IT Security Risk Management practices in large Swedish organisations

Abstract

The main purpose of my work is to investigate current IT Security Risk Management practises used in large Swedish organisations and compare the results with an earlier report from 2003 by the author. The aspects that will be studied in more detail are:

- How IT Security Risk Management Methods and Risk Assessments tools are used by the organisations. What kind of methods and tools are used. How advanced are the tools and are any computer aided tools used? Is an IT Security Risk Assessment done for the whole organisation and in this case what is the frequency or is only new application systems considered?
- How the reuse of IT Security Risk Assessment result is handle. How simple is it to add changes and make a new IT Security Risk Assessment without starting the analysis again from the beginning.
- How IT Security Risk Management decisions on different organisational levels is done and how the decisions interact with each other and what frequency is used. Organisation normally has three different levels where IT Security Risk Management decisions are made; top management, middle management and staff.
- How the Socio-technical framework is used and that both social countermeasures and technical countermeasures are considered against threats of different kinds. A countermeasure can also deter, prevent, detect, respond or recover against on or more threats and all of these aspects should be covered.
- How organisations have adopted the relationship between Compliance and IT Security Risk Management. Compliance means confirming with stated requirement like predefined countermeasure of different kind. The disadvantage is that compliance is not risk oriented i.e. there are no valuation when it is relevant to have a specific countermeasure.

First a brief overview of current IT Security Risk Management / Risk Assessment Methods and Tool will be done. In the second step IT Security Risk Management practice in a number of large Swedish organisations will be studied by interviewing IT Security staff.

Few studies of how IT Security Risk Management is used in practice have been presented. The result from this study hopefully leads to a better understanding of the field and improve the future use of different methods and tools.