Risk Reduction Overview

Manual

Authors	Hellen Havinga and Olivier Sessink
Date	September 7 2014
Version	1.0
Website	This manual can be found at: rro.sourceforge.net

Inhoudsopgave

1. Risk Reduction Overview in short

Risk management is balancing risks and measures. The "Risk Reduction Overview" (RRO) [1] is a visualization method to give insight in the coherence between risk's, measures and residual risk's.

The risk reduction overview consists of two parts: a flowchart with all initial risks, measures, residual risks, and ultimately the final residual risks that have to be accepted, and an appendix with a detailed description of these risks and measures.

The RRO methodology is designed to support business management making decisions about complex security issues in ICT. The methodology can support important decisions on complex issues.

Most ICT designs focus on the security measures taken, but do not give insight in the coherence between measures and the residual risks of the design. When you read the design document it is hard to imagine the residual risks that are still there when the design is implemented and hard to decide if these residual risks are acceptable for business. When the designer uses a RRO to clarify his design, he makes life easier for college's and managers to comprehend the design and tot decide about it.

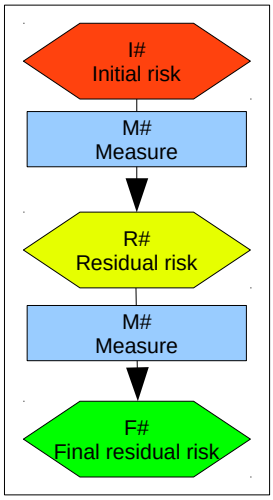

Figure 1: basic elements of RRO

The risk reduction overview is a flowchart. The flowchart starts with all the initial risks that are identified for the particular design of the existing implementation. All initial risks are followed by one or more measures. The initial risks are reduced to residual risks, which are followed by more measures, and finally end with a final residual risk. Arrows depict the flow.

The flow is not necessarily linear: multiple measures from different flows may lead to the same residual risk, and multiple residual risks may follow a single measure. Arrows are drawn from risk to the resulting residual risk. When the measure itself introduces a new risk (the security measure “patching” may result, for instance, in loss of functionality) an arrow can be drawn from that measure to a new risk.

The final residual risk describes the chance and impact that this risk occurs when all measures are taken. The business owner should decide if this final residual risk is acceptable for business: the acceptable residual risk. When the final residual risk is too high, additional measures must be taken.

By presenting the interconnection between risks, measures and residual risks, a RRO gives a simple overview of complex security problems, which is comprehensible for reviewers, auditors, managers and business owners.

The simple drawing method gives a direct view of the initial risks that are taken into account in the design. It gives an overview of the consecutive measures that are taken to reduce the risks and finally, the final residual risks that are still there after taking all the measures. The effects of both procedural and technical measures, and both preventive and reactive measures can be brought together in the same overview. Together they reduce the risks.

The RRO gives no guarantee the design is safe. It simply tells what measures are taken and makes it easier to comprehend what risks were taken into account and what residual risks have to be accepted.

The RRO gives an overview, helps to guide discussions and stimulates the careful choices between different measures. Therefore the use of RRO leads to transparent and traceable decision making.

2. Who can use a RRO for what?

1) A **security designer** is forced to rethink his design decisions when drawing a RRO. He is forced to rethink the initial risks, why certain measures are taken, and what their actual effect is on the initial risk. Furthermore, a designer is forced to write down the residual risk, after all measures are taken. The RRO gives an overview of the layered defense and the diversity in defense that is employed. It helps the designer to divide the measures in to preventive measures and reactive measures.

2) A **security designer** can optimize his design by using the RRO. Double measures or measures that do not reduce risks any further, are easily discovered. The order in which measures are taken, may also affect the cost of the design. If a low-cost measure is the first line of defense and already takes away a lot of the initial risks, the next lines of defense might be simpler in design and cost less.

3) A **reviewer** of a RRO gets a direct overview of the initial risks that are taken in to account in the design of the system. If a particular risk is not in the list of initial risks, it is an indication that the creator of the system has not identified that risk, so the system might not be secure.

4) A **reviewer** can evaluate every security measure, whether he agrees with the effect of the measure on the initial risk: the residual risk. If the residual risk is much higher in reality, than this is an implication that the effectiveness of the measure is overestimated. Again, this may be an indication that the system is not secure.

5) The **business owner** gets an overview of the initial risks, the measures taken, and most importantly the final residual risks to accept for his system. When the business owner decides that the final residual risks are too high for his business, the design must be the adjusted and it is probably necessary to take more or different measures. By letting a number of experts evaluating the RRO, the business owner can receive a quick assessment of the quality of the RRO and of the quality of the underlying design.

6) Risks change in time. New vulnerabilities occur and the chance that vulnerabilities are actually used to hack into a system, also changes in time. By adjusting the risks (and vulnerabilities) in the RRO, the **security designer** can estimate the impact of the changes on the final residual risk. The **business owner** needs to re-decide about the acceptance of the new residual risks.

7) A **security designer** can use an existing RRO as source of inspiration for the design of a new or similar system. A **reviewer** can use an existing RRO to compare the assumptions and security measures of different systems.

3. Risk reduction overview explained

A RRO consists of two parts: a flowchart and an appendix. The flowchart provides insight in the coherence between all risks, measures and final (residual) risks. The position of the measure and its relation to other measures in the flow, define if a measure strengthens (defense in depth), or supplements (the measure reduces another aspect of the risk) other measures or is independent of any other measure (the measure is taken against a very different risk). The appendix gives the description and details of each risk and each measure.

The flowchart (figure 1) is based on two basic elements: risks and measures. We subdivide risks into 4 types:

1) initial risks;
2) residual risks;
3) final risks; and
4) acceptable risks

Acceptable risks can only be introduced when they are known beforehand.

All security flows in the RRO flowchart follow the same pattern: a stream starts with an initial risk, one or more measures are taken in order to reduce the risk, leading to residual risks. Each flow ends in one or more final (residual) risks. When the acceptable risk is known in advance, it is possible to indicate in the diagram if the final risk is lower or higher than the acceptable risk. The flow is not necessarily linear. Sometimes various measures lead to the same rest risk or one measure leads to multiple different residual risks.

Risks and measures in the RRO all have a unique identifier (the hash stands for a unique number):

I# identifier of an initial risk
R# identifier of a residual risk
M# identifier of a measure
F# identifier of a final risk
A# identifier of an acceptable risk

In the flowchart, each unique identifier is followed by a short description of the risk of the measure. Details and more information (chance, impact) are described in the appendix.

4. Example

Figure 2 illustrates a simplified RRO. It gives an example of what happens when it is allowed to transfer e-mail messages between internet and a confidential network and vice versa. Figure 2 does not describe a real-life design. Real risk reduction overviews often have over ten initial risks and over twenty measures (figure 3). Further examples can be found at rro.sourceforge.net

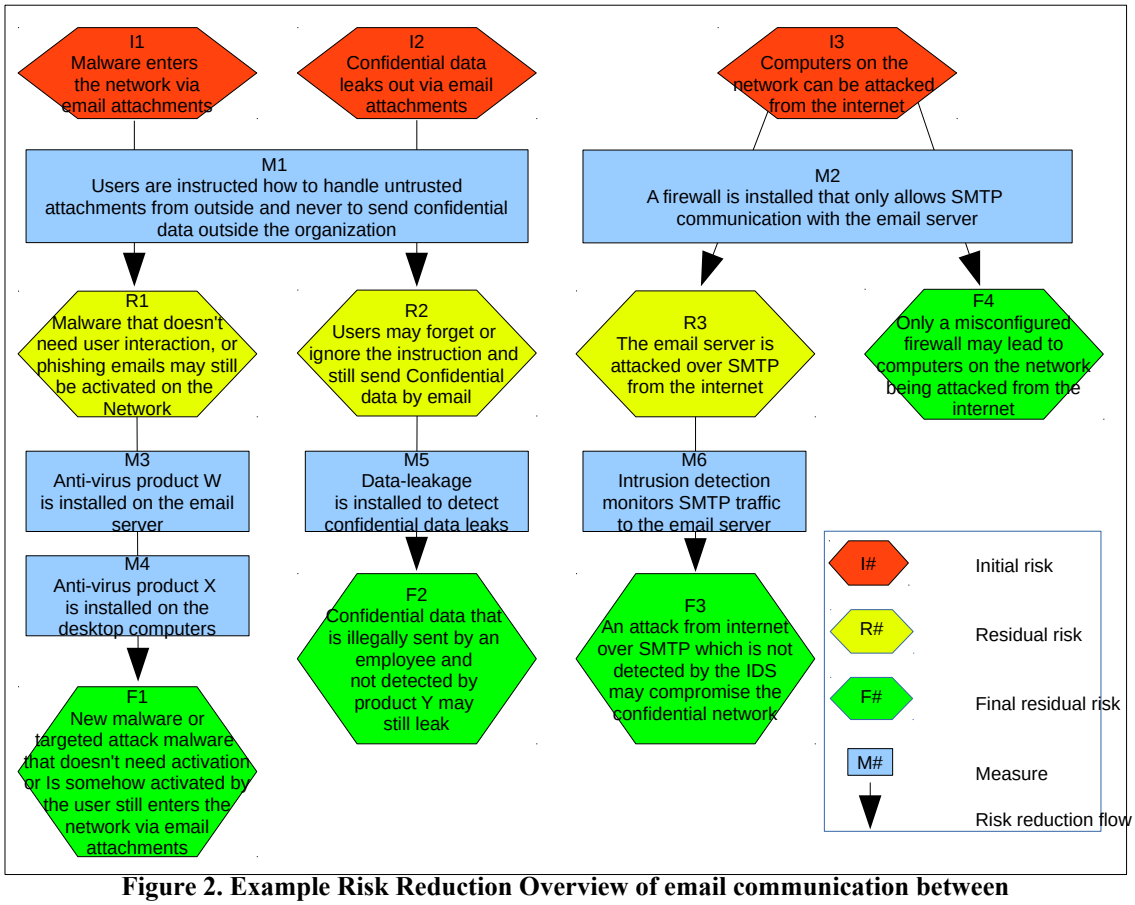

Figure 2. Example Risk Reduction Overview of email communication between a network with confidential data and the internet.

The example in figure 2 shows a change in an existing confidential network. The RRO shows what extra risks are introduced by the change, what measures are being taken and what the final (residual) risks are, after taking the measures.

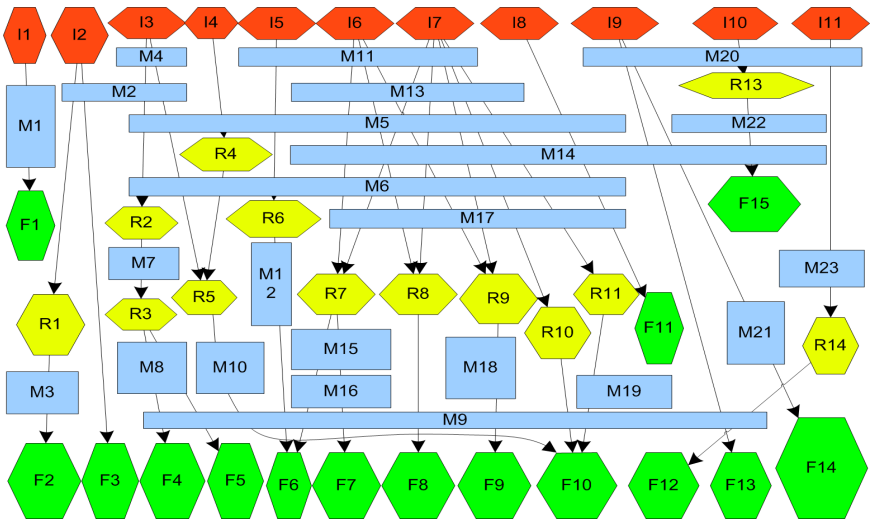

Figure 3: Example of a real RRO (sensitive information is removed)

5. How to make a Risk Reduction Overview

Before making a RRO, an initial set of risks and measures must have been identified already. The initial risks are the risks if one would take no security measures at all. The initial risks can be derived from the threats to the business combined with all possible vulnerabilities in your systems, processes, networks, employees, partners, subcontractors and customers.

STEP 1
The first step is to place all identified initial risks at the top of the flowchart.

Then create a list of the various technical and procedural measures that you have in mind to keep your system secure. Then start to lay out the measures below the initial risks and derive the residual risks from the measures. Complementary measures may be placed below to reduce the residual risks even further. Place preventive measures, that reduce the chance that a threat occurs, above reactive measures, that reduce the damage when the threat actually does occur.

Continue until all measures are positioned and only final residual risks are left.

If two measures provide an identical risk reduction (for defense in depth) they should follow up on each other without residual risk (for instance: measure 3 and 4 in figure 2).

Similar measures and similar risks should be placed near each other, to ease the next steps. The first step often results in a large overview that is hard to understand. There are some techniques to optimize and simplify the flowchart to a more compact overview. Step 2 and 3 give these techniques.

STEP 2
In the second step similar measures are joined together to make the overview more compact and easier to comprehend, as can be seen in figure 4. This step is greatly facilitated if similar measures have been positioned early in the flow during step one, because re-ordering measures changes all the residual risks. Once the generic measures are applied early in the flow, the residual risks become more specific, so eventually all the detail is still present in the overview.

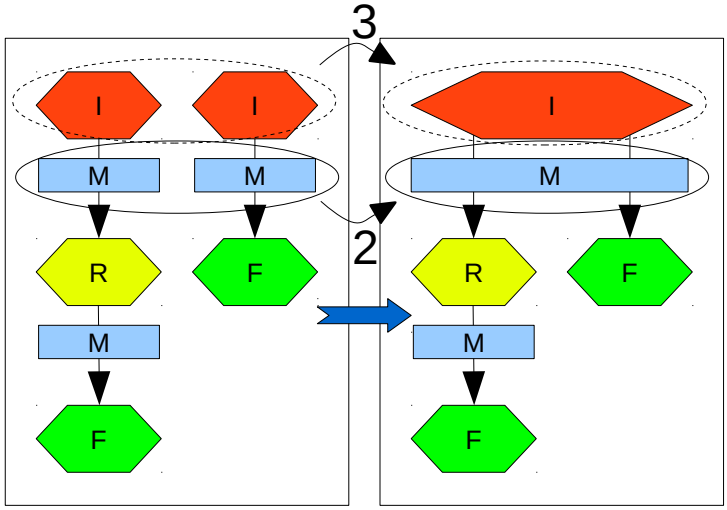

Figure 4: before and after step 2 and 3

STEP 3
In the third step similar risks can be joined together, as can be seen in figure 4. It is often possible to rewrite similar risks into a single more generic description, especially early in the flow. In that case they can be joined together. Lower down in the flow residual risks become very specific and

combining them would result in loss of essential detail.

Sometimes taking a measure itself introduces a new risk (for example: patching introduces possible loss of functionality). These risks should also be drawn in the diagram, by drawing an arrow originating in the measure and ending in the residual risk, the measure introduces.

STEP 4
The last step is to number and describe each risk and measure in the appendix. The appendix has four sections.

1. In the first section all initial risks are described.
2. In the second section all measures are described.
3. In the third section all residual risks are described.
4. The fourth and last section describes all final residual risks.
5. A fifth section can be added to describe the acceptable risk.

The appendix is structured as follows.

To describe a risk:

Risk <identifier>	Title of the risk as it is named in the flowchart
Frequency	Indication of the chance that the threat becomes real.
Impact	Description of the impact, when the risk becomes real. The description should provide a business owner enough information in a clear and comprehensive way to assess if the final residual risk is acceptable. An indication of the cost of possible damage could be added to help the decision maker.

To describe a measure:

Measure <identifier>	Title of the measure as it is named in de flowchart.
Effect	Description of the measure and the effect of the measure. Describe if the measure has effect on the chance of a risk becoming real or on the impact of a risk becoming real. Provide enough detail to the engineers for them to choose the right technical solution.
Implementation	(optional) Description of the (current) implementation.

6. How to review a Risk Reduction Overview

1) Before you review a RRO, you should draw a list of initial risks, you think should be taken into account for the system. Then open the RRO and check if your initial risks are mentioned in the top layer of the drawing. When risks are missing the RRO is incomplete. Give the missing risks as feedback tot the architect. The architect can decide if extra measures need to be taken.

2) Look at all the measures and compare the risks before and after taking the measure. Check if you agree with the measures' risk reducing effect as it is stated in the RRO. Are there extra residual risks not mentioned, or does the measure itself introduce a new risk (for example: a certain measure could introduce a single point of failure)?

3) Look at the final risks. Are they acceptable for business? How do they compare to accepted risks in other systems in your business?

7. Terminology

Threat: the possibility that a vulnerability is used, to endanger the confidentiality, integrity and availability of information.

Risk: the chance that the threat becomes reality and business is damaged in some way.

Measure: The action that reduces the risk by bringing down the chance that the risk occurs or reduce the impact of the risk on business.

Residual risk: the risk that remains after taking a measure or a new risk that occurs after taking a measure.

Final (residual) risk: the ultimate risk after all measures are taken. When the business owner accepts these final risks, they become accepted risks.

Accepted risk: final risk that is accepted by the business owner. No more measures are taken to reduce this risk further.

8. References

[1] H.N.J. Havinga, O.D.T. Sessink, Risk Reduction Overview *Published in:* Availability, Reliability, and Security in Information Systems, Lecture Notes in Computer Science Volume 8708, 2014, pp 239-249 http://dx.doi.org/10.1007/978-3-319-10975-6_18