passed	Not passed	Not passed	Not passed
Major	Significant	Major_Significant	Not passed	Not passed	Not passed	Not passed	Not passed
Major	Moderate	Major_Moderate	Not yet completed	Not yet completed	Not passed	Passed	Not passed
Major	Minor	Major_Minor	Not yet completed	Not yet completed	Not passed	Passed	Not passed
Major	Avoided	Major_Avoided	Not yet completed	Not yet completed	Not passed	Passed	Not passed
Significant	Significant	Significant_Significant	Not passed	Not passed	Not passed	Not passed	Not passed
Significant	Moderate	Significant_Moderate	Not yet completed	Not yet completed	Not passed	Passed	Not passed
Significant	Minor	Significant_Minor	Not yet completed	Not yet completed	Not passed	Passed	Not passed
Significant	Avoided	Significant_Avoided	Not yet completed	Not yet completed	Not passed	Passed	Not passed
Moderate	Moderate	Moderate_Moderate	Passed	Passed	Passed	Passed	Passed
Moderate	Minor	Moderate_Minor	Passed	Passed	Passed	Passed	Passed
Moderate	Avoided	Moderate_Avoided	Passed	Passed	Passed	Passed	Passed
Minor	Minor	Minor_Minor	Passed	Passed	Passed	Passed	Passed
Minor	Avoided	Minor_Avoided	Passed	Passed	Passed	Passed	Passed

Figure 2-9 Table for calculation for the risk treatment status

Define which methodology is applied

The TRA method offers variants on how to perform the method steps, and in the TRA method description, two main approaches are described in the TRA method description see Specifying impacts.

After an analysis, Company / Business Unit should decide which variant is to be used. In line with this decision, TRA tool needs to be configured. The respective tool configurations are also described in the TRA method description see Specifying impacts.

Interrelation with other risk management processes

Risk management in the project of a Company / Business Unit has to cover many topics, including safety, technical risk management and project risk management. Product and solution security is another topic, and hence the relation of PSS risk management with other risk management processes has to be clarified.

For example, the FMEA (Failure mode and effect analysis) method is used within Siemens to identify and analyze safety risks. ACP (Asset Classification + Protection) provides a framework for management of security risks. In particular, the security risks that derive from potential attacks on Siemens data and Siemens infrastructure are handled according to the ACP process. For IT-applications running in the Siemens Intranet that are products and handle Siemens and customer data, PSS risk management and risk management for Siemens data and Siemens infrastructure has to be coordinated.

The natural way of establishing PSS risk management will need adaptations in existing PLM processes and/or PM@Siemens processes and/or Engineering processes. Doing so it has to be decided whether an alignment with other implemented risk management processes is appropriate (for example alignment of communication and reporting paths).

Relation with other risk management processes have been discussed in the TRA piloting workshops, and some observations are listed and briefly explained:

- *Safety risk management*
  With respect to safety risk management, handling of safety risks is in most cases managed according to regulations, e.g. FDA regulations or IEC EN 61508. The causes and the countermeasures differ for safety and PSS risks, so there is no need to integrate the two processes. Note: this does not mean that safety impacts are ignored in PSS risk management – safety is one of the impact categories in the impact rating scheme of PSS TRA (see Figure 2-1).
- *Technical risk management*
  In technical risk management, typically a broad variety of potential problems is considered. While security weaknesses could be discovered in a technical risk analysis, experience shows that a focused PSS TRA workshop is required to systematically find security weaknesses and get a good overview of security risks. However, the impacts considered in PSS TRA should be aligned with the impacts considered in a technical risk analysis, e.g. for impacts concerning the non-availability of the system in operation at the customer site.

Week: 17   Month: 33   Year: 301
Detailed page statistics

Page created 9 years and 99 days ago.
Page last edited 3 years and 214 days ago.

1 Comment

Jiří Machacek

Specifying impacts link does not seem to work.