

Residual risk

Risk is associated with uncertainty, both in the technology itself and in the usage of technology. One example of an industry that faces risk and uncertainty is the telecommunications industry. In some cases the telecommunications workforce does not have a complete understanding of the risks and uncertainties associated with the hardware or its users. Even after people have informed themselves of potential risks when buying a new handset, changes in technology and information security will occur. In today's technological environment it is challenging for users to consistently be well informed and possess the most up-to-date information regarding the risks associated with their products and services.

Human behaviour is presumably the highest risk factor as it is always possible to deceive people. People often do not use available controls to reduce risks and often store sensitive information in insecure places such as on the Internet. Future events cannot be foreseen and technology develops at a rapid pace. New versions of malicious software and other harmful risks are a constant threat to users of technology. For example, many users of Google openly trust that they are secure when using the services offered by Google, but at the moment, it is uncertain that Google will ever be able to close all of its security holes.

In order to address the risks associated with the use of telecommunication hardware and services, a risk assessment and risk treatment plan must be implemented. Once a risk treatment plan has been made, residual risks need to be determined. Residual risks are those risks which remain present following a risk treatment [3]. This means that the risk assessment has to be updated, taking into account the expected effects of the proposed risk treatment. If the level of residual risk present still does not meet the risk acceptance criteria, a further iteration of risk treatment may be necessary before proceeding to risk acceptance. More information can be found in ISO/IEC 27002, clause 0.3 [1]

As stated, residual risk is the risk that remains after risk treatment [3]. It is often difficult to assess or measure and it differs considering the threats present. It's the risk remaining after you have completed one of the following:

- Accepted the risk
- Avoided the risk
- Transferred the risk
- Reduced the risk

How to “live with” residual risks

It is important that companies, institutions, regulators, inspection authorities, manufacturers, organisations, associations and even individuals regularly assess their risk associated with telecommunications. The results of the risk assessments might even be published on the Internet and sent as text messages to end users.

Telecommunication companies might consider marketing information security in levels of high, medium and low. In case of high level security, features that are prone to risk may be closed or set to a secure default setting, which the user must change in order to accept the risks himself.

Changes and improvements in technology require regular reassessments and updates of knowledge and software to prevent hackers from finding new ways to exploit weaknesses and vulnerabilities and attacking users. Ignorance in regards to information security and risks is dangerous. Regular updates to telecommunication hardware and services are needed, as well as monitoring, anti-virus control, spyware, fines (penalties) and prohibition of technology and software. Ergo, residual risks need to be reviewed and re-assessed on a regular basis. Awareness of the dangers of such risk to financial interests can be vital for the wellbeing of organizations and end users.

When accepting risk after the completion of a risk treatment, it is important to have a solid understanding of the risks and the potential harm said risk may cause the organization or end users. This risk acceptance is especially important in a situation where controls have been selected as future controls or the implementation of controls is postponed, for example as a result of budget restraints or limited resources to address the risk.

The effectiveness of the risk treatment depends on the results of the risk assessment. It is possible that the risk treatment will not immediately lead to an acceptable level of residual risk. In this situation, another iteration of the risk assessment with changed context parameters (e.g. risk assessment, risk acceptance or impact criteria), if necessary, may be required, followed by further risk treatments (see Figure 1, Risk Decision Point 2).

International standard ISO/IEC 27005 clause 10 states, [2]:

“In some cases the level of residual risk may not meet risk acceptance criteria because the criteria being applied do not take into account prevailing circumstances. For example, it might be argued that it is necessary to accept risks because the benefits accompanying the risks are very attractive, or because the cost of risk reduction is too high. Such circumstances indicate that risk acceptance criteria are inadequate and should be revised if possible. However, it is not always possible to revise the risk acceptance criteria in a timely manner. In such cases, decision makers may have to accept risks that do not meet normal acceptance criteria. If this is necessary, the decision maker should explicitly comment on the risks and include a justification for the decision to override normal risk acceptance criteria.”

Other aspects of residual risks

Our environment is constantly changing, security holes are found and risks must be analysed and evaluated (assessed) on a regular basis. There is no such thing as 100% security; it will always be a question of maximum achievable security.

Information security resources are limited for most people, companies and institutions. Limited resources must be taken into account when planning risks treatment, for example the associated cost factors of the treatment.

In Figure 1 it is depicted how risk can be lowered to a feasible residual risk with optimum control [4]. Four bars are shown that represent four different examples of risks that are being mitigated by security controls. The bars demonstrate the overall security risk. The part of the risk which is marked with A has been met with controls which have already been implemented. A residual risk that still exists is split into B and C, where B is the portion of the residual risk that can be mitigated by more or better controls, C demonstrates the minimum residual risk which cannot be mitigated further and will remain. In the two upper bars, residual risk exists which can be reduced even further with additional controls or improved functionality of already implemented controls.



$A+B+C$ = Overall security risk

A = Security risk which has been mitigated by implemented controls

B = Residual risk which can be mitigated by additional implementation of controls

C = Residual risk that cannot be mitigated by controls

Figure 1 – Risk control used to lower residual risk

Residual risk can also be explained with a three dimensional matrix. Risk is calculated as the multiple of asset value, threat impact, and vulnerability of asset facing a threat. After countermeasures are taken by implementing security controls, there is still residual risk remaining.

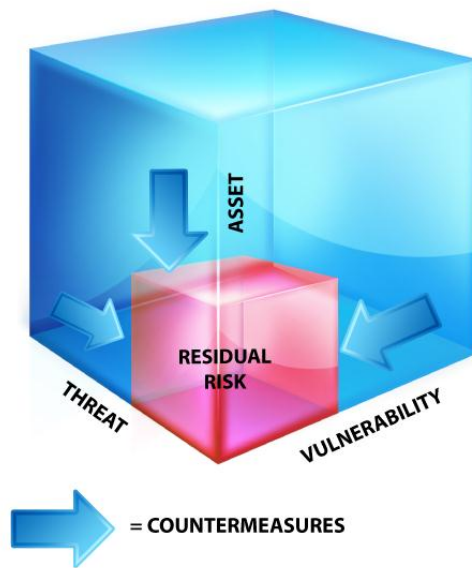


Figure 2 – Residual risk depicted in a three dimensional way

Residual risk can be calculated as any other risk to an asset. One method is to base the risk calculations on the following evaluations:

- The value of the asset
- The probability of a specific threat
- The vulnerability of the asset
- The impact of the threat

The risk can be evaluated by the user regarding these four variables through a simple multiplication or a four dimensional matrix. Sometimes the probability of risk is inserted into impact of threat for simplicity reasons.

In figure 2 the residual risk is depicted in a three dimensional way [5]. It is the multiple of asset value, threat impact, and vulnerability of asset facing a threat. The probability is considered in the threat impact value.

After countermeasures are taken by implementing security controls, there is still residual risk present.

RM Studio, a dynamic risk management tool developed by Stiki, offers users a platform for calculating, assessing and monitoring risks, as well as implementation for further risk reduction (Bars A and B in figure 1). The RM Studio solution provides users with an overview of the risks involved in a given project and helps identify the remaining residual risk present. For more information on RM Studio, please visit www.riskmanagementstudio.com.

Residual risk will always be present within an organization. However, the utilization of a risk management tool, such as RM Studio, offers those responsible for risk management a solution to monitor and reduce residual risk.

Svana Helen Björnsdóttir
CEO of Stiki – developer of RM Studio®

References

- [1] ISO/IEC 27002, clause 0.3
- [2] International standard ISO/IEC 27005; Information technology-Security techniques- Information security risk management, Reference number ISO/IEC 27005:2008(E)
- [3] ISO/IEC 27001:2005, clause 3.9
- [4] <http://www.dnb.nl/openboek/extern/id/en/all/41-117819.html>
- [5] <http://www.scribd.com/doc/49886138/A-Qualitative-Risk-Analysis-And-Management-Tool-Cramm>