7

An object-oriented approach to an IT risk management system

Gunnar Wahlgren
SÄKdata AB, Ingenjörscentrum, S-198 78 Sollentuna, SWEDEN

The need of continuous control of the IT security in an organisation has increased as the organisations dependencies of computers has increased. To make such analysis simpler computer aided systems (tools) have been developed.

There is a need for a IT risk management tool to be used in the continuous control process. This tool shall be used to react fast on changes in the IT-system and the surrounding environment. Properties needed in such tools are:

- Be able build and store a model of complex IT-systems
- Be able to automatically give advise of measures to be taken when a change is done

There exist attempts to produce such systems today. However these system have a number of limitations like being too inflexible. Some of the limitations can be avoided if an object-oriented approach is used. The interesting properties of objects and the object-oriented approach can assist in increasing flexibility and reducing risk.

1. Introduction

1.1 The risks of IT-systems

An organisation and its information system is exposed to different threats, both inside and outside the organisation, which can have an negative effect on the objectives of the organisation. By the introduction of computers the threat pictures have changed as new threats have arise.

The role of the IT-system is to provide services of different kind to the organisation. If we want to evaluate the value of the IT-system for the organisation we must look at the IT-system from a business perspective [KEEN91].

As the value of an IT-system must be looked upon from a business perspective the same thing is valid for the security of that IT-system. There is of course little need to spend much effort on security measures for an IT-system that have little business impact for the organisation. It is therefore necessary to have a balanced and realistic view of the risks of IT-systems.

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

1.2 The complexity of IT-system

For an organisation should work it must have some kind of information system. In order to make an organisation more effective part of the information system has been computerised. The information system of an organisation is tremendously complex and it is only a small part of it that has been computerised.

Even if the computerised part of an organisations information system is far more simple then the total information system it is nowadays usually also very complex. An organisation of any size normally have many computers at many physical locations (maybe connected in some type of network) and are running a large number of different application systems on these computers. The threat picture for this kind of computerised information system is naturally also very complex and the different combinations of safeguards that can be installed against the threats practically unlimited.

1.3 Dynamic dimension

One of the most important aspect is the dynamic "dimension"; things are always changing [WAH92]. As the risk situation continuously is changing, the IT security officer needs to have information about the current situation. To be able to monitor change, the IT security officer needs some kind of model that describes the current situation. The model must cover both the IT-system and the environment around the IT-system. The conclusion is that we need a model that reflects the dynamic situation and, where it is possible, to store information about one state and only register changes to create a new state.

1.4 New trends for IT risk management

We end this section by summing up some of the most important aspects for a computer aided IT risk management system:

- The risk management (RM) system should model the IT-system from security point of view and the model together with the risks of the IT-system at one point of time should be saved as a "state".
- The RM-system should be used for continuously following-up the risk of the IT-system when the IT-system and/or the environment around the IT-system is changing It should be possible to compare the (possible) different risk situation with this new "state" against the old state
- The RM-system should suggest actions to be taken so the IT-system should reach some desirable "state" as defined by the management (bring the risk of the IT-system in "balance").
- The RM-system should contain "external" information about threats, vulnerabilities of assets, and effects of safeguards, thus being a repository of knowledge [AND93].
- The RM-system could have a bookkeeping function and act as a part of a configuration management system [OTW90]

2. Model of IT-systems security

2.1 Modelling problem

There are some problems we have to deal with when we want to model IT-system security:

- An asset has relations to many other assets
- The same threat can affect many assets
- One asset can be affected by many threats that will cause the same impact
- The same safeguard can protect many assets from one or many threats
- Threats and safeguards affect information asset impact areas indirectly via components (like computers)

The figure below shows a draft to a model of the complex situation.

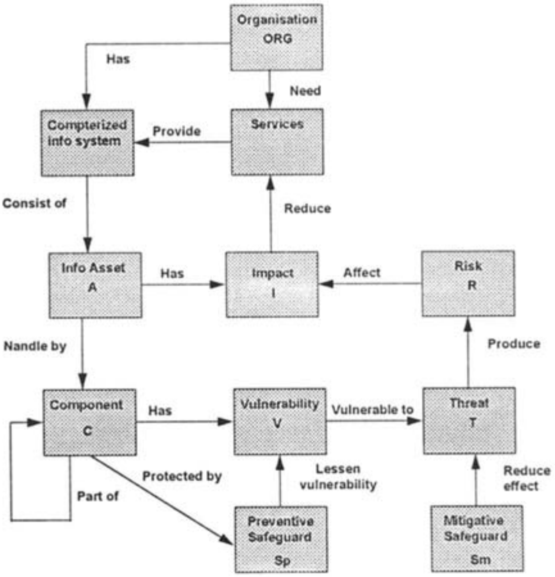

Figure 1: Model of IT-system security

2.2 Modelling of assets

One of the key problems is to model the assets and the relation between assets. First this requires a list of different assets to select from. A list could be divided into sublists (e.g. computer could have a sublist with different computer brands). To relate selected assets to each other requires information for each asset type which other asset type it could be related to.

The result will be a number of hierarchical structures of different kinds. Example of a structure is organisation (organisation, department, group etc.), building (building, room etc.). In the lowest level we have information asset related to one or more component asset. On the next level we have component asset related to other component asset (e.g. a program is running on a computer). The asset on next level could in turn be related to other levels (e.g. room in a building) which in principle can go on forever. In practice, however, there are normally not more than three levels.

The final result could be seen as a large number of asset element of different types where each asset is a part in and/or a part of other asset structures.

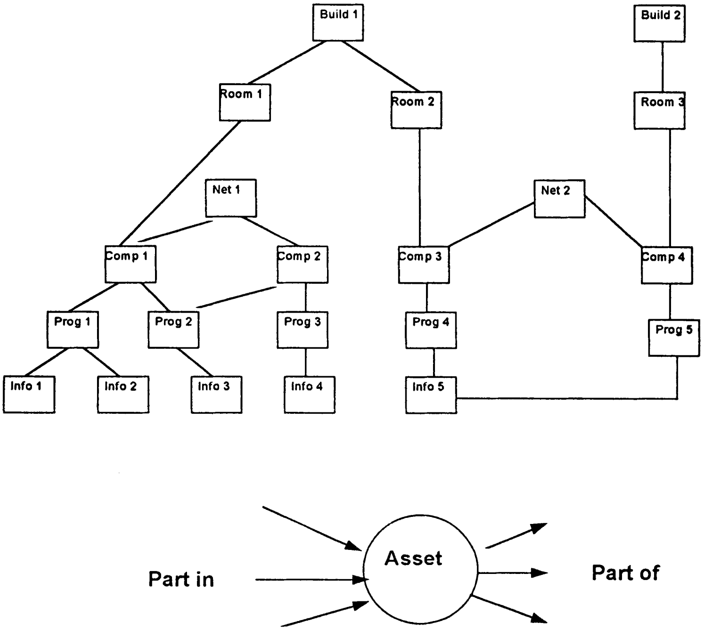

Figure 2: Model of assets

3. Handling of changes

As we have indicated earlier one of the most important work for the IT-security officer is to use the IT risk management system to handle change in the IT-system and in the surrounding environment. In this section we will look at what happens when different changes of the current IT-system are made.

The desire is that a change can be made with as little need for the IT-security officer to re-enter information as possible. The ideal situation is that only information of the change is entered. To reach this requirement it is necessary that the elements and relation between elements are stored, but it is also necessary that new elements and relations are created automatically.

Let us first look at some examples of asset changes which probably is the most common thing that will happen:

- Two cases are obvious; new assets (like a new application system) are added or an asset (like a computer) is not longer used.

- A third case represent a situation where the value of an asset for an organisation change. The negative effect for the organisation in terms of lost confidentiality can, for some reasons, have changed (e.g. the information is not so important to the organisation any longer).

There are lot of examples when we have to change the current threat situation:

- One case is when we have received information that a certain threat will affect assets of certain type in a different way than before. Recent knowledge could for example indicate that water does not damage certain type of computer hardware as seriously as we thought before.
- An other case is a situation when we have information that the possibility that a threat occurs (threat strength) has changed. The reason can for example be some change in the environment round the organisation (like a new petrol station as neighbour) that will make the possibility for a fire more likely.
- A last case is when a totally new threat is discovered. We not only need information of the new threat but also how this threat can affect certain assets due to certain vulnerabilities and what effect certain safeguards (hopefully) will have on that threat.

Change in the current vulnerability situation is similar to change in the threat situation described above:

- One example could represent a situation when a computer is moved from one room to another room where the vulnerability to certain threats are different (because the new room is situated on another floor).

Examples of changes of the current safeguard situation are as common as the change of assets.

- A new safeguard is installed or an existing safeguard is no longer valid.
- An other case is when an existing safeguard is used in a more efficient way. Example could be that an installed access control system is used in the way it was intended (passwords are changed regularly etc.).

Change of risk represent situation when the management, due to some change in the information security policy; want to have another desirable risk level for one or many impact areas. If the management for some reason (e.g. embarrassment) considered the negative effect of confidentiality to be more harmful than before then maybe they do not want to accept the same risk for that impact area as before.

4. Object-oriented approach

As we have seen an IT risk management system must be able to handle models of complex IT-systems which are constantly changing. One way to do that is to use object-oriented technique. The interesting properties of the object-oriented approach are:

- The possibility to inherit characteristics from more general objects which makes it easier to store knowledge.
- The possibility to let objects, with help of relations, affects other objects
- The possibility to build models of large IT-systems where the relation between the parts of the system are complex
- The possibility to easily maintain the model when new parts are added or deleted
- The possibility to easily change the characteristics of an object then evaluated which effects this will have on the IT-system as whole.

4.1 Object-oriented model.

The figure below shows a draft of an object-oriented model. The model includes the basic element as objects; assets (A), threats (T), vulnerabilities (V), safeguards (S) and risk (R). The model also includes other objects. The reason for this is the way many to many relations between the basic elements are model.

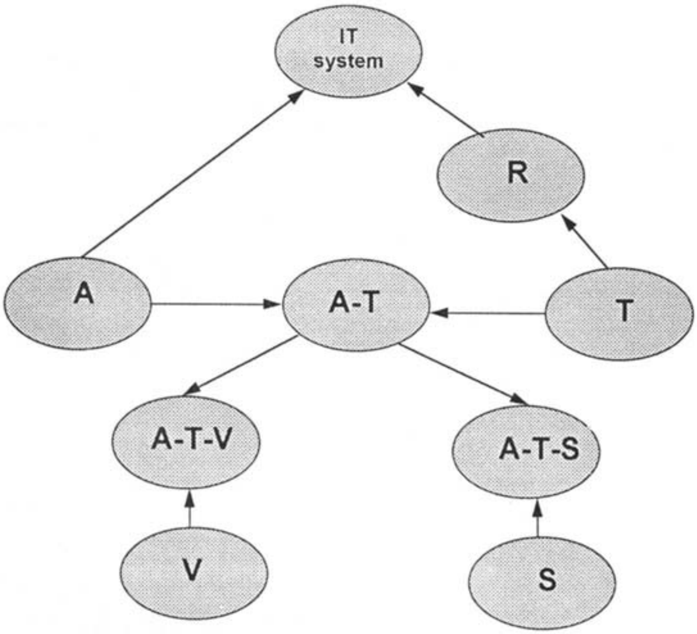

Figure 3: Object-oriented model

4.2 Objects specifications

Object modelling normally consists of three kinds of models:

- The object model that describes the static structure of a system in terms of objects and the relationships between objects.
- The dynamic model that describes the control structure of a system in terms of event and states.
- The functional model that describes the computational structure of a system in terms of values and functions.

Even if the risk analysis problem places different emphasis on the three kinds of models all three models are necessary. These models are then combined into a refined description of objects where the objects also will include properties from the dynamic and functional models. We end this paper by showing the different refined objects with their attributes and operation

IT system

Attributes:

- Desirable risk for each impact area
- Current risk for each impact area

Operations

- Define assets
- Evaluate asset
- Define current vulnerability situation (including current safeguards and threats)
- Evaluate current risk situation
- Evaluate desirable risk situation

Asset

Attributes:

- Asset value for each impact area

Operations:

- Create asset
- Relate asset to other asset
- Evaluate asset
- Define threat situation (= relate asset to threats)

Threat

Attributes:

- Threat strength for each impact area
- Desirable risk for each impact area
- Current risk for each impact area

Operations:

- Create threat
- Evaluate threat strength

Asset-threat

Attributes:

- Threat effect for each impact area
- Threat probability for each impact area
- Current risk for each impact area

Operation

- Create asset-threat
- Define vulnerability situation (for asset-threat combination)
- Define safeguard situation (for asset-threat combination)
- Evaluate threat effect
- Evaluate threat probability
- Calculate risk

Asset-threat-vulnerability

Attributes:

- Threat probability for each impact area

Operation

- Create asset-threat-vulnerability
- Define vulnerability situation (for asset-threat-vulnerability combination)
- Evaluate threat probability

Vulnerability
Attributes:
- Vulnerability situation

Operation
- Create asset-vulnerability
- Evaluate vulnerability situation

Asset-threat-safeguard
Attributes:
- Threat probability or threat effect for each impact area

Operation
- Create asset-threat-safeguard
- Define safeguard situation (for asset-threat-safeguard combination)
- Evaluate threat probability or threat effect

Safeguard
Attributes:
- Safeguard strength

Operation
- Create asset-safeguard
- Evaluate safeguard strength

Conclusion

A computer aided risk management system is needed to model the complex IT-system of an organisation from security point of view. The risk management system must also be able to handle change in the IT-system and in the surrounding environment in a simple way. The use of object-oriented technique will make it easier to build such IT risk management system.

References

AND93 A. M. Anderson, D. Longley and A. B. Tickle, "**The Risk Data Repository: a novel approach to security risk modelling**", Proceeding of the Ninth IFIP International Symposium on Computer Security, IFIP/Sec'93, Deerhurst, Ontario, Canada, May 1993.

KEEN91 P. G. W. Keen, "**Shaping the Future; Business Design through Information Technology**", Harvard Business School Press, 1991.

OTW90 K. Otwell and B. Aldridge, "**On the Automation of Computer Security Risk Management**", Proceedings 3rd International Computer Security Risk Model Builders Workshop, Santa Fe, New Mexico, August 1990.

WAH92 G. Wahlgren and J. Carroll, "**General System Theoretic Model of InfoSecMan**", Proceedings IFIP Working Group 11.1 workshop on information security management, Singapore, May 1992.