Risk Reduction Overview for Risk Management

Dr. ir. Olivier D.T. Sessink
Head of section Innovation & Research
Joint IT command, Ministry of Defense


Ministerie van Defensie

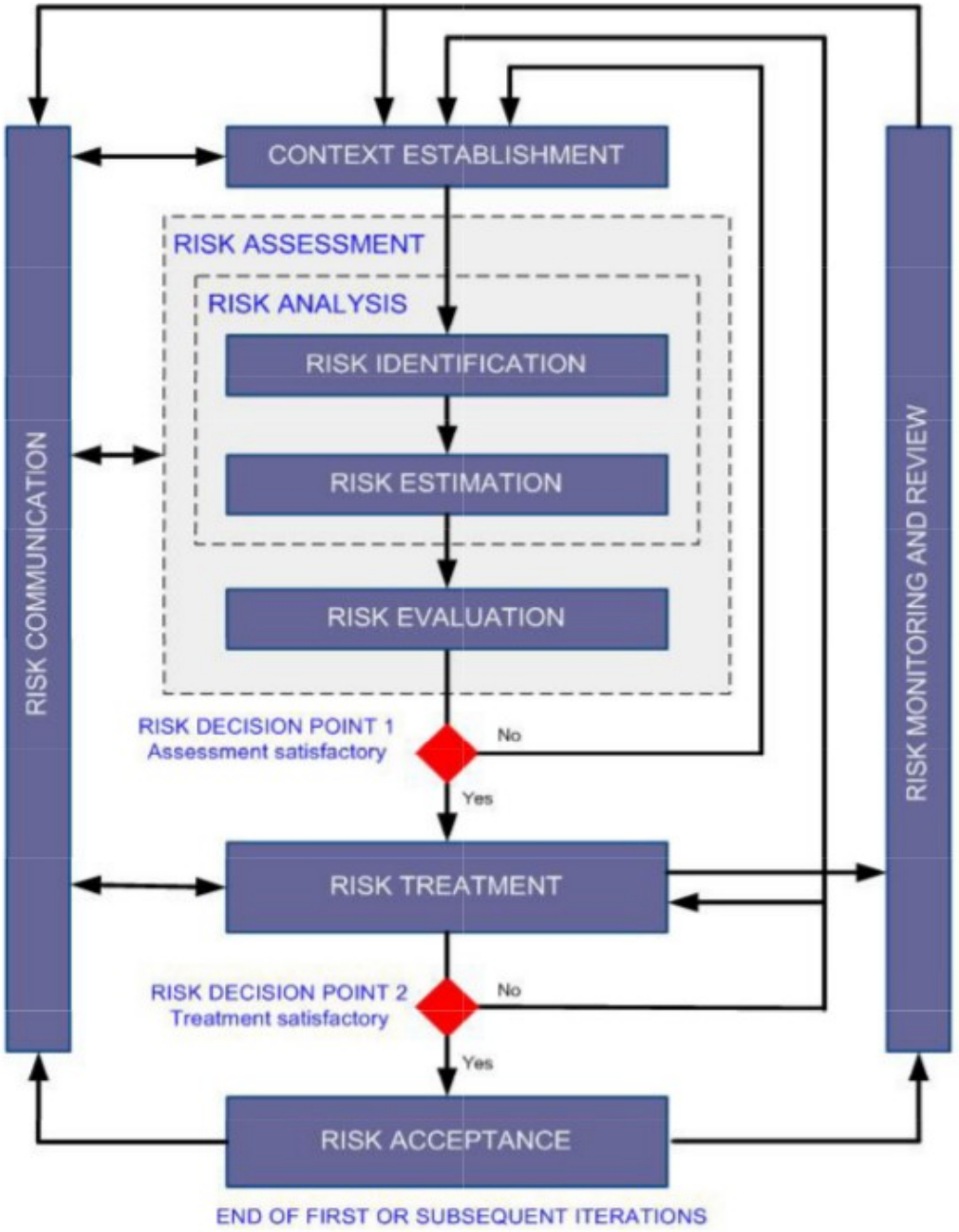
Ir. Hellen N.J. Havinga
Enterprise security architect
Central Information Services, Rijkswaterstaat


Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

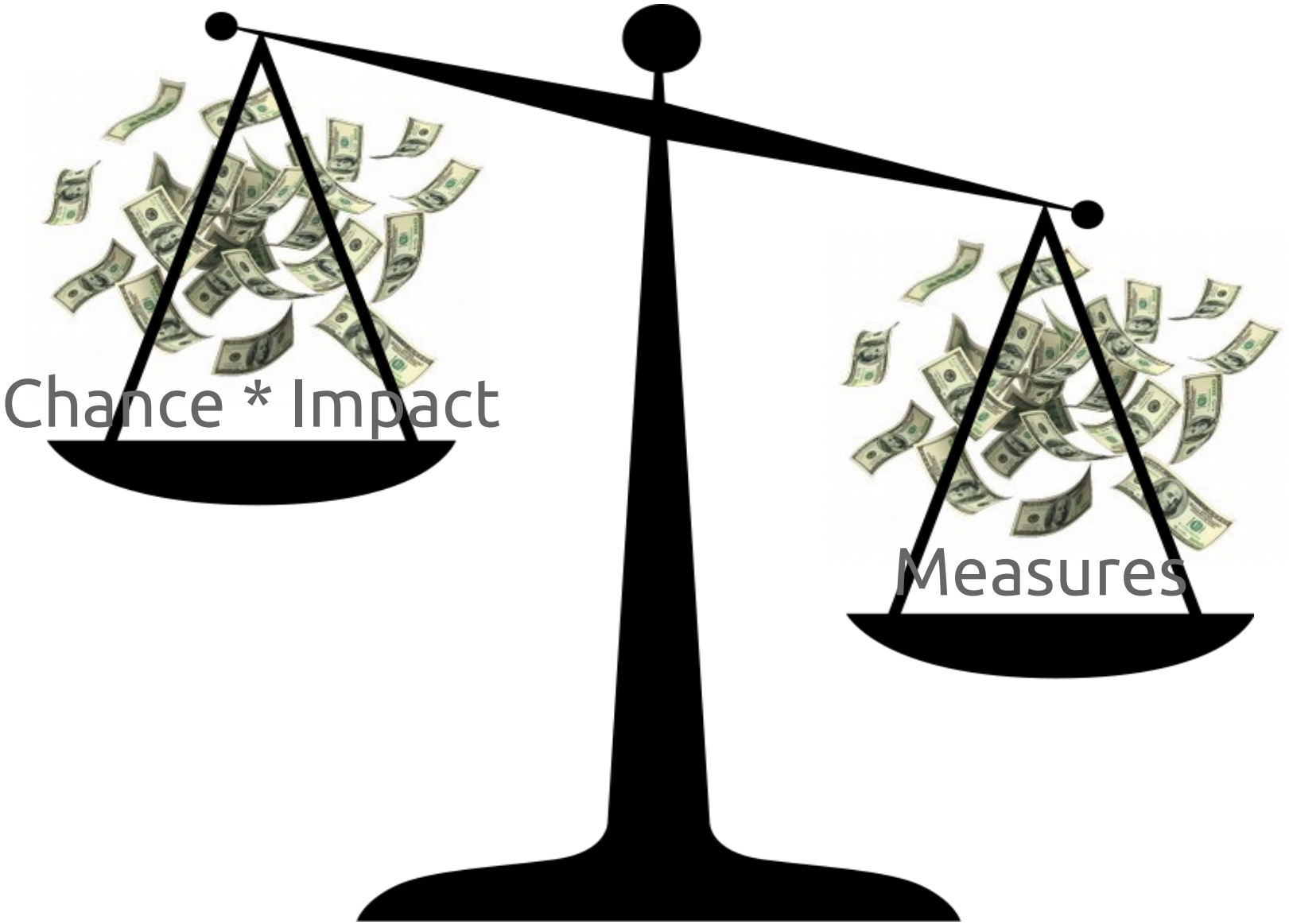
Contents

- Introduction to Risk Management
- IT Risk management challenges
- Objectives
- The Risk Reduction Overview method
- Risk Reduction Overview benefits
- Evaluation

ISO27005 Risk Management



Risk acceptance



Why is risk management hard ?

- Threats and the chance that they might cause damage are unknown external factors

Why is risk management hard ?

- (Known) vulnerabilities change with high rate

Vulnerable? Exploit ? Patch?

- IT changes continuously affecting chance and damage

Why is risk management hard ?

- Cost of damage is hard to estimate

Sensitive information leaked? Business process interupted ?

Loss of trust ? Reputation damage?

Why is risk management hard ?

In **large** organisations the situation is even worse :

- Large number of roles & people involved in risk management
- Large numbers of interconnected systems
- Different requirements from different business units

Risk acceptance in large organizations

Existing methods

Existing methods (such as CRAMM and IRAM) include generic baseline measures.

However : the relation between these baseline measures and the residual risk is not clear

How can we improve the situation ?

Objectives: present an overview such that:

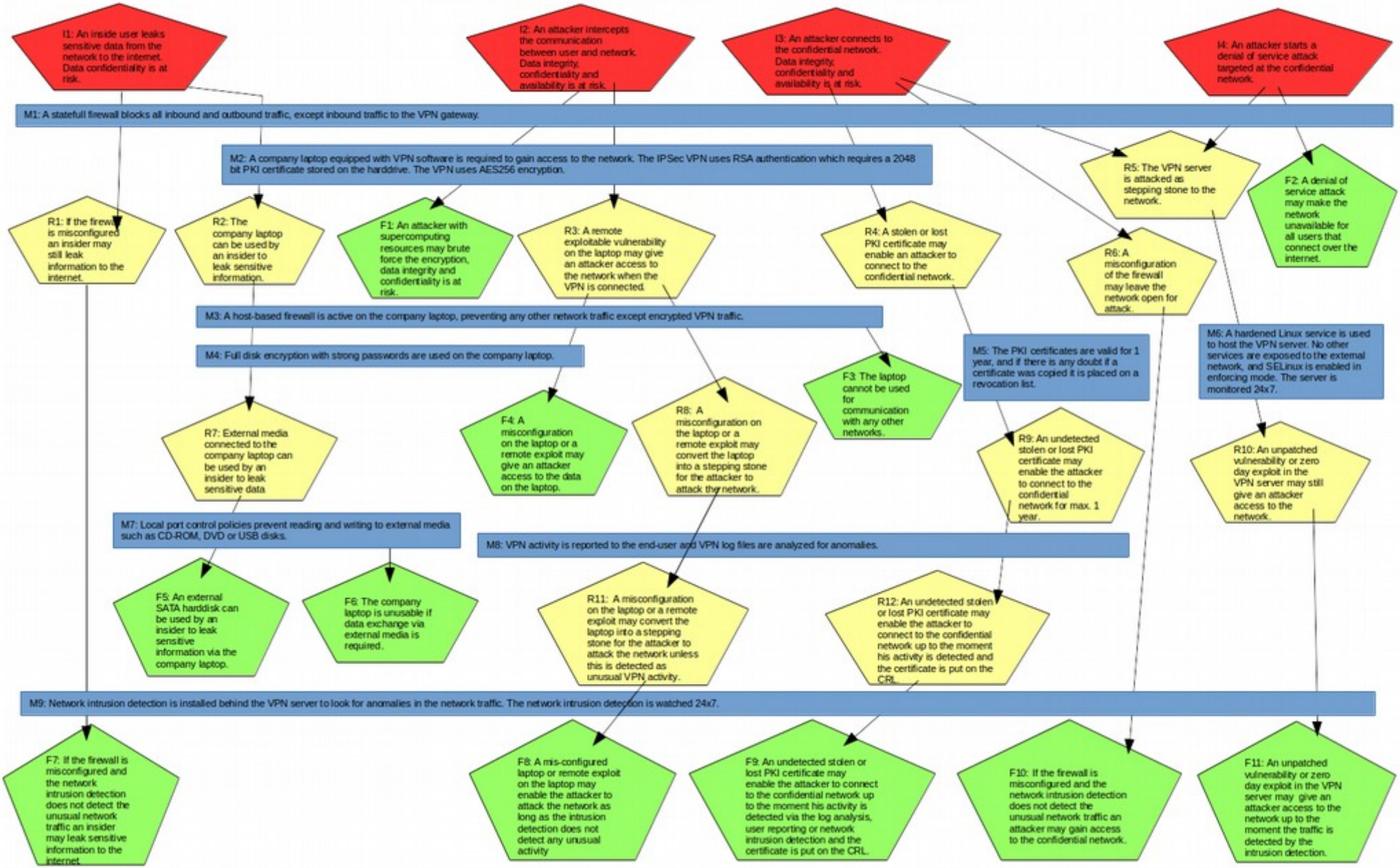
- Residual risks can be evaluated
- The relation between risk, measures and residual risk is clear
- It is useful for people in different roles and with different background
- It is applicable for a design or implemented system

Risk Reduction Overview

Example Risk Reduction Overview:

Giving users access to a network with sensitive data over the internet.

This example is purely hypothetical and does not reflect an existing design.



RRO application and benefits

- Drawing forces to rethink design decisions
- Unneeded measures and effect of the measures is easily identified
- Missing risks are easily identified
- Realism of risk reduction is easily evaluated
- Final residual risks are directly visible
- Impact of changes is easily derived
- Future designs can re-use risk reduction patterns

RRO Evaluation

Several years of use:

- Dutch Ministry of Defence, Joint IT command
  - Information security of military and national sensitive information
- Rijkswaterstaat (national civil infrastructure and waterway agency)
  - Cyber security of vital infrastructure

Evaluation results 1/2

- The RRO has been found to be beneficial in all seven mentioned application areas.
- First time reviewers with different backgrounds find the RRO intuitive and easy to understand
- Reviewers indicate they need less time to review measures and residual risk
- Reviewers indicate the RRO gives far more overview than traditional design documents

Evaluation results 2/2

- Business owners point out that the RRO enables them to discuss measures with IT specialist – something they found very difficult in the past

Which is exactly what ISO 27005 risk management requires

Risk Reduction Overview

Makes **communication** about risks, measures and residual risk possible between people with various different roles and backgrounds.

http://rro.sourceforge.net/

Questions ?