# IT Security Incidents Escalation in the Swedish Financial Sector: A Maturity Model Study

G. Wahlgren, A. Fedotova, A. Musaeva and S. Kowalski

Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden
e-mail: wahlgren@dsv.su.se

## Abstract

This paper reports the primary results of a design science research study to deal with the problem of IT security escalation in Swedish government and private organizations. A maturity capability escalation model was used to perform evaluations of two of Sweden's four largest banks. The evaluation indicated that banks were aligned with the current Swedish regulations minimal requirements for IT security incident handling and where on a level 3 of a 5 level model.

## Keywords

Incident Escalation, Maturity Models, IT Security Risk Management, Financial Sector

## 1. Introduction

IT-related security incidents in the financial sector can have a cascading effect on other sectors in the economy. If bills cannot be paid, then both production and delivery slow down and in some case stop completely. For example, in 2011 a major IT services provider in Sweden caused an IT-related security incident that had major operational disruptions among a number of government and private organizations in Sweden (MSB, 2014). In order to prevent and mitigate this cascading problem for IT security incidents in Sweden the Swedish Financial Supervisory Authority (FSA) have developed and defined a number of different controls and regulations. An important part of these controls is how IT security incidents are handle and how escalations of these incident both with and between business and agency in the sector should occur.

As part of a doctoral research program at the Department of Computer and Systems Sciences, Stockholm University we are performing a 3 cycle design science research project to deal with the problem of IT security escalation with and between government and private sector organization in Sweden (Wahlgren and Kowalski, 2014). To deal with the problem we are developing and evaluate the use of a maturity model to measure an organization's escalation capability of IT-related security incidents. Some of the main reasons for using maturity models for an organization development is that it gives the organization the possibility to do self-evaluations and to also the possibility follow-up measurable results for stepwise

improvement. The Escalation Maturity Model (EMM) for an organizations escalation capability of IT-related threats consists of 6 different maturity levels from "Non-existent" to "Optimized" and also 6 maturity attributes from "Awareness" to "Procedures and Tools".

In the first cycle of our research we constructed a version of our maturity model. This version was evaluated with help of IT security specialist from both the private and public sector and also researchers from the academic world. Based on the evaluation we made improvement and the second version of our model was ready for a trial in late 2014. In this cycle, the second cycle, we evaluated version 2 of our model on different organisation. To do this we constructed a query package to evaluate the organizations maturity levels, both the total level and the level for the different attributes. This paper describes and reports the result of cycle 2 were we evaluate our model on two of Sweden's four largest banks.

We have divided the rest of the paper into 4 sections. In the background section we present some related works in IT security risk management and incident escalation. In the second section we describe our research plans and our maturity model for escalation capability. In the following section we first compare the requirements of the various maturity attributes of the model with the regulations set by the Swedish Financial Supervisory Authority for the players in the financial sector. We then present the results of evaluating the maturity model on two of Sweden's largest banks. In the last section we conclude the paper with a discussion of how our model currently being developed for cycle 3.

## 2. Background

### 2.1. IT Security Risk Management

The International Standard Organization (ISO) has established a standard for IT Security Risk Management (ISO, 2008A). The term IT Security Risk Management refers to approaches and methods that lead to cost effective security solutions. This is done by a process of measuring the security risk to IT systems and assuring adequate levels of protection. IT Security Risk Management is a continuous process and consists of the following steps: (i) Risk monitoring, (ii) Risk assessment/Risk treatment, and (iii) Risk communication. NIST (NIST, 2010) has introduced the framework of Enterprise-wide Risk Management using three different levels (Tiers) where one can look at the organization from different views where IT Security Risk Management decisions are made: (i) Top management, (ii) Middle management, and (iii) Operational Staff.

### 2.2. Escalation, and Escalation of IT-related security incidents

In common language the term escalation is used when different conflicts are sharpened and the conflict therefore is handled by a higher level in the organization or society (Kahn, 1965). In our study we use the term in the sense that you seek assistance from a higher level when you yourself cannot handle an incident. In both

cases, this means that you also pass the responsibility to deal with an incident to a level above.

According to ISO (Information security incident management) an information security incident is defined as: " single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (ISO, 2011). IT Infrastructure Library (ITIL) which relies on ISO/ISE 20000 ("IT Service Management") defined an incident as: "Any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service" (ISO, 2005). For our study however, have used the definition from Swedish Civil Contingencies Agency (in Swedish: Myndigheten för Samhällsskydd och Beredskap, MSB) in our research: "An IT incident is an undesired and unplanned IT related incident affecting the security of the organization's or society's information processing and that may cause a disruption of the organization's ability to conduct its operations" (MSB, 2012). An IT related incident might be:

- Disruption in software and hardware
- Loss of data
- Security vulnerabilities in products
- External attacks
- Human errors in handling
- Interference in the operating environment
- External events

When handling incidents of different kind, each organizational level has to consider if the incident would harm the acceptable risk level of the entire organization. Each level has basically three alternatives: (i) you can accept the risk, (ii) you can try to mitigate the risk (Risk Treatment), or (iii) you can escalate the risk to the organizational level above. Another alternative is to transfer the risk to a third party but these options are usually only available at the strategic level. Reasons to escalate could for example be budgetary considerations to implement new countermeasures, or that the incident is so serious that help from a higher level is needed. Escalation of an IT-related security incident will probably lead to Risk Treatment of some kind. If a crisis occurs the organization of cause must respond and recover from the damage the incident has caused. If the incident does not require immediate action, escalation could in the future mean that new countermeasures to deter, prevent, and detect should be installed if similar incidents will happen.

### 2.3. Maturity models

Nolan (Nolan, 1973) was the first to present a descriptive stage-theory concerning the planning, organizing, and controlling activities associated with managing the organizational computer resource. Nolan developed a model with stages of growth and some workable variables identifying the stages and several other researchers have been inspired by Nolan. The capability maturity model was first described by

Humphrey (Humphrey et al., 1987) who used maturity models for assessing software engineering capability of contractors. Design principles of maturity models are discussed in ISO Assessment of organizational maturity which defines organizational maturity as "An expression of the extent to which an organization consistently implements processes within a defined scope that contributes to the achievement of its business goals (current or projected)" (ISO, 2008B). Solli-Sæther (Solli-Sæther and Gottschalk, 2010) discuss the modelling process for stage models. They suggest 5-step procedure for the stage modeling process. Pöppelbuβ (Pöppelbuβ and Röglinger, 2011) describe three design principles for maturity models: (i) Descriptive, (ii) Prescriptive, and (iii) Comparative. Philips (Philips, 2003) describes how to use a Capability Maturity Models (CMM) to derive security requirement and how to use System Security Engineering CMM (SSE-CMM) as a useful foundation. Karokola (Karokola, 2012) describes how to integrating E-government deployment maturity model with a new maturity models concerning IT-security. ISACA (ISACA, 2009) presents how maturity models could be used to recognize on what maturity levels different IT-security Risk Management processes are.

# 3. Approach

## 3.1. Research methods and research cycles

Our approach is based on scale-development theory (Nolan, 1973). Once the scale is developed, it must be tested for validity and reliability. Scale development in this study consists of three stages or cycles. In the first stage, the scale items already described in the literature will be evaluated. In the second stage a reliability and validity test will be used. In the third and final stage we will perform a formal testing of the scale's reliability and validity. We will use scale development to build our maturity model to be able to measure the maturity level of different organization. Combined with scale-development theory we have use a design science approach. Design science research methodology consists of 5 process steps (Vaishnavi and Kuechler, 2004). In the first step we gather information and built up awareness of the real world problem. The next step is a suggestion for a tentative design with the tentative design as output. The third step is an attempt for an artifact design which is developed from the tentative design. In the following step the artifact is evaluated with help of performance measures. Finally, the design processes are completed and conclusions (results) are drawn. The design process is iterated back until the real-world situation is improved. As mentioned above our research is divided into three cycles where each cycle consists of the 5 process steps.

In the first cycle we constructed the primary version of our maturity model. This version was evaluated with help of IT security specialist from both the private and public sector and also researchers from the academic world. Based on the evaluation we made some improvement and the second version of our model was ready late 2014. In cycle 2 we tested version 2 of our model on different organization. To do this we first constructed a query package. After answering the question in the query package it is possible to evaluate the organizations maturity levels, both the total

level and the level for the different attributes. In cycle 3 we will create test scenarios which are to a large extent based on actually IT-related security incidents that have been reported in Sweden. We will then use these scenarios to establish the predictive ability of our maturity model.

### 3.2. The maturity model and query package

According to Philips a capability maturity model is: "a model for judging the maturity of the processes of an organization and for identifying the key practices that are required to increase the maturity of these processes" (Philips, 2003). We present a maturity model for measuring the escalation ability for handling IT-related security incidents. We have used ISACA´s Risk IT Framework (ISACA, 2009) as a starting point when we defined our model and have used almost the same maturity levels and attributes.

| Attribute / Level | Awareness | Responsibility | Reporting | Policies , standards | Knowledge, education | Procedures, tools |
|---|---|---|---|---|---|---|
| Non-existent | | | | | | |
| Initial | | | | | | |
| Repeatable | | | | | | |
| Defined | | | | | | |
| Managed | | | | | | |
| Optimized | | | | | | |

**Figure 1: Maturity model for escalation capability**

The maturity model for escalation capability has 6 different maturity levels:

0. **Non-existent** means that different processes are not applied and there is no need for any kind of measures.
1. **Initial** means that the need for measures has identified and is initiated but the processes that are applied are ad- hoc and often disorganized.
2. **Repeatable** is when measures are established and implemented and the various processes follow a regular pattern.
3. **Defined** is when measures are defined, documented and accepted within the organization.
4. **Managed** means that the processes are monitored and routinely updated.
5. **Optimized** means that processes continuously evaluated and improved using various performance and effective measures tailored to the organization's goals.

There are also six different maturity attributes:

1. **Awareness** deals with various aspects of how aware people are in the organization of various IT-related security incidents.
2. **Responsibility** deals with various aspects of accountability within the organization of IT-related security incidents.
3. **Reporting** is concerned of the reporting channels and how regular reporting of IT-related security incidents are done.
4. **Policies and standards** are concerned with whether different policies and standards for IT-related security incidents exist.
5. **Knowledge and education** deals with the different skills and knowledge that are needed in the organization for IT-related security incidents
6. **Procedures and tools** are concerned with methods of using various procedures and tools for handling IT-related security incidents.

These attributes are being suggested heuristically as a starting point. To help the organization perform a self-assessment we developed a query package. The number of questions in the current version is 37. The answer to each question (one or more) of the different maturity levels and attributes are "Yes" or "No". Here are examples of questions for the different attributes and to which maturity level each question belongs:

- Is there awareness among employees on various IT-related security incidents? (Attribute 1, level 1)
- Is it absolutely clear about the responsibilities of each employee for occurred IT-related security incidents? (Attribute 2, level 1)
- Has regular reporting on IT-related security incidents to the organization's management been defined, documented and accepted? (Attribute 3, level 3)
- Have policies and standards for the management of IT-related security incidents been identified and initiated? (Attribute 4, level 1)
- Have the knowledge requirements in the form of concrete training plans for employees of IT-related security incidents been established and implemented? (Attribute 5, level 2)
- Is there a routine updating of procedures for the handling of IT-related security incidents? (Attribute 6, level 4)

It is important to mention that all of the maturity attributes in one maturity level must be satisfied before the next level can be obtained. Further, the maturity level for various processes within one level, also apply for the next level. The way to calculate the total maturity level is to take the maturity attribute that has the lowest value. If an organization, for example, shall reach the total maturity level "Defined", all the individual maturity attributes at least must have the maturity level "Defined".

# 4. The study

## 4.1. Swedish Financial Supervisory Authority's (FSA) regulations

Before we started to validate our maturity model of the participating banks, we want to compare the requirements of the various maturity attributes of our model with the

regulations set by the FSA for the players in the financial sector. We did this by an interview with a representative from the FSA and also by studying the FSA's regulatory codes (FFFS 2014:1, 2014), (FFFS 2014:4, 2014). The interview was conducted with the Operational Risk Analyst unit Swedish Financial Supervisory Authority in the month April 2015. According to FSA's recommendations and regulations the following applies for the different maturity attributes:

- **Awareness**. There must be awareness among employees of various It-related security incidents. Employees should know the risks of the various IT-related security incidents affecting the organization.
- **Responsibility**. FSA stipulates that it is the management who has responsibility to clarify employee roles and responsibilities for the management of IT-related security incidents.
- **Reporting**. An organization should have a procedure to regularly report the risks that exist or may be expected to occur to the Board, the CEO and other functions that need this information. The information should be reliable, current, complete, and reported in right time.
- **Policies and standards**. Every organization should have policies and standards for the management of operational risks.
- **Knowledge and education**. FSA has no specific requirements for the training on IT-related security incidents for all employees within the organization. However, directly involved employees in the incident management process must have the knowledge and training to manage their tasks.
- **Procedures and tools.** FSA has no strict requirements that procedures for managing IT-related security incidents must be automated. However, there are banks that are trying to reduce dependency on human decisions because the decisions makers are hard to reach so it will take time to make a decision. The larger the organization is the more reason to try to automate the management of IT-related security incidents.

The conclusion that one can draw from FSA's recommendations is that they correspond well with the requirements of the various maturity attributes in our model. The difference is that with our model, we have introduced different levels, making it possible for an organization to stepwise improvement of their processes. If you compare FSA's recommendations to the levels in our model, all attributes except "Procedures and tools" reach the level "Optimized". "Procedures and tools" only achieve the level "Defined" as the requirement for automated procedures for managing IT-related security incidents already exist on the level "Managed".

### 4.2. Use of the maturity model on two large Swedish banks

In the next step, we tested our maturity model on two of Sweden's largest banks by conducting interviews with persons responsible for IT-related security incidents, both interview subjects were from the tactical level of the organization which in our model is divided into operational, tactical, and strategic levels. Both interviews were

conducted in the month April 2015. The Banks show broadly similar patterns for the different maturity attribute.

For the maturity level "**Initial**", all the maturity attributes were fulfilled. All processes have been identified and initiated within the organization. All maturity attributes for the maturity level "**Repeatable**" are met for the banks. At this level of maturity, all processes are established and implemented and follow a regular pattern. Both Banks also reaches the maturity level "**Defined**". This means that all aspects for the maturity attributes Awareness, Responsibility, Reporting, Polices, Knowledge, and Procedures are met. All processes are defined and accepted in the organization. The maturity level "**Managed**" means that there exists a routine update of all the maturity attributes. Both Banks meet all of the maturity attributes except one, which is "Procedures and Tools" where the procedures for managing IT-related security incidents are not fully automated. The highest maturity level "**Optimized**" means that all processes are evaluated and continuously improved using various performance measures. This applies for the attributes Awareness, Responsibility, Reporting, Polices and standards, as well as Knowledge and education.

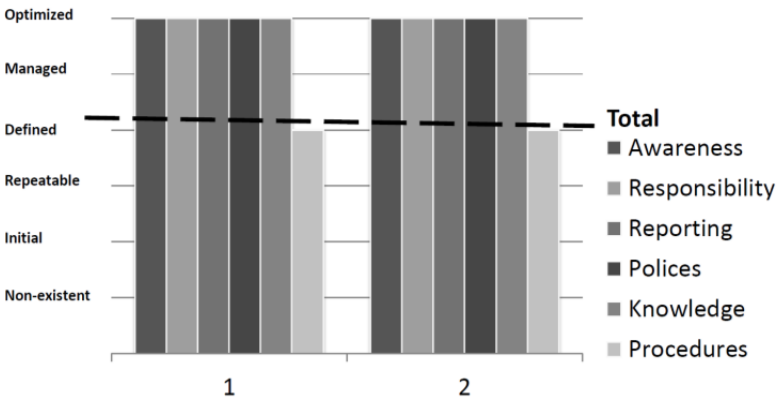


**Figure 2: Result from Bank 1 and 2**

If we take the maturity attribute that has the lowest value, the total maturity level for both banks only reach the maturity level "Defined" because the maturity attribute "Procedures and Tools" only reach the maturity level "Defined". The figure above shows both maturity levels of the individual maturity attributes and the total maturity level of the two banks.

## 5. Conclusion

Although these finders are from only two banks, these banks represent about 30 percent of the Swedish banking market (Swedish Bankers´ Association, 2016). The representatives indicated that query package was relevant to evaluate the escalation process within the organization and that the maturity model for escalation capability

of IT-related security incidents can be used to perform self-assessment in the banking sector in Sweden. The FSA´s representative thought that the requirement of the different attribute in the maturity model already exists in most large banks that use the standard controls such as ISO 27002 (Code of practice), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Control Objectives for Information and Related Technologies (COBIT), and Information Technology Infrastructure Library (ITIL). Our view is that certainly many of the requirements exist in other standards, but with our maturity model we have refined, systemized, and distributed the requirements to different maturity attributes. By introducing different levels within the various attributes, our maturities model gives the possibility of a stepwise process of improvement. This may be applicable to other, smaller players in the financial sector. Example of why stepwise development is to prefer is the maturity attribute "Procedures and tools". Procedures for managing IT-related security incidents is not fully automated and therefore both banks only reach the maturity level "Defined". This maturity level seems to be sufficient according to FSA's requirement but both banks strive to implement this feature in the future.

Currently we are developing a web-based tool to assist organizations in the self-assessment process. In this new version we will among other things review and, if necessary, clarify the questions. In future versions of the tool, we will also consider using more than "Yes" and "No" in response to questions. The tool will be used by organizations to enter answers to the questions in the query packet and then automatically calculate the total level of maturity as well as the maturity level of the individual attributes. The tool will also suggest what action the organization could take to achieve the desired level of maturity. We will use the tool for a number of organizations to compare the level of maturity that different organizational levels (strategic, tactical and operational level) within the same organization reaches.

In cycle 3 of our research, we will create test scenarios which are to a large extent based on actually IT-related security incidents that have been reported in Sweden. We will then use these scenarios to establish the predictive ability of our maturity model. That is to say given these IT-related security incident scenarios, the organization with the higher maturity level should deal with the incidents in a more effective and efficient manner than the organization with the lower maturity level. An independent expert observer, who is unaware of the organization establish maturity level, will be used to judge the response of the organization to these test scenarios.

## 6. References

FFFS 2014:1 (2014), "Regulations and General Guidelines regarding governance, risk management and control at credit institutions", Finansinspektionen, Sweden.

FFFS 2014:4 (2014), "Regulations and General Guidelines regarding governance, risk management of operational risks". Finansinspektionen, Sweden.

Humphrey, W., Edwards, R., LaCroix, G., Owens, M., and Schulz, H. (1987), "A Method for Assessing the Software Engineering Capability of Contractors", Technical Report, Software Engineering Institute, Carnegie Mellon.

ISACA (2009), "The Risk IT Framework", ISACA Rolling Meadows, IL, 60008 USA.

ISO, (2005), "Information technology – Service management", ISO/IEC 27000-1, International Standard Organization.

ISO, (2008A), "Information security risk management", ISO/IEC 27005, International Standard Organization.

ISO, (2008B), "Information technology – Process assessment; Assessment of organizational maturity", ISO/IEC Technical Report 15504-7.

ISO, (2011), "Information technology – Security techniques — Information security incident management", ISO/IEC 27035, International Standard Organization.

Kahn, H. (1965), "On Escalation: Metaphors and Scenarios", Praeger.

Karokola, G. (2012), "A Framework for Securing e-Government Services", Doctoral Thesis, Department of Computer and System Sciences, Stockholm University, Sweden.

MSB, (2012), "Nationellt system för it-incidentrapportering (in Swedish)", Myndigheten för samhällsskydd och beredskap.

MSB, (2014), "International Case Report On Cyber Security Incidents – Reflections on three cyber incidents in the Netherlands, Germany and Sweden", Swedish Civil Contingencies Agency.

NIST, (2010), "Guide for Applying Risk Management Framework to Federal Information Systems" NIST Special Publication 800-37 Revision 1, National Institute of Standard and Technology, U.S. Department of Commerce.

Nolan, R. (1973), "Managing the Computer Resource; A Stage Hypothesis", *Communication of the ACM*, July 1973*,* Volume 16, Number 7, pp. 399-405.

Philips, M. (2003), "Using a Capability Maturity Model to Derive Security Requirements", SANS Institute.

Pöppelbuβ, J., Röglinger, M. (2011), "What makes a useful Maturity Model? A Framework of general design principles for Maturity Models and its demonstration in Business Process Management", *Proceedings of the Nineteenth European Conference on Information Systems (ECIS 2011)*, Association for Information Systems (AIS).

Solli-Sæther, H., Gottschalk, P. (2010), "The modelling process for stage models", *Journal of Organizational Computing and Electronic*, Volume 20, pp. 279-293.

Swedish Bankers´ Association, (2016), "Banks in Sweden" [Retrieved from: www.swedishbankers.se, last accessed March 2016]

Vaishnavi, V., Kuechler, W. (2004), "Design research information systems" [Retrieved from: http://desrist.org/design-research-in-information-systems/, last accessed March 2016]

Wahlgren, G., Kowalski, S. (2014) "Evaluation of Escalation Maturity Model for IT Security Risk Management: A Design Science Work in Progress", *Proceeding of 2014 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*.