Maturity Modelling to Prepare for Cyber Crisis Escalation and Management

Grethe Østby[a] and Basel Katt[b]
Norwegian University of Science and Technology, Department of Information Security and Communication Technology, Gjøvik, Norway

Keywords: Crisis Management, Maturity Escalation Model, Maturity Models, Crisis Escalation, Maturity Model Evaluation.

Abstract: The aim of this study is to evaluate a newly developed maturity escalation model, that is based on ISO 27005 and ISO 27035 standards. The evaluation is done by applying the model to assess the maturity escalation level of an organization in the healthcare domain in Norway, which is called the Inland Hospital Trust. In this study, we applied several theories, including escalation management modelling. After using and analysing the maturity model in the healthcare organization context, we identified drawbacks of the current maturity escalation model, and suggest improvements.

1 INTRODUCTION

Recent industrial research report indicates that if an organization was to use technology alone to remediate security vulnerabilities, it would only solve 26 percent of the cyber security problem (Cisco, 2018). Consequently, it appears that in order to remediate a major part of the problems, i.e. 74%, social or socio-technical remedies need to be considered. Related socio-technical security research on incident handling and readiness of organization and society in general has focused on modelling and measuring incident maturity in organization and create new tools and programs to process and communicate security intelligence in organizations.

Although tools and programs have been implemented, Bruer research has shown that the current competence levels on digitalization process among leaders in the public sector in Norway has led computer security work to be isolated from strategic planning daily operation (Bruer, 2017). Consequently, upper management (leaders) are focused on efficiency, not to society readiness and emergency preparedness (Baugerød Stokke, 2009).

The Norwegian Auditor General's administration study number 1, 2018 about digitalization in governmental sector, concluded that the digitalization among departments and directorates is going too slowly (Office of the Auditor General of Norway, 2018). However, cyber security and safety are not mentioned in any part of the report, only personal information in the matter of how to transfer these data from one department to another. This is also underlined by governmental priorities.

"Norwegian health authorities have identified a common goal for ICT development in the Health and Care sector for the years to come: a health service where the patient is in the centre. E-health solutions allow for better communication and information flow between actors that interact regarding patients in the specialist health services and in the municipalities." Bent Høye, Norwegian Health minister

Digitalization appears to require more complex risk- and resilience analysis process than those that society has been using in the past (Haimes, 2009). Communication in public to enhance the understanding and the significance of cyber- security and safety within public services is therefore required to improve the awareness of the consequence's socio-technical cyber failures may have.

Current research indicates that governmental maturity in different departments and organizations within a country differs (Wahlgren & Kowalski, 2016), and that before generalized country wide cyber-security solutions can be adopted, there is a

[a] https://orcid.org/0000-0002-7541-6233
[b] https://orcid.org/0000-0002-0177-9496

Østby, G. and Katt, B.
Maturity Modelling to Prepare for Cyber Crisis Escalation and Management.
DOI: 10.5220/0008871602490256
In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*, pages 249-256
ISBN: 978-989-758-399-5; ISSN: 2184-4356

need to understand the current escalation maturity levels of relevant departments and organizations.

In the research this paper refers to, we have used an escalation maturity model newly developed by Wahlgren and Kowalski (Wahlgren & Kowalski, 2019) to test the level of maturity in the Inland hospital trust of Norway. As the model is newly developed and only tested in Sweden before, we aim to expand the use, and evaluate it usefulness to differentiate the maturity on different layers in an organization. We analysed the results of our study and compared them to similar research in Sweden. Furthermore, we evaluated the maturity model used, and we suggest some changes to the model to make it better usable for organizational improvement and vaster use.

After the introduction, in section 2, we present background and relevant literature. In section 3, we present materials and methods used in the test, before presenting the results from the test in section 4. In section 5, we discuss the results and the use of the model, to present conclusions and future directions in section 6.

2 BACKGROUND AND RELEVANT LITERATURE

There appears to be a disconnect between how risk is managed at the different levels in society. The National Institute of Standards and Technology (NIST) has ranged three different tiers in the framework of risk management. These tiers are strategic, tactical and operational (Locke & Gallagher, 2011). Wahlgren and Kowalski has used socio-technical methods to model and measure the degree of maturity between these different levels of Swedish government agencies (Wahlgren & Kowalski, 2019). The escalation maturity model is presented in figure 1.

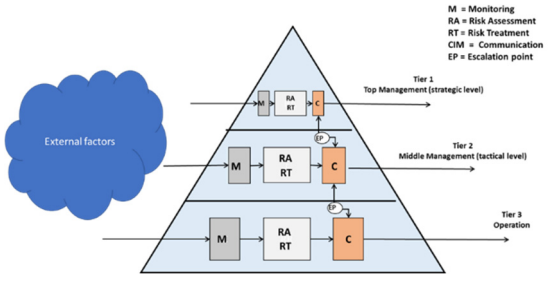

Figure 1: Escalation management model.

Risk assessment and risk treatment in the escalation model is based on ISO/IEC 27005, which provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review (ISO 27005, 2018). As Figure 2 illustrates, the information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment can increase the depth and detail of the assessment at each iteration. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that high risk is appropriately assessed.

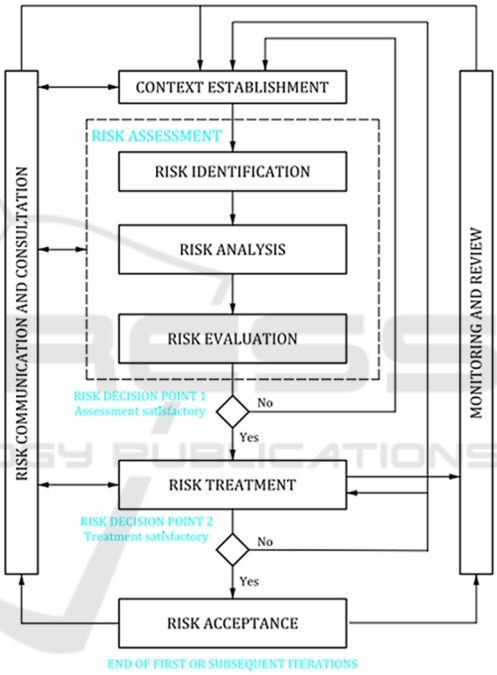

Figure 2: Information security risk management guidance.

The context is established first. Then a risk assessment is conducted. If this provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level, then the task is complete, and the risk treatment follows. If the information is insufficient, another iteration of the risk assessment with revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) is conducted, possibly on limited parts of the total scope (see figure 2, risk decision point 1). The effectiveness of the risk treatment depends on the results of the risk assessment. Responsibilities in Wahlgren and Kowalski model is based on ISO 27035 part 1 and ISO 27035 part 2,

especially the 27035 – 2, which gives guidelines to planning and preparedness for incident response.

To diffuse cyber-security awareness and prepare for cyber-incidents and exercise best practice, Wahlgren and Kowalski suggested the use of escalation maturity models research (Wahlgren & Kowalski, 2016). Maturity models have become popular in many industries since the development of the Capability Maturity Model for Software (SW-CMM).

A maturity model consists of a sequence of maturity levels for a class of objects. It represents an anticipated, desired, or typical evolution path of these objects shaped as discrete stages. In our context, these objects are organizations or processes. The bottom stage stands for an initial state that can be, for instance, characterized by an organization having little capabilities in the domain under consideration. In contrast, the highest stage represents a conception of total maturity (Becker, Knackstedt, & Pöppelbuß, 2009).

Additionally, maturity models outline characteristics associated with various levels of maturity, thereby serving as the basis for an organization's capability maturity assessment. The models serve to help organizations to understand their "as is" situation and enable them to transition to the desired "to be" maturity, through deriving and implementing specific practices or improvement roadmaps. These improvement maps support a stepped progression with respect to organizations capabilities, enabling them to fulfil the characteristics required to meet specific maturity levels (Carcary, 2012).

If a maturity model is purely descriptive on progression though, the application of the model would be single point encounters with no provision for improving maturity or providing relationships to performance. This type of model is good for assessing the here-and-now i.e. the as-is situation. A prescriptive model provides emphasis on the domain relationships to business performance and indicates how to approach maturity improvement in order to positively affect business value i.e. enables the development of a road-map for improvement (Bruin et al., 2005). De Bruin suggest 6 phases to successfully implement the use of maturity-models: 1. Scope, 2. Design, 3. Populate, 4. Test., 5. Deploy and 6. Maintain.

3 RESEARCH APPROACH

In this paper, we approach the challenges mentioned in the introduction, using what can be referred to as a naive inductivist approach. The naïve inductivist approach starts by first observing a phenomenon and then generalizing the phenomenon which leads to theories that can be falsified or validated (Kowalski, 1994). This approach will use the methodology outlined by design science research in information systems (DSRIS) (Kuechler & Vaishnavi, 2012). This methodology uses artefact design and construction (learning through building) to generate new knowledge and insights into a class of problems.

DSRIS requires three general activities: (1) construction of an artefact where construction is informed either by practice-based insight or theory, (2) gathering of data on the functional performance of the artefact (i.e., evaluation), and (3) reflection on the construction process and on the implications the gathered data (from activity (2)) have for the artefact informing insight(s) or theory(s) (Kuechler & Vaishnavi, 2012).

How to work on these steps was presented in a thesis written by Karokola (Karokola, 2012). He visualized this approach as outlined in Figure 3. As we are approaching our work in a naive inductivist approach, we modified the logical formalism in the model from abduction to induction.

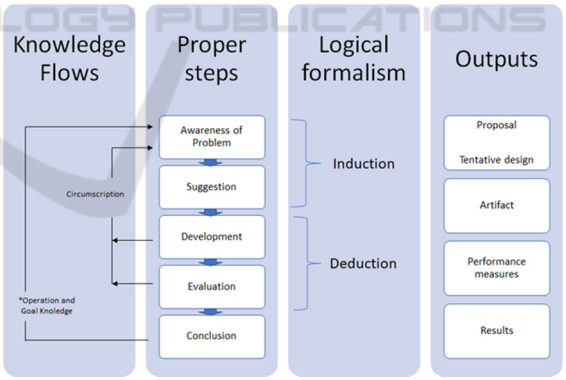

Figure 3: Design research methodology – modified.

To propose an artifact in an inductive approach, we started up by using a newly developed cyber-incident escalation maturity model to present the problem(first step in the 2nd column). We chose the model as it is based on socio-technical research in general, and more specific for managerial purposes. We also considered maturity models like EMRAM which is universally recognized maturation model of hospital's electronic medical record (EMR) environment (Ayat & Sharifi, 2016). However,

EMRAM is not considering information security and incident handling. We also considered resilience maturity modelling, but ultimately, resilience is not just about 'bouncing back from adversity' but is more broadly concerned with adaptive capacity and how to better understand and address uncertainty in our internal and external environments (Gibson, 2010).

For the next step in this research we asked the participants to test our suggested model (second step in the 2nd column). We then discussed further development of the model and evaluated the research in comparison with similar research in Sweden (third and fourth step in the 2nd column).

The goal of this paper is to build a best practice of using escalation maturity models research to diffuse cyber-security awareness and prepare for cyber-incidents and exercises (first and second steps in the 4th column), in which we want to use when preparing for cyber exercises at the Norwegian Cyber Range (NCR). NCR will be an arena where exercise will be used to expose individuals, public and private organizations, and government agencies to simulate socio-technical cyber security events and situations in a realistic but safe environment. We plan to evaluate our results when executing exercises for the Inland hospital trust.

3.1 The Escalation Maturity Model

A process in a maturity model can be assessed in more than one project (i.e., multiple instances of a process). All instances are aggregated in order to rate the process. Thus, increasing the number of process instances in assessment should not be interpreted as measuring organizational scope.

As shown in Figure 4, Wahlgren and Kowalski maturity model consists of a matrix whose rows represent different maturity levels and whose columns represent different maturity attributes. They used ISACA´s (ISACA, 2009) maturity model as a base for their model. The maturity levels are the same as the five maturity levels Humphrey et al. (Sweet, Edwards, Lacroix, Owens, & Schulz, 1987) used, and like ISACA they added a sixth level “Non-existent”. They used ISACA´s maturity attributes as a starting point but adapted them around escalation of IT-related security incidents. The main requirements for the escalation maturity model are:

- First, the incident must be detected
- If this should be possible, you must be aware that it is an IT-related security incident
- To be aware, knowledge of different incidents is required
- It is then necessary to know your responsibility for further handling the incident
- The next step is to handle the incident, which means that there must exist procedures that show how to behave
- These procedures must of course be anchored in a policy defined by the management
- If the incident shall be escalated directly, you must know to whom; that is, there must be predefined groups (organizational structure) that can handle the incident
- If the incident will be escalated later, there must be established reporting to the management
- There must exist means like appropriate risk analysis methods for analysing incidents

Attribute / Level	A Awareness	B Responsibility	C Reporting	D Policies	E Knowledge	F Procedures	G Means	H Structure
0 Non-existent								
1 Initial								
2 Repeatable								
3 Defined								
4 Managed								
5 Optimized								

Figure 4: Escalation maturity model.

Based on the requirements discussed before, 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 been 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 eight different maturity attributes:

A. Awareness deals with various aspects of how aware employees are of various IT-related security incidents.
B. Responsibility deals with allocation of responsibilities within the organization for IT-related security incidents.

C. Reporting deals with the reporting channels and how regular reporting of IT-related security incidents are done.
D. Policies deal with different policies for IT-related security incidents.
E. Knowledge deals with the different skills and knowledge that are needed for handling IT-related security incidents.
F. Procedures deal with various procedures for handling IT-related security incidents.
G. Means deal with various tools for handling IT-related security incidents.
H. Structure deals with various predefined groups for handling IT-related security incidents.

To measure the different attributes a query package of 67 questions were developed. The different questions have different maturity attributes and levels they belong to. All the different questions in the questionnaire have been defined on different levels, and program suggestions is defined for every question. After doing the test, every participant gets a report on what programs should be initiated based on their own answers to each question.

3.2 Information Letter and Consensus

Regulations made by Norwegian Centre for Research Data (NSD) require notification on personal data if it consist of any data relating to an identified or identifiable person whether you are going to process personal data, and how you are going to process personal data (NSD, 2019). The MM-escalation system required notification as the information could be stalked back to a person's identity if the information was charged on the stand-alone computer. Thereby NSD required an information letter and consensus from the participants, which was provided and signed by the participants.

4 RESULTS

In this paper we present the maturity levels for cyber security incident escalation performed in a study at the Inland Hospital trust, in May and June 2019. We present the results on each NIST-tiers, and the total result of the test. From the strategic level, three participants were randomly selected. From the tactical level, there were only two participants as it is only two tactical ICT-managers at the hospital trust. From the operational level, three participants were randomly selected. Thus, a total amount of eight participants took part in the study. All selected participants accomplished the test. The results are ranked on mentioned 6 levels, from non-existent (0) to Optimized (5). If a total value score of non-existent on the attribute, the participant will not be visible in the figures.

4.1 Strategic Participants Results

The results from the strategic participants show little variance within the group. Only on responsibility, and because of that, the total maturity level score is non-existent. The results clearly show a need for improvement on every attribute, even on organizational attributes, though this is what shows best results. The results are presented in Figure 5.

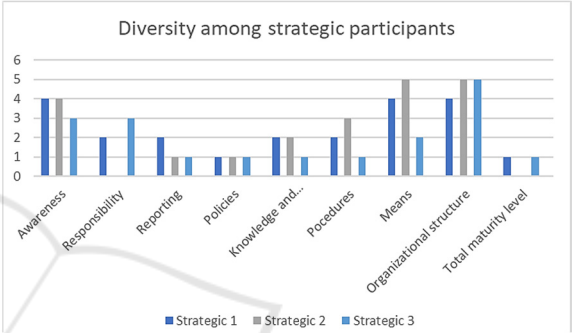

Figure 5: Maturity results on strategic level.

4.2 Tactical Participants Results

The results from the tactical managers were also aligned within the group. The results themselves were worse though. Non-existent results on responsibility, knowledge and education and procedures, gives us signals about major gaps in these areas. The results are presented in Figure 6.

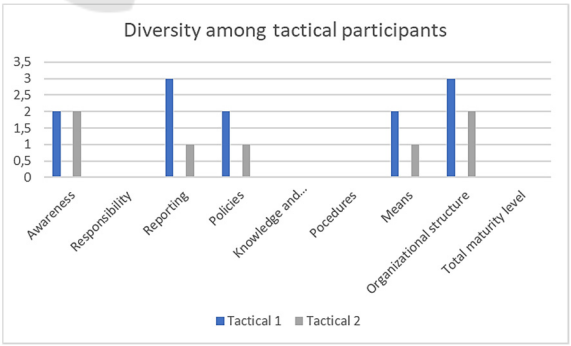

Figure 6: Maturity results on tactical tier.

4.3 Operational Participants Results

The results on operational tier is a little bit better than on the other tiers. The variance within the group is

bigger though. And still, knowledge and education are the weakest in this group. The results in this group is presented in Figure 7.

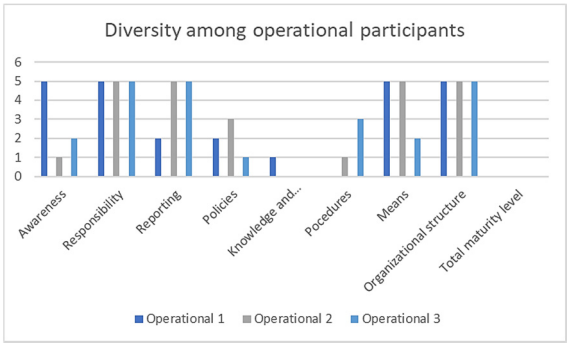

Figure 7: Maturity results on operational tier.

5 DISCUSSION

5.1 Results Analysis

When contracting all the results into one diagram, the results indicate that policy, knowledge and education are the weakest attributes. We know that the hospital trust has policies and guidelines on information security and emergency escalation, but the results might indicate that they are not well known. We also know that the hospital trust run educational programs on systems, but information from the hospital trust indicate that there is limited collective education on information security, except the annual reminder about change in passwords and limited relevant areas. Several innovative system-implementations take place at the hospital trust now, and we have suggested a couple of master-thesis' on information security attached to these innovation-projects, to do research on how the hospital trust follow up on their information security policies in such projects. As a result of our research, we also suggest new research on regularity and content of information security education.

Additionally, the results from the strategic participants suggests that reporting is barely initiated. The reason might be that ICT is outsourced to Sykehuspartner of which run the ICT-systems for all hospital trusts in Norway. This might have led to distance between the hospital trusts and the Sykehuspartner, and the incident and event reports are in internal systems in Sykehuspartner, and not necessarily accessible for the hospital trusts management on a regular basis.

Results from the tactical participants is the weakest, with three attributes on non-existent level. The other scorings are also low rated. The difference in the results from the other participants is that they suggest responsibility to be one of the non-existent attributes. Both responsibility, knowledge and education and procedures are scored as non-existent from all the participants at the tactical level. The low score on responsibility might come from the lack of role definitions and function description of these roles. To get a better grasp of this analysis, our future research will cover investigation on emergency and contingency plans. This might also be the fact for procedures, as emergency and contingency plans also should cover such issues.

Operational participants' scores are the highest. The difference from the other participants seems to be on awareness, even though one of the participants scores this up to Optimized. It is good to know that the operational team score high. That should mean that they will be able to manage their jobs. Still, they suggest that the awareness overall in the organization is weak, and that knowledge and education is non-existent. It would be of great importance for the organizations to work on knowledge and education, and hopefully this will bring better awareness to the organization as well.

As awareness came up as one of the weakest results in the test in total, but mostly on operational level, we run a quick security check on the hospital trusts open sources to see if these results could be confirmed also from such vulnerability scanning. We found at least 3 vulnerable and exposed IP-addresses. The hospital trust was immediately warned. The security check confirmed the results from the research, and open sources will be one of the issues we suggest focusing on during the training and exercises at the cyber range.

As the answers from the three layers in the organization are diverse (but comparable within the groups), we will prepare for the planned exercises adjusted to these facts. We plan to have collective instructions and separate instructions to meet the diversity. As this research is a part of a long-term research at the hospital trust, we will present these diverse suggestions on the weakest research results.

5.2 Results Comparison

When comparing our research approach with studies in Sweden, performed in 2019 (Wahlgren & Kowalski, 2019), we found the following differences: In Sweden 3 different organizations within the health sector did the test, but only one person (with relevant

Information security competence) from each organization. The results from the tests in Sweden varied a lot, from non-existed in one organization to almost optimal in another organization. This was the main reason for us to use the NIST-tiers to push forward several participants on all tiers. In our test, we see that on the different tiers the results are comparable, but there are differences between the tires. This shows us that it is necessary to do the test on all tiers to get the best possible picture to plan for further use of the results. Compared to other maturity models, e.g. the Community Cyber Security Maturity Model (CCSMM) (White, 2007), the Wahlgren and Kowalski model does not only look at the community measured as an entirety, but also when looking at different tiers in the organization, gives suggestions on what to do to improve the situation. In comparison to the CCSMM, the Wahlgren and Kowalski model also uses the ISO-standards for Information Security, like 27005 and 27035 to be in line with what is expected in cyber crisis management. Wahlgren and Kowalski escalation maturity model gives an overview of what should be done within each maturity attributes (as a part of the individual report), to improve the situation. The results vary from Non-excitant to Optimized on the same attributes, but we see that there is consensus on the different tires. Based on those results it will be important to divide program and action points between the different tiers, not only per participant.

In our analysis of the results, we intuitively focused on the weakest scores. It is also important to analyse the high scores, to find the strength of the organization, and how to keep and evolve that as well. After analysing the results, it is nevertheless important to prioritize which attributes to work with. We suggest presenting a suggested prioritization to the management board of which will select acceptable levels. When prioritized, an action strategy must be defined within the regulations of project management in the organization.

Next important step is how to implement the projects. As mentioned in or model-analysis, we suggest implementing plans at acceptable levels, both on information security acceptable levels and on human acceptable levels. When acceptable levels are decided, implementation should be applied step by step.

6 CONCLUSIONS AND FUTURE RESEARCH

Our research tested escalation MM at the Inland hospital to understand level of maturity to support diffusion of cyber security awareness and escalation, give good knowledge for preparation for the hospital trust exercises at the best possible level when executing at the Norwegian Cyber Range (NCR). We also conclude that the best use of the model is by testing maturity on both strategic, tactical and operational levels in the organization, and next to prepare for equalization amongst the tiers.

We also suggest an improvement maturity process with concrete improvement-suggestions on each maturity-step, which can be used for preparation for instructions in general and exercises in special. We also propose to use this process in instructions and exercises, to improve cyber security resilience step by step. We plan to use the improved maturity model to do a broad research within municipalities, and consequently we will suggest necessary development to contract and compare results from a connected database.

ACKNOWLEDGEMENTS

We would like to thank the Inland hospital trust for being all positive and welcoming to do this research. We would also like to thank Gunnar Wahlgren and Stewart James Kowalski for giving us the opportunity to use their newly developed maturity escalation tools. Additionally, we would also like to give a special thanks to Kieren Niċolas Lovell, RNorN RTD, for doing the vulnerability scanning on open sources at the hospital trust.

REFERENCES

Ayat, M., & Sharifi, M. (2016). Maturity Assessment of Hospital Information Systems Based on Electronic Medical Record Adoption Model (EMRAM)— Private Hospital Cases in Iran. *International Journal of Communications, Network and System Sciences*, *09*(11), 471–477. https://doi.org/10.4236/ijcns.2016.911038

Baugerød Stokke, O. P. (2009, March 23). Advarer it-sjefer mot effektivitet. *Computerworld.No*. Retrieved from http://www.cw.no/artikkel/enterprise/advarer-it-sjefer-mot-effektivitet

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management.

Business & Information Systems Engineering, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Bruer, A. (2017, August 9). Ny undersøkelse: Stort etterslep på mellomlederes IT-kompetanse i offentlig sektor. *Digi.No*. Retrieved from https://www.digi.no/artikler/ny-undersokelse-stort-etterslep-pa-mellomlederes-it-kompetanse-i-offentlig-sektor/398792

Bruin, D., de Bruin, S., de Bruin, T., Rosemann, M., Freeze, R., Kulkarni, U., & Carey, W. (2005). *Understanding the Main Phases of Developing a Maturity Assessment Model*. Retrieved from https://eprints.qut.edu.au/25152/

Carcary, M. (2012). *IT Risk Management: A Capability Maturity Model Perspective*. Retrieved from www.ejise.com

Cisco. (2018). *Annual cyber security report*.

Gibson, T. (2010). *Australian Journal of Emergency Management, Volume 25 Number 2, April 2010*.

Haimes, Y. Y. (2009). On the complex definition of risk: A systems-based approach. *Risk Analysis*. https://doi.org/10.1111/j.1539-6924.2009.01310.x

ISACA. (2009). The risk IT framework. Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

ISO 27005. (2018). *ISO 27005*. Retrieved from www.iso.org

Karokola, G. R. (2012). *A framework for Securing a-Government Services, The case of Tanzania*. Stockholm University.

Kowalski, S. (1994). *IT Insecurity: A Multi-disiplinary Inquiry*. Stockholm University.

Kuechler, W., & Vaishnavi, V. (2012). *A Framework for Theory Development in Design Science Research: Multiple Perspectives*. *Journal of the Association for Information Systems* (Vol. 13).

Locke, G., & Gallagher, P. D. (2011). *Managing Information Security Risk Organization, Mission, and Information System View JOINT TASK FORCE TRANSFORMATION INITIATIVE NIST Special Publication 800-39*. Retrieved from http://csrc.nist.gov/publications.

NSD. (2019). NSD. Retrieved from https://nsd.no/nsd/english/index.html

Office of the Auditor General of Norway. (2018). *admin report nb. 1*. Retrieved from https://www.riksrevisjonen.no/rapporter/Sider/Digitalisering.aspx

Sweet, H. W. L., Edwards, R. K., Lacroix, G. R., Owens, M. F., & Schulz, H. P. (1987). *A Method for Assessing the Software Engineering Capability of Contractors*. Retrieved from http://www.sei.cmu.edu

Wahlgren, G., & Kowalski, S. (2016). A Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents in Sweden. *Assosiation for Information Systems*.

Wahlgren, G., & Kowalski, S. (2019). *Business Information Systems*. (W. Abramowicz & R. Corchuelo, Eds.) (Vol. 353). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-20485-3

White, G. B. (2007). *The Community Cyber Security Maturity Model*.