Appendix: Mapping to ISO/IEC 27005 information security risk management

Risk Management in general ensures coordinated activities are in place to direct and control an organization in regard to risk assessment and treatment. The maturity of, and the degree to which Risk Management is implemented in an organization (across sectors or Companies / Business Units) may vary significantly.

To present the main activities of Risk Management and its relationship to TRA, we refer to the following generic Risk Management process steps specified in "ISO/IEC 27005 - Information security risk management" (Please refer to the ISO/IEC 27005 or other risk management standards for more detailed information).

Context Establishment

For each product, solution or service the first process step of Risk Management is *Context Establishment*, which is intended to enable the organization with methods, tools and metrics to be used for the Threat and Risk Analysis.

For PSS Risk Management as defined in the PSS Guide, this corresponds to the step RM1: Establish a PSS risk analysis and treatment approach as part of a PSS risk management strategy.

Risk Assessment

Risk assessment is the process step required to identify, analyze and evaluate threats and risks. For this purpose adequate methods should be applied.

This step corresponds to RM2: Perform threat and risk analysis (TRA).

Risk Treatment

Risk Treatment is the activity of selecting and implementing countermeasures to modify the risk (rating).

Risks can be treated in various ways such as:

- Avoidance (eliminate, withdraw from or not become involved)
- Transferring (outsource or insure a risk)
- Retaining risk (accept and allocate budget)
- Mitigating / reducing risks (selection of adequate countermeasures)

Risk mitigation measures / countermeasures should be selected by taking particularly a cost-benefit analysis into account, to evaluate the ratio between the cost(s) for implementing countermeasure(s) and their effectiveness with regard to risk reduction. It is the goal that a risk can be reduced to an acceptable level by selecting adequate countermeasure(s). Risk mitigation measures can be technical, physical and organizational or combinations of them.

This step corresponds to RM3: Plan and track PSS risk treatment

Risk Acceptance

Risk acceptance is the process step to accept risks after risk treatment. There are different levels of risks and thresholds, with a desired target level of risk.

Typically the acceptance of risks (of a certain risk level) is related to the organization or project hierarchy. The decision if a risk can be accepted shall take into account the risk rating and the risk circumstances. E.g. risks that could result in noncompliance with regulations or laws may not be accepted, while acceptance even of high risks may be allowed e.g. if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period or the effort to mitigate the risk exceeds the potential impact by far.

This step corresponds to the final step of RM3: Plan and track PSS risk treatment.

Risk Communication and Consultation

Risk communication and consultation is a continuous activity to achieve agreement on how to manage risks by exchanging and/or sharing information about risk between the decision-makers and other stakeholders.

It is intended to address various aspects such as:

- Integrate results of the TRA in the organization's risk management
- Collect risk information
- Share the results from the risk assessment and present the risk treatment plan
- Support decision-making
- Give decision makers and stakeholders a sense of responsibility about risks
- Improve awareness

Risk Monitoring and Review

Risks and their associated threats and ratings (i.e. likelihood, impacts, risk levels, vulnerabilities) shall be monitored and reviewed on a regular basis or in case of major changes. The goal is to identify any changes with respect to the product, solution or service and the related threats and risks. The continuous risk monitoring and review process step ensures that identified in former threat and risk analyses are regularly checked and revised, if necessary.

Week: 4 Month: 9 Year: 93
Detailed page statistics

Page created 9 years and 99 days ago.
Page last edited 3 years and 222 days ago.