

# Risk Analysis – A Model

By Per Rhein Hansen

The purpose of this paper is to describe a model for analysing the business risks related to the use of IT, which are often called IT-risks.

An IT risk may be described as a possible damage which a company with some likelihood may expect in connection with breaches of confidentiality, integrity or the availability of IT resources (data, systems, network, servers etc.)

## **Terminology:**

- *A **risk** expresses a combination of **the likelihood** of an unwanted occurrence (threat) and the extent of the **consequences** (the losses) of this*
- *A **threat** is an occurrence which potentially may cause (considerable) damage to an organization/company*
- *A well-established **control environment** may minimize the likelihood that threats become real while an environment with weak control and security measures may be characterized as vulnerable which increases the possibility of threats becoming real*
- *A **risk analysis** is a process by which threats are registered and related to the control environment. Thus achieving an assessment of the risks*
- *The **risk assessment** which is a result of the risk analysis may for instance be presented in a "scorecard" with built in priorities*

By doing a risk analysis an attempt is made to identify all risks in order to find out how to manage them. In doing this an identification of the threats against IT resources (data, systems, network) as well as an assessment of the existing control environment must be carried out. Threats may be events, which cause breaches in IT security, which primarily are characterized by terms such as confidentiality, integrity and accessibility. Authentication, accountability and non-deniability are complementary terms.

The process of risk assessment may be described as a systematic method of identifying

1. ***The scope of the assignment** (a business unit, a new system, a service)*
2. ***The assets** to be protected (data, systems in operation, network, servers)*
3. ***Security threatening events**, both the ones which have occurred within recent years as well as those which may occur in the future (taking into consideration the new IT technologies and the use of the new IT in relation to IT strategy)*
4. *The damage which the company will suffer if a threat causes a breach in IT security, as well as the frequency of such a threat*
5. ***The level of threats** as a summary of the observations under item four*
6. ***The control environment (safeguards) and its strength***
7. ***The total risk** with the total level of threat held against the strength/weakness of the control environment assessed on a scale from (1) acceptable – (2) partly acceptable – (3) unacceptable*

In order to reduce the known risks ("risk management") the control environment must be strengthened, or more safeguards must be introduced. Then the risk analysis may be repeated iteratively until a satisfactory (low) level of risk has been obtained.

A risk analysis may be carried out for all interesting areas of a company for instance an organizational unit, a system, a project or a business process – in order to prevent too great risks in connection with development or to reduce risks arisen or discovered in connection with the daily operation.

**The steps of a risk assessment process are:**

**1. *Scoping the assignment***

Specifying which area needs a risk analysis:

- A department
- A business unit
- A new system under development
- A service

With the purpose to map the business risks in using IT

**2. *Selecting the assets to be protected***

The area's use of IT is based on a series of IT resources, which must be protected in order to avoid releasing security-threatening events. The IT resources are typically:

- The network, including the operative system software
- Servers, e.g. in groups
- User systems e.g. grouped by security classification
- Databases, including database software
- Communications software

**3. *Analysing the threats***

Security threatening events occur where threats can take advantage of vulnerabilities. Threats may be accidental or deliberate, but in both instances they should be identified and the probability should be assessed. Threats may typically be identified within the following main groups:

- Wrong use
- Oversights
- Deliberate harmful acts
- Technical errors
- Hacking
- Viruses
- Manipulated code

One should keep in mind that an attempt to make up an exhaustive list is doomed to fail in that it continuously will change in accordance with the development of the business area and IT technology. In the process of identifying current threats it is therefore advisable to use historic events, past experiences and the updated knowledge of the people involved. Thus, an IT auditor who interviews users and IT-employees regarding the overall threat will aim at trying to keep up to date through newsletters and articles in journals and look at current threatening events. In time, the IT-auditor will probably create his or her own private list of threats. But at the same time he or she must also be open to keeping it updated.

In the interviews there should also be questions regarding:

- How frequent a threat has occurred/may occur
- Who might the intruder be, including their motivation and resources
- Which asset could it be
- Particular elements in the surroundings (e.g. danger of fire next door or flooding)

It is worth noticing that a threat in itself isn't dangerous unless there are vulnerabilities it can take advantage of. Vulnerabilities may for instance be:

- Unprotected lines of communication
- Unqualified or careless users
- Wrong choice and use of passwords
- Insufficient quality insurance
- Weak access control both physically and logically
- No backup, neither of data or software
- Physical damaged IT equipment

The vulnerabilities should be indicated in a separate column if they are immediately recognisable, but their inclusion is not vital for the threat assessment.

Finally, it is also worth noticing that a threat rarely can be removed, instead it should be met by a security measure. For instance, a water pipe through a computer room may pose a threat, which can be eliminated. However, this will often be too costly. Instead it may be preferable to add additional safeguards e.g. a waterproof cloth under the pipe and covering the computers.

#### **4. *Evaluating the negative impact and frequency***

Above are the assets, which could be influenced by the identified threats. But it is also necessary to have them valued. However, this is not as simple as it may seem, as it is not only a question about the price of the individual asset, but also about the value of the asset to the company. The effect of a server being physically damaged may for instance equal the intrinsic value plus the value of the lost business due to a server breakdown for a period where they have been unable to serve the customers.

It cannot immediately be determined whether the asset value or the commercial value predominates; this will depend of the size and character of the company. Even the effect of the damage should also be estimated according to the basic security criteria, i.e. whether the IT breakdown is for a period of time (availability), whether information has become available to the wrong people (confidentiality), and whether data has been destroyed or manipulated with (integrity).

Naturally, the assessment of the impact of the damage is a very difficult task, which must be carried out in collaboration with the owners and users of the said assets, i.e. not IT employees. The closest to quantifying the effect of the damage is most often these three levels: high – middle – low, with high indicating critical consequences for the company. This may be sufficient if the goal primarily is to carry out a mutual prioritisation.

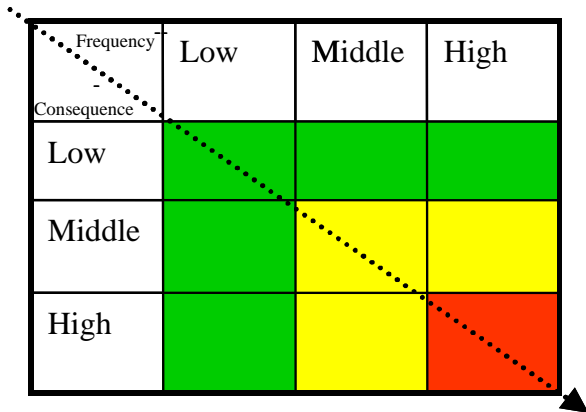
The possibility or the frequency of a given threat should then be evaluated and when it concerns technical threats it will typically be the IT employees who have the most relevant knowledge. Here quantification into high – middle – low is also the most precise method.

#### **5. *Rating the level of threat***

The level of threat is laid down in a diagram "threat assessment" with damage effect/consequence and frequency as axes, as each security threatening events should be marked with its own unique number and then be rated on the sloping dotted scale for the level of threat. This scale: high – middle – low is rendered visible by the colours red - yellow – green in the diagram. In other words, the

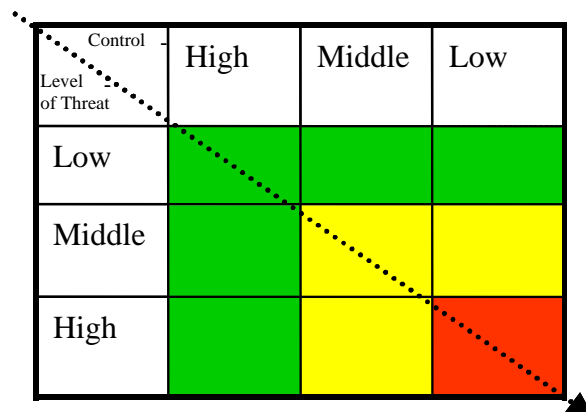
markings in the green area are of little importance while red markings are critical. By looking at the largest concentration of markings alone it will give a comprehensive view of the level of threat.

Matrix for threat



The level of Threat

Matrix for risk



The level of risk

**6. Considering the Control Environment**

During the threat assessment we haven't taken into consideration the effect of the control environment. This is why all existing security safeguards and procedures surrounding the asset in question should be identified and their efficiency evaluated in relation to each observation (security threatening event). Then each observation and the controlling measures connected to it should be marked in the diagram "risk assessment".

**7. Summarising the risks**

In the risk assessment diagram the scale showing the level of risk (the dotted line): unacceptable – partly acceptable - acceptable rendered visible by the colours red – yellow – green in the diagram. In other words, the markings in the green area are of little importance while red markings are critical. By looking at the largest concentration of markings alone it will give a comprehensive view of the level of threat.

We will now be able to ascertain, that the numbered markings made in the level of threat diagram have moved towards the left in the risk assessment diagram due to the controls, which have been identified. Still, the level of risk will probably be too high (accumulation in the red and yellow areas), and the idea is then to gradually introduce more controls (security measurements and procedures) in order to move the markings for security threatening events back on "the level of risk" scale. As a minimum requirement the aim is to remove all markings in the red area and most of the markings in the yellow area.

At this point the financial considerations become relevant, as any company should consider the costs and the difficulties connected to introducing more security against the risks at hand. The problem is mainly how to quantify the risks, making it both necessary and useful to leave this decision to the board of directors when the sums are considerable.

Appendix – The risk circle:

