Evaluation of Escalation Maturity Model for IT Security Risk Management:
A Design Science Work in Progress

Gunnar Wahlgren
Department of Computer and Systems Sciences, Stockholm University
Room 7501, Forum 100, SE-164 40 Kista, Sweden
E-mail: wahlgren@dsv.su.se

Stewart Kowalski
Faculty of Computer Science and Media Technology, Gjøvik University College
Gjøvik, Norway
E-mail: stewart.kowalski@hig.no

ABSTRACT
In this early stage paper we present a draft of an IT Security Risk Escalation Capability Maturity Model. This model is used to develop a new approach to IT Security Risk Management where IT Security Risk Management is placed as a recurring activity at all levels of the organization including the strategic, tactical and operational levels. To construct this model we combined ISO 27005 framework for IT Security Risk Management with NIST Multitier framework and take elements from the ISAC IT Risk framework. We end our paper with an outline of our current plans to evaluate this escalation maturity model by using expert groups to rank outcomes of response to similar IT incidents by different organizations that have been ranked according to this maturity model. In this way we hope to establish if there are correlations as to the maturity level of an organization and how well it responds to an IT incident.

Keywords: Incident escalation, Maturity models, IT security risk management, IT security risk monitoring, IT security risk communication.

INTRODUCTION
Do we need a new IT Security Risk Management framework for managing IT Security Risks given the current rapid change in IT technologies? IT Security Risk Management frameworks have been developed over the years to deal with a number of changing IT technologies approach ranging from mainframe to client services to now the every present cloud based services. Are new IT security frameworks required when we change our IT technology base? Do we have to reinvent the wheel of risk management? The research goal for this study is to propose a framework that would facilitate organizations to effectively handle escalation of incidents.

According to International Standard Organization IT Security Risk Management consists of three main steps: (a) IT Security Risk Assessment, (b) IT Security Risk Monitoring, and (c) IT Security Risk Communication (ISO/IEC 27005, 2008). During the different eras in history of computing, from mainframe to cloud computing, IT Security Risk Assessment appear to have
has almost remained the same and but a number of different tools have been developed during the years (ENISA, 2005). The main step that needs to be change is primarily IT Security Risk Monitoring as it is necessary to react fast on new threats and incidents. This means that also the third main step, IT Security Risk Communication between different organizational levels, also need to be changed so organizations have a well-documented and communicated monitoring and escalation processes.

Ackerman (2000) has the following definition of social-technical gap: “The social-technical gap is the divide between what we know we must support socially and what we can support technically”. There does appear to be a growing systemic gap between what you can do with IT and the way you can control which is shown in the figure below (Kowalski, 1994). The gap in this figure could be technical, socio or socio-technical. The technological gap is the difference between what a computer security system is capable of enforcing and what it is expected to enforce. The socio-technical gap occurs when socially expected norms are not consistent with computer security policies. The social gap is when individuals do not act according to the expected social norms. To not handle escalation in fast way is an example of a growing of gap as you cannot control an incident in consistent with the computer security policies.

Figure 1: Abuse Opportunities and Control Capabilities vs. time (Kowalski, 1994)

The purpose of this paper is to propose a mature model for IT Security Risk Management which attempts to fill the socio-technical control gap without reinventing the wheel on the entire IT Risk management model but rather focus on socio-technical IT Risk Management issue like communication and monitoring. The paper is divided into 6 sections. In the first section we present ISO 27005 and other related works. In the second and third section we present a new mature model for IT Security Risk Escalation. In the next section we have a discussion of our research plans to evaluate this new model. In the two last sections we conclude the paper with a discussion of our new model.
BACKGROUND AND RELATED WORK

IT Security Risk

We use the term IT Security Risk to distinguish it from other Business Risk such as investment risk, credit risk, market risk etc. NIST (2002) has the following definition: “Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization” (p. 8). IT Security Risks are then adverse event on the Information Technology systems of an organization.

All organisations today have some kind of information system (IS) based on information Technology (IT). Organizations are exposed to different threats both inside and outside the organization. These threats can be avoided with help of countermeasures of different kinds. However it is difficult to justify spending effort on countermeasures for an IT-system that have little business impact for the organisation. To find the right mix of countermeasures a number of IT Security Risk Management methods and tools have been developed to assist the organization.

IT Security Risk Management

IT Security Risk Management is a part of Information Security Management which in turn is related to IT Security Governance. As a part of Information Security Management, ISO has established a standard for IT Security Risk Management (ISO/IEC 27005, 2008).

The term IT Security Risk Management refers to approaches and methods that lead to cost effective security solutions and countermeasures (ISO/IEC 27005, 2008). 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 outlined in the figure below.

![Figure 2: ISO 27005 IT Security Risk Management (adapted from ISO/IEC 2008).](image-url)
Baskerville (2013) has pointed out that survey of risk management practices show that the majority of organizations use no automated support for their risk management. Wahlgren (2004), in his study of large Swedish organization, has come to a similar conclusion and the tools used for risk analysis are rather simple and only in very few cases a more comprehensive tool is used.

One interesting aspect is IT Security Risk Management contra Compliance. 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. During recent years the use of compliance has increased for example by the US Sarbanes-Oxley Act (SOX compliance). This is discussed by Baskerville who compares Exposure Control Reasoning against Ethical Control Reasoning (Baskerville, 2009).

**NIST Multitier Organization-Wide Risk Management**

National Institute of Standard and Technology (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. Organization can be modeled to have three different levels where IT Security Risk Management decisions are made: (i) Top management, (ii) Middle management, and (iii) Operational Staff. The decision of top management is often of strategic nature while middle management is of tactical nature. Staff on the other hand had to deal with real IT security risk incidents and often had to react directly. The figure below describes NIST multitier organizational-wide risk management and the different tiers.

![Figure 3: NIST Multitier Organization-Wide Risk Management (adapted from NIST 2010).](image)

On the first Tier we look at risks from an organizational perspective. Risk management activities at Tier 1 directly affect activities on the other tiers by implementing governance structure that is consistent with the strategic goals of the organization. Governance includes such thing as determination of risk tolerance. Risk tolerance is the level of risk that is acceptable to the organization. Risk tolerance is often influence by the culture of the organization.

Tier 2 view risk from a mission/business processes perspective by designing and implementing processes that support business functions defined at Tier one. Important issues at Tier 2 are enterprise architecture where information security architecture is integral part.
Another issue is risk response strategies, which could be; accept, avoid, mitigate, share, and transfer.

Information system perspective at Tier 3 is guided by the risk decisions and activities at Tier 1 and 2. Risk management activities at Tier 3 are also integrated into the system development life cycle. At Tier 3 risk-based decisions are made regarding the implementation, operation and monitoring of organizational information system.

**IT Security Risk Assessment and Risk Treatment**

One of the main steps in IT Security Risk Management is Risk Assessment and Risk Treatment where different risks are compared against a risk levels and if necessary, new countermeasures are installed.

There are basically two ways to calculate risk: quantified or qualified approaches. The quantitative approach uses the expected number of adverse events per year and the average cost for the occurrence of one event. The qualitative approach, on the other hand, use a scale with (e.g.) three values: low, medium or high. This scale is used for expressing both the expected number of events and the cost for one occurrence.

The result of Risk Assessment and Risk Treatment is an IT security risk model that represents how an organization handles threats to information assets with help of countermeasures of different kind.

As an alternative to the Probability-based risk analysis, which is described above, Baskerville presents Possibility-based Risk Analysis (Baskerville et al. 2013). Possibility theory is an extension of fuzzy set theory that considered both the possibility and the necessity of an event.

**IT Security Risk Monitoring**

The next main step in IT Security Risk Management is Risk Monitoring. To maintain an acceptable IT security risk level IT Security Risk Monitoring need to be an ongoing process. NIST (2011b) define Information Security Continuous Monitoring (CM) as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions” (p. VI). According to NIST (2012), the data sources for CM include people, process, technology, and environment. Many CM implementations focus on technology as it is easy to automate data collection.

A number of Data Collection methods can be used to collect data. Examples are Surveys, Standards Based Methods and Tools, as well as Sensors of different kind. The methods could be both automated and manual. Data collection could be truly continual (always on) or continuous (collected periodically at some set interval).

**IT Security Metrics**

IT Security Risk Monitoring use Security Metrics of different kind. According to Brotby (2006), metrics is a term used to indicate a measure based on a reference and involves at least two points, the measure and the reference. There is some difference between monitoring and metrics. Metrics (benchmarks) provide information and monitoring is conducted to assess whether benchmarks are being achieved or not.
Security metrics can be categorized by what they measure for example performance, outcomes, trends, and probabilities. These categories of measurement can be further categorized by the methods used to measure them. Methods can include maturity, benchmarking, and statistical analysis. Security metrics may also be classified according to how they are measured for example quality, throughput, frequency, and magnitude. Brotby propose a taxonomy that defines 10 fundamental characteristics of metrics, which include the following categories (Brotby, 2006):

- Objective/Subjective
- Quantitative/Qualitative
- Static/Dynamic
- Absolute/Relative
- Direct/Indirect

**IT Security Risk Communication**

The last main step in IT Security Risk Management is Risk Communication which includes risk response strategies like risk acceptance and risk mitigation in a multitier organization (NIST, 2011a). Rasmussen (1997) has proposed a multi-level model which describe the organization risks, not only internally, and but also risk outside the organization as for example communication to and from the Government level.

![Multi-level model](adapted from Rasmussen 1997)

The figure above, originally from Rasmussen, has been slightly modified. The model for instance describes how it code and decode signals and communicate result between levels. The right side of the model describes “signals” from lower to upper levels in form of observation and report of different kind. This “signals” could lead to some kind of actions at the upper level and/or could be sent to next the level. The model also shows environmental stressor that can affect the organization from fast pace of technological change to changing.
political climate. The left side of the model describes different “signals” from one level to the level below from public opinion to judgment on the Government level, which then could become laws to the next level where laws will lead to regulations of different kind. Regulations in turn will lead to company policy etc.

**IT Security Competence and Responsibility**

An important aspect is the difference in Competence, Authority, and Responsibility (CAR model) on the different organizational levels (Pigeau et al. 2002) which is shown in the figure below. The different level use different terms and concepts depending on their authority, IT competence and responsibility. The top management has for example high authority but sometimes lack the IT competence and language to communicate with individuals in IT operations. It is necessary that there is a balance between the various organizational levels concerning competence, authority, and responsibility. Lock et al. (2009) present a graphical and analyze technique for responsibility modelling within organization. The technique is used to explore shortage in the responsibility structure.

During the last years, responsibility for middle management has increased without an equal increase in authority. In many cases the IT competence for middle management has decreased for example due to outsourcing of different kinds and it is not unusual that middle management is caught between top management and operations.

<table>
<thead>
<tr>
<th>Authority</th>
<th>IT Competence</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Management</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Middle Management</td>
<td>Middle</td>
<td>Middle</td>
</tr>
<tr>
<td>Staff</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

**Figure 5:** Authority, IT Competence, and Responsibility at different organizational levels.

**IT Security Risk Escalation**

One of the most important aspects of IT Security Risk Communication is the way risk escalation is handle. When handling incidents of different kind, each level has to consider if the incident would harm the acceptable risk level of the organization. Each level has basically three alternatives; you can accept the risk, you can try to mitigate the risk (risk treatment), or you can escalate the risk to the organizational level above. 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. One alternative for top management is to externalize the IT risk using insurance. The next figure shows the alternatives when incident are handled on different organizational levels.
Maturity Models

Humphrey et al. (1987) use Maturity Models for assessing software engineering capability of contractors. The following are example of the different Process Maturity Levels that are used.

1. **Initial**: The initial environment has ill-defined procedures and controls and the organization does not use modern tools and technology. Level 1 organization may have serious cost and schedule problems.

2. **Repeatable**: At Level 2, the organization has generally learned to manage costs and schedules, and the process is now repeatable. The organization uses standard methods and practices for management.

3. **Defined**: In Level 3, the process is well characterized and reasonably well understood. The organization has made a series of organizational and methodological improvements.

4. **Managed**: In Level 4, the process is not only understood but is quantified, measured, and reasonably well controlled. The organization typically bases its operating decisions on quantitative process data and tools are used increasingly to control and manage the design process.

5. **Optimized**: At Level 5, organizations have not only achieved a high degree of control over their process, they have a major focus on improving and optimizing its operation.

Example of using Capability Maturity Model as a vehicle for software process improvement that helped Motorola is described by Diaz et al. (1997).

The People CMM’s (Capability Maturity Model) primary objective is to improve the capability of the workforce and is an organizational change model (Curtis et al. 2002). The People CMM is a process-based model and provides a roadmap for transforming an organization.
Pöppelbuß et al. (2011) describe three design principles for maturity models:

- **Descriptive**, where the maturity model is used as a diagnostic tool and the assigned maturity levels can then be reported to internal and external stakeholders.
- **Prescriptive**, where the maturity model serves a prescriptive purpose and indicates how to identify desirable maturity levels and provides guidelines on improvement measures.
- **Comparative**, where the maturity model serves a comparative purpose and allows internal or external benchmarking.

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 (2012) describes how to integrating E-government deployment maturity model with new maturity models concerning IT security. The Risk IT Framework (ISACA 2009) presents how maturity models could be used to recognize on what maturity levels different processes are. These maturity models have been use as a base for our own maturity model which is discussed in more details later in this paper.

Puhakainen present an overview of different Information Security Maturity approaches. Example of other approaches than the one mention above, are approaches made by Al Aboodi, Chapin and Akridge, Mayer and Fagundes, NIST, Stacey, Thomson and von Solms, Williams, and Woodhouse. The maturity levels in these approaches differ from three to nine levels. Puhakainen own approach use three maturity levels; (a) Novice, (b) Intermediate, and (c) Mature (Puhakainen et al. 2010).

**METHOD**

**Combined approach**

We will use the well-known ISO and NIST framework as a starting point. First we combined the both framework. The reason for this is that we claim that each organizational level use their own individual Risk Assessment / Risk Treatment, Risk Monitoring, and Risk Communication. With this as background, it is extremely important that the communication between the different organizational levels is working and that there are tools that can secure this.

After the first initial IT Security Risk Assessment and Risk Treatment which act as a base for the organization we believe that IT Security Risk Management exists at each organizational level. The first initial Risk Assessment / Risk Treatment is a collaboration between Tier 2 which have the knowledge what impact different threat will have and Tier 3 which have knowledge of different threats to the IT environment. The Risk Assessment / Risk Treatment are governed by Tier 1 perception of risk tolerance and the risk culture of the organization. In the next figure we describe our combination of ISO 27005 and NIST multitier framework and the basic steps that each organizational levels have consider when dealing with a new incident.
Figure 7: Combination of ISO and NIST framework.

The framework for each organizational level all consist of the following basic steps.

- Evaluate the new incident with IT Security Risk Assessment of some kind.
- In some cases mitigate the new risk (IT Security Risk Treatment) with help of new countermeasures or in some cases just accept the new risk.
- Use IT Security Risk Communication of the new risk to other organizational levels if necessary.

Operational level (Tier three) handles a lot of incidents. Examples are surveillance of IT systems, servers, and networks. Other examples are end users error reports etc. Incidents at next level, Middle Management level (Tier two), are such thing that could influence the business processes which Middle Management are responsible for. At Top Management level (Tier one) incident that concern the core mission of the organization and incident that might affect risk tolerance. Example of communication from the top level to lower levels is policy document of different kind.

**IT Security Incidents**

The figure below shows how different security metrics are analyzed with help of some kind of Risk Assessment and depending on the outcome determines if the incident should be accepted, resolved or escalated. Some of the questions one need to ask when handling possible incident are:

- Is it actually an incident?
- Is it a security incident?
- Are there multiple events and impacts?
- What immediate actions must be taken?
- Who must be notified?
- Is it becoming a disaster?
Figure 8: Handling of incident with help of security metrics.

An incident is an event that has a human root cause. All incidents are events but many events are not incidents. However in this paper we will consistently make use of the term incident. An incident is an observable change to the normal behavior of a system. A normal incident does not affect critical components and to not require participation of senior personnel.

Incidents are often handled by a Help Desk which may filter incidents before some incidents are sent to The First Responder who performs the preliminary analysis. In some cases senior technical resources are assigned to resolve an incident.

An escalated incident on the other hand affects critical production system and normally need participation of senior personnel. An emergency incident needs to be handle by an Emergency Response team. Escalation process can either be Technical or Management.

Methodology

Nolan was the first to present a descriptive stage-theory concerning the planning, organizing, and controlling activities associated with managing the organizational computer resource (Nolan 1973). The methodology of our approach is based on scale-development theory. Once the scale is developed, it must be tested for validity and reliability. Scale development in this study consists of three stages. 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. The reason we choose Capability Maturity Model as a base for modeling IT Security Risk Escalation is that escalation routines are a combination of processes and tools and to handle this combination we will use Maturity Models to be able to measure the maturity level of different organization.
ARTIFACT DESCRIPTION

IT Security Risk Escalation Maturity Model

According to Philips (2003) 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” (p. 3). We present here a first draft to an IT Security Risk Escalation Capability Maturity Model. We will use ISACA’s Risk IT Framework (2009) as a starting point when we defined our model and will use the following maturity levels:

0. Non-existent when processes are not applied at all.
1. Initial when processes are performed ad hoc and disorganized.
2. Repeatable when processes follow a regular pattern.
3. Defined when processes are documented and communicated
4. Managed when processes are monitored and measured.
5. Optimized good practices are followed and automated.

Our model is built around the following attributes:

- Awareness and communication.
- Responsibility and accountability.
- Goal setting and measurement.
- Policies, standards and procedures.
- Skills and expertise.
- Tools and automation.

Escalation can be of both technical and management types which will affect some of the attributes as both need be fulfilled to reach the maturity level. The escalation maturity model consists of maturity levels and different attribute. Some of the attribute our more technical oriented like Tools and Automation. Let us look at the different attribute in our escalation maturity models and what implications this could have for various organizations.

First we have Awareness and Communication where requirements for responding to risk are the main issues. Next attribute, Responsibilities and Accountability, it is very important that different roles are clearly defined and some kind of job descriptions exist. It is vital that both technical and management responsibilities are covered.

For Goal Setting and Measurement attribute, reporting is the main issues and which organizational level reports are reaching. Policies, Standard and Procedures attribute is especially important, for example that policies and standard are defined and documented.

Skills and Expertise attribute main issue is education in different form. Both technical and management skill requirements need to be defined and documented and a formal training plan should exist. The last attribute, Tools and Automation, the degree of automation play a vital part for example the use of workflow tools.
Table 1. IT Security Risk Escalation Capability Maturity Model

<table>
<thead>
<tr>
<th>Maturity level</th>
<th>Awareness and Communication</th>
<th>Responsibility and Accountability</th>
<th>Goal Setting and Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-existent</td>
<td>Does not recognize the need</td>
<td>Does not recognize the need</td>
<td>Does not recognize the need</td>
</tr>
<tr>
<td>Initial</td>
<td>Minimal individual awareness of threats</td>
<td>No support for individual responsibility and minimal accountability</td>
<td>Minimal reporting to management</td>
</tr>
<tr>
<td>Repeatable</td>
<td>Individual awareness of threats</td>
<td>Roles only partially defined and contain overlaps. Confusion about responsibilities and a culture of blame tends to exist</td>
<td>Regular manual reporting to local management</td>
</tr>
<tr>
<td>Defined</td>
<td>General understanding and individual awareness of business impacting threats</td>
<td>Both technical and management roles are clearly defined and job description includes risk response responsibilities at each organizational levels. Both technical and management responsibility and accountability are defined at each level</td>
<td>Regular reporting to management</td>
</tr>
<tr>
<td>Managed</td>
<td>Individual understanding and awareness of requirements for responding to risk</td>
<td>Both technical and management responsibility and accountability are defined and accepted. A reward culture is in place that motivates positive action</td>
<td>Regular reporting to business management</td>
</tr>
<tr>
<td>Optimized</td>
<td>The organization is well aware of requirements for responding to risk</td>
<td>Employees at every level take direct responsibility and the organization collaborates with external entities</td>
<td>Reporting includes measure of effectiveness</td>
</tr>
</tbody>
</table>
Table 2. IT Security Risk Escalation Capability Maturity Model (continued)

<table>
<thead>
<tr>
<th>Maturity level</th>
<th>Policies, Standards and Procedures</th>
<th>Skills and Expertise</th>
<th>Tools and Automation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-existent</td>
<td>Does not recognize the need.</td>
<td>Does not recognize the need.</td>
<td>Does not recognize the need.</td>
</tr>
<tr>
<td>Initial</td>
<td>Minimal standards and policies exist but are not kept up to date.</td>
<td>Skills requirements exist on an ad hoc basis but are not actively developed. IT personnel lack skills to determine the business relevance and may force the organization to accept risk beyond tolerance level.</td>
<td>No workflow around incidents exists.</td>
</tr>
<tr>
<td>Repeatable</td>
<td>Policies and standards are established.</td>
<td>Minimum skill requirement are identified and some training is provided but is only provided in response of a need that occurs on the job.</td>
<td>Tools may exist but there is no coordinated approach.</td>
</tr>
<tr>
<td>Defined</td>
<td>Both technical and management policies and standards are defined and documented.</td>
<td>Both technical and management skills requirements are defined and documented and a formal training plan has been developed.</td>
<td>Workflow tools are used to escalate incidents between organizational levels.</td>
</tr>
<tr>
<td>Managed</td>
<td>Both technical and management policies and standards reflect business risk tolerance.</td>
<td>Both technical and management skill requirements are routinely updated and the effectiveness of the training plan is evaluated.</td>
<td>Automation of workflow tools.</td>
</tr>
<tr>
<td>Optimized</td>
<td>Both technical and management policies and standards are dynamically updated.</td>
<td>Continuous improvement of both technical and management skill requirements and training.</td>
<td>Real-time monitoring of risk incidents.</td>
</tr>
</tbody>
</table>

EVALUATION

Problem formulation
During the different eras in history of computing, from mainframe to cloud computing, IT Security Risk Assessment has almost remained the same and a number of adequate tools have been developed during the years. The main step that needs to be change is primarily IT Security Risk Monitoring as it is necessary to react fast on new threats and incidents. This means that also the third main step, IT Security Risk Communication between different organizational levels, also need to be changed so organizations have a well-documented and communicated monitoring and escalation processes.

Research Motivation
The overall motivation for our research is how to deal with changes inside or outside the organisation in a fast and efficient way to preserve an acceptable IT security risk level. This will involve IT Security Risk decisions on all organizational levels and are of vital importance.
to handle incidents that needs to be escalated. There is no need to reinvent the wheel for risk management but there is a needed to review and develop risk communication (escalation) and risk monitoring process at all levels in the organization.

The research goal for this study is to propose a framework that would facilitate organizations to effectively handle escalation of incidents. This is done by answering the following research question:

- How can the proposed framework be evaluated to effectively and appropriately meet the demands for IT Security Risk Manager?

**Choice of Research Methodology**

A generic research process (GROP) shown in the figure below will be used to guide the research work (Saunders et al. 2003). The GROP has the following layers: research philosophies and research approaches, research methods (choices) and strategies, research time horizons, data collection and analysis techniques.

![Figure 9: Generic Research Onion Process – GROP (Saunders et al. 2003)](image_url)

Research Philosophies assumption can be Positivism which assumes that reality is objectively given with measureable properties independent of the researcher, or Interpretivism that assumes that access to reality is subjective. As the goal of this research work is to develop a framework, Interpretivism is chosen as research philosophies.

Research Approaches are of deductive and/or inductive type. In the deductive research approach, knowledge are generating from theory. Inductive research approach on the other hand, deeper understanding of the real-world problem is the main issue often with the researcher as a part of the research process and therefore inductive research approach is chosen.
Research Methods (choices) and Research Strategies describe the way to collect knowledge either through observation (qualitative) and/or measurement (quantitative). Qualitative research methods involve such things as interviews and document reviews. Examples of qualitative research strategies are case-study, survey-study, and action research. Quantitative research methods use quantitative properties like statistical data. Mathematical-modelling and laboratory experiments are example of quantitative research strategies. A Qualitative research method is chosen and the selected research strategies are case-study, survey-study, and action research.

Time horizons can either be Longitudinal or Cross-sectional where Cross-sectional will be chosen. Technique and procedures for data collection and analysis are described in the next section.

**Research Steps**

The reason we chose a design science approach is that we want to develop an artifact where we can use different cases to validate our model. We will have a similar case in form of a scenario as described by Borell (Borell et al. 2013) that we will test on different organizations. Baron describe a number of cases in a Cloud Computing Environment (Baron et al. 2013) that can be used as an input to a scenario description. By using case studies to validate our model we will try to fill the gap between what you can do with IT and the way you can control as IT Security Risk Monitoring and Communication (escalation) have not kept up for today’s new type of computing. Another alternative that could be used are computer simulated scenarios that is described by Doner (Doner et al. 2008).

![Figure 10: Design research methodology (Vaishnavi et al. 2004).](image)

Design science research methodology consists of the following process steps. 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
Evaluation of Escalation Maturity Model for IT Security Risk Management

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. Our hypothesis is: “Organization with higher maturity level can handle incident in a more efficient way” (We will measure “handle” and “efficient” using independent observers). In the next section we will describe our research steps in more detail.

Research Cycle 1: Create an escalation maturity model.
- **Awareness of the problem:**
  - The gap between the various organizational levels concerning competence, authority, and responsibility is too big. Better escalation of incident between organizational levels will fill the gap of what you can do and the way you can control IT to keep up with today’s new type of computing (Proposal)
- **Suggestion:**
  - Better escalation routines (Tentative design)
- **Development:**
  - Design of the current escalation maturity model (Artifact)
- **Evaluation:**
  - IT Security Risk Specialists and Managers (5-10) representing different organizations will be asked for their ratings with help of the evaluation criteria and their comments of the maturity model will be noted by an observer in the form of field notes.
  - The selection criteria are private and public organizations plus academic security researchers.
  - The current maturity model will be the independent variable. Performance measures are the criteria described in the appendix which is the dependent variable. Here we will use the same methods as Karokola (2012) use to evaluated e-government maturity models.
- **Conclusion:**
  - If necessary the escalation maturity model will be improved. (Result)

Research Cycle 2: Build a tool and evaluate the escalation maturity levels within different organizations.
- **Awareness of the problem:**
  - Improved maturity model (Proposal)
- **Suggestion:**
  - Design a tool to handle maturity models (Tentative design)
- **Development:**
  - Build a tool based on the improved escalation maturity model (Artifact)
  - The tool will include a number of questions about the different attributes in our escalation maturity model.
- **Evaluation:**
  - We will test our tool in practice with number of individuals who claim to represent different organizational levels (strategic, tactical, and operational).
  - We will assist these individuals to self-evaluate their organize using a structure interview template.
  - The selection 2 – 4 organization will be of similar size and in both the private and public sectors.
The tool with the improved maturity model will be the independent variable. Performance measures are if the persons from same organization will have equal escalation maturity level for the organization which will be the dependent variable.

- **Conclusion:**
  - Adjust of the tool based on the evaluation (Result)

**Research Cycle 3: Confirm the hypothesis**

- **Awareness of the problem:**
  - Improved maturity model (Proposal)

- **Suggestion:**
  - Create cases to test the model (Tentative design)

- **Development:**
  - Design of cases involving incidents (Artifact)

- **Evaluation:**
  - The selection 2 – 4 organizations with different self-evaluate maturity levels.
  - During a half-day session, security people from each organization will evaluate how the organization will escalate the incidents. This will be judged by an independent observer preferably from an organization representing a regulator like Data Inspection Board or associations like ISACA and Swedish Standard Institute.
  - The organizations maturity level will be the independent variable.
  - Performance measures are if there is a correlation between that people from organization could handle an incident more efficient, and higher maturity level, which is the dependent variable.

- **Conclusion:**
  - Confirmation of the hypothesis (Result)

---

**Figure 11:** Research steps
DISCUSSION
Design science research can be divided into two type descriptive and prescriptive knowledge. (Gregor and Hiver. 2013). The knowledge contribution is of four types; (a) Routine Design, (b) Improvement, (c) Exaptation, and (d) Intervention. The contribution of this study will be of Improvement type which means to develop new solutions for known problems.

One important implication for an organization is to use the escalation maturity model as a base for a GAP analysis for finding key areas for action. In this way both technical and organizational shortage could be analyzed and if necessary corrected. Key areas can for example to improve skills and in form of education or deploy workflow tools to reach desired maturity level.

Organizations could be on various maturity levels for different attribute. It is very important to have a balance between the different attribute; all attribute need to be fulfilled before a new maturity level could be reached. The escalation maturity model could be used by an organization as a self-assessment tool to rate itself from least mature level (Non-existent) to the most mature (Optimized) and could in some cases also be used for benchmarking.

CONCLUSIONS
In conclusion one can say that there appear to be is no need to reinvent the wheel for risk management but there is a needed to review and develop risk communication (escalation) and risk monitoring process at all levels in the organization.

The most important contribution of our work is that IT Security Risk Management can be better adapted changes in the current situation of computing. The maturity escalation model could for example be used by organizations to understand where shortcomings exist and help define target and action to overcome these shortcomings which will reduce the social-technological gap.

REFERENCES
Ackerman, M. 2000. The intellectual challenge of CSCW : The gap between social requirements and technical feasibility. Human-Computer Interaction, 15(2), 179-203
Evaluation of Escalation Maturity Model for IT Security Risk Management


Philips, M. 2003."Using a Capability Maturity Model to Derive Security Requirements”, SANS Institute
Evaluation of Escalation Maturity Model for IT Security Risk Management


APPENDIX

Evaluation Criteria

<table>
<thead>
<tr>
<th>Framework Evaluation Criteria</th>
<th>Description of the statement</th>
<th>Ranking Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplicity</td>
<td>The framework is designed in such a way that it is clear and easily understandable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
<tr>
<td>Coverage and Completeness</td>
<td>The framework adequately addresses technical security issues.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The framework adequately addresses non-technical security issues.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The framework adequately addresses practice related security issues.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
<tr>
<td>Compliance to security standards</td>
<td>The framework is aligned with current security standards such as ISO 27001/2, NIST and ISACA.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
<tr>
<td>Dynamics &amp; flexibility</td>
<td>The framework is dynamic enough to deal with possible future risk and threats.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
<tr>
<td>Usefulness</td>
<td>The framework will be very useful to implementers when dealing with security related risks and threats.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
</tbody>
</table>