LUND UNIVERSITY

# A Maturity Model for IT Dependability in Emergency Management

Weyns, Kim; Höst, Martin; Li Helgesson, Yeni

*Published in:*
Lecture Notes on Computer Science

*DOI:*
10.1007/978-3-642-13792-1

2010

Link to publication

*Citation for published version (APA):*
Weyns, K., Höst, M., & Li Helgesson, Y. (2010). A Maturity Model for IT Dependability in Emergency Management. In A. Babar, M. Vierimaa, & M. Oivo (Eds.), *Lecture Notes on Computer Science* (Vol. 6156, pp. 248-262). Springer. https://doi.org/10.1007/978-3-642-13792-1

*Total number of authors:*
3

**General rights**
Unless other specific re-use rights are stated the following general rights apply:
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.
• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Read more about Creative commons licenses: https://creativecommons.org/licenses/

**Take down policy**
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

LUND UNIVERSITY

PO Box 117
221 00 Lund
+46 46-222 00 00

LUND UNIVERSITY

Department of Computer Science

LUP

Lund University Publications
Institutional Repository of Lund University
Found at: http://www.lu.se

This is an author produced version of a paper presented at Product-Focused Software Process Improvement, PROFES 2010, 2010-06-21, Limerick, Ireland

This paper has been peer-reviewed but does not include the final publisher proof-corrections or journal pagination.

Citation for the published paper:
Kim Weyns, Martin Höst, Yeni Li Helgesson;
*"A Maturity Model for IT Dependability in Emergency Management"*
in Lecture Notes on Computer Science, 2010, v.6156., p. 248-262

DOI: http://dx.doi.org/10.1007/978-3-642-13792-1
Access to the published version may require subscription.
Published with permission from: Springer

# A Maturity Model for IT Dependability in Emergency Management

Kim Weyns, Martin Höst, and Yeni Li Helgesson

Department of Computer Science, Lund University
P.O. Box 118, SE-211 00 Lund, Sweden
{kim.weyns,martin.host,yeni.li_helgesson}@cs.lth.se

**Abstract.** In many organisations a gap exists between IT management and emergency managemement. This paper illustrates how process improvement based on a maturity model can be used to help organisations to evaluate and improve the way they include IT dependability information in their emergency management. This paper presents the IDEM3 (IT Dependability in Emergency Management Maturity Model) process improvement framework which focuses especially on the cooperation between IT personnel, emergency managers, and users, to proactively prevent IT dependability problems when the IT systems are most critical in emergency situations. This paper describes the details of the framework, how the framework was developed and its relation to other maturity models in related fields.

**Keywords:** Dependability, Emergency Management, Maturity Model, IT Management

## 1 Introduction

In recent years governmental actors have come to depend more on IT systems for all their everyday tasks. For communication, they depend on landline telephone networks, mobile phone networks, web servers, email servers, etc. Other important systems are used for patient administration in health care and social care, school administration or city planning.

Just as for their everyday tasks, governmental actors now depend on all kinds of IT systems for their responsibilities in crisis situations [1]. These systems include not only specially built systems for emergency situations but also the everyday systems described above. The latter category of systems is of special interest, because under normal conditions an occasional unavailability of these IT systems is fully acceptable, but in emergency situations, when time is a critical factor, any unexpected unavailability can have disastrous consequences [2], [3].

Therefore it is important that these IT systems are an integral part of all major risk and vulnerability analyses conducted. This way information about the dependability of the different IT systems can be combined with information about how critical the systems are in different situations [4]. IT dependability management for organisations with a critical role in emergency situations is a

complex process of managing software in terms of IT systems. The occurrence of a number of critical IT incidents in the recent past shows that there is room for improvement. Earlier research [5] has shown that there is a particular need for improvements with respect to the communication between emergency managers and IT-management. This is a complex problem for which no quick solutions exist that fit all organisations. Instead, organisational improvements in this area must be based on the organisation's current situation and its goals for the future, that is through a process improvement approach.

This paper presents a maturity model for the coordination of emergency management and IT dependability management. The main focus of the framework is on the cooperation between emergency managers and IT personnel. The purpose of this maturity model is to help organisations to identify, evaluate and improve their IT dependability processes.

## 2 Background

The maturity model presented in this paper is based on the result of a series of case studies on how governmental organisations deal with IT dependability issues in emergency management [3], [5]. The main conclusion from these studies was that many organisations today experience problems and frustrations concerning IT dependability in emergency management. The main cause of many of these problems could be traced back to communication and cooperation problems between the personnel in different roles involved. Further these studies also pointed out a lack of useful tools that support IT dependability improvements across a whole organisation. This maturity model is meant to offer a process improvement model that is simple and general enough to be applicable to many organisations and at the same time effective enough to make a substantial difference in an organisation's IT dependability practices.

## 3 Related Work

In the field of IT management a number of international standards and best practice frameworks have been published, among those ITIL [6], COBIT [7] and ISO/IEC 27002 [8]. These frameworks are more suited to be used by large corporations with very large IT resources and are less suited for smaller organisations and often do not take into account the special requirements for organisations with an operative role in crisis relief. Of these frameworks, COBIT is structured as a maturity model. Frühwirth [9] has discussed the mismatch of software dependability management and industry standards today.

The maturity model presented in this paper is based on a number of maturity models from related fields. The first successful maturity models were developed by the Carnegie Mellon Software Engineering Institute [10]. Since the development of the Capability Maturity Model, maturity models have been applied in many other fields. The problems between emergency management and IT management are related to some of the problems in software requirements

management and therefore the process improvement methods that have been successfully applied in software engineering can also benefit IT management.

In 2008, SEI published a preliminary version of the CERT Resiliency Engineering Framework [11] for the use in the field of business continuity management with a special focus on IT systems. In the field of IT management, Luftman [12] presents a simplified maturity model with a strong focus on the business value of IT systems. In the field of safety management, maturity models have also been proposed as a way of assessing an organisation's safety culture [2], or product design safety [13]. Section 8 focuses especially on how each of these maturity models relate to the maturity model presented in this paper. The maturity model presented in this paper does not try to replace any of these maturity models or to cover any of these related fields completely. From each related field, this maturity model contains only those attributes that are specifically important for the dependability of IT systems in emergency management.

Recently, Santos et al. [1] have published a maturity model for the use of information technologies in emergency response organisations. Their model does not cover the dependability of the IT systems in emergency situations, but instead focuses on information management practices. The IDEM3 maturity model described in this paper is most suited for an organisation where the IT services are provided by an IT department that is part of the organisation. For evaluating the resiliency of IT services provided by external suppliers, Bhamidipaty et al. have developed the Resiliency Maturity Index [14], a framework for characterizing and evaluating the resiliency of an IT services organization. However this model does not evaluate the relationship between the resiliency of the service supplier and the dependability requirements of the organisation.

## 4 Methodology

To support organisations that want to evaluate and improve their IT dependability practice, this paper presents the IDEM3 (IT Dependability in Emergency Management Maturity Model) process improvement framework.

The research that resulted in the IDEM3 maturity model was conducted in a number of steps: the identification of the attributes, followed by mapping the different levels of each of the attributes to the five levels of the maturity model, then an off-line validation and currently the maturity model is being evaluated in a practical setting. This process is presented in Figure 1.

First, the case studies [5] that describe the need for this kind of maturity model also resulted in a list of factors that are important for the coordination of IT dependability management and emergency management. These key factors formed the first basis for the attributes of the maturity model.

Secondly, the factors were mapped to the general architecture of a maturity model with five levels as found in other maturity models such as CMMI [15]. For the model to be applicable by small organisations, it was necessary to simplify the structure by replacing the concept of 'key process areas' by the more modest 'attributes' found in the model.

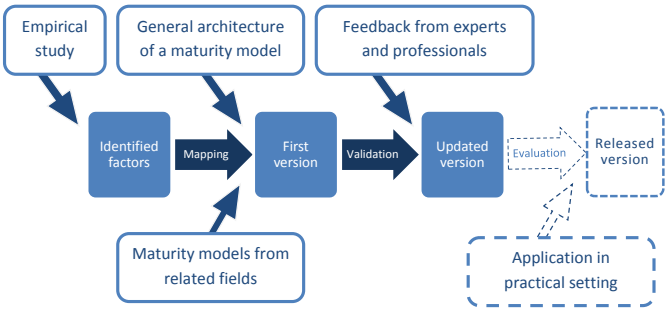


**Fig. 1.** Development process of the maturity model. Dotted lines indicate ongoing activities

In this mapping the attributes were also compared and complemented with similar attributes found in maturity models from related fields, as described in more detail in Section 8. Before the model was applied in a practical setting, the model was validated with the help of experts and practitioners in the field. Finally, the model is currently being evaluated through the application of the model in a series of large case studies. The validation and the first results from the evaluation are further discussed in Section 9.

## 5 Process Improvement with IDEM3

This section shortly explains how IDEM3 can be used as part of an organised process improvement effort. First, the model can be used to assess the current maturity of the organisation in dealing with IT dependability in emergency management. For this assessment the current practices in the organisation should be matched with the attributes described in Section 6. The recommended way to do this is to select some of the most critical systems, preferably systems that are quite different in nature and together are representative for the critical IT systems in the organisation. For each of these systems, personnel with different roles should be interviewed individually based on a detailed questionnaire, where they are each asked to describe how they are currently experiencing each of the attributes of the maturity model. The involvement of personnel from different parts of the organisation is an essential part of this maturity model to make sure that IT dependability is not only evaluated from a technical point of view. The interviews should at least include users of each of the systems, system managers, safety managers in the domain where the systems are used and of course IT personnel.

The responses from all these interviews should be analysed in detail by the process manager overseeing the assessment with special attention for differences between the answers of different respondents and between the different systems. The analysis of the interviews should then be the basis for a focus group meeting where the organisation can be assessed on the maturity scale for each of the

different attributes presented in the maturity grid shown in Table 1. The 22 attributes are ordered in such a way that attributes are most strongly correlated to those attributes just above and below. Therefore the maturity of an organisation in these 22 attributes can be presented in a spider web diagram, offering a clear representation of the organisation's strengths and weaknesses.

Finally, after this assessment, the organisation can decide whether the measured level of maturity is sufficient for the organisation. Not all organisations need to aim for the highest maturity level, mostly depending on how critical the role of the organisation is. The process improvement needed to reach a higher level of maturity is a long term project and should be organised as such. This means that a realistic time plan with explicit long and short term goals should be agreed upon. For the long term planning, it is important to realise that after each step from one maturity level to the next, some time is needed to make sure all procedures are well incorporated in the organisation and to make sure improvements are not too easily lost again. An improvement of more than one maturity level per year is probably unrealistic. Organisations should not try to skip certain levels or to implement a new level too quickly after the previous one since each level builds on the achievements of the previous level being well understood. For the short term planning, the organisation can focus most of all on those attribute for which they received the lowest maturity score. The organisation as a whole should focus on achieving a stable IT dependability management at this new maturity level. The actual improvements can be implemented with the help of those project management mechanisms that are most suited for the organisation in question. While implementing these planned improvements, it is important that regular critical self-assessments are held to evaluate the organisation's progress and to make sure the selected improvements are correctly implemented and are not easily lost again. A single assessment based on the IDEM3 maturity model can also be done separately from any planned process improvement based on the 5 maturity levels. An organisation can conduct a one-time assessment of its IT dependability based on this maturity model to identify its current strengths and weaknesses in this field. The results of this assessment will then form an excellent basis for a discussion on how to involve all stakeholders to improve the organisation's IT dependability in emergency management. Unlike with some other maturity models, IDEM3 assessment is not meant to be used as a basis for certification or for direct, objective comparison between different organisations.

## 6 Maturity Levels

Just like most other maturity models discussed in Section 3, the IDEM3 model has five maturity levels. The levels have similar names as in these other maturity models, and the basic idea behind each of the levels are also comparable. The Initial level is the most basic level, representing an organisation where some critical IT systems have not been analysed from a dependability point of view and nobody takes responsibility for initiating a more strategic discussion about

IT dependability. The second, Managed, level is characterised by an organisation where the dependability of all critical IT systems is managed on a system-by-system basis leaving the organisation very dependent on the competence of the system managers for every system.

The third level is referred to as the Established level. This means that the organisation has established a centrally coordinated approach for dealing with IT dependability. This will usually be established by appointing one central IT dependability manager who distributes standard procedures for dependability analysis to all system managers. A standardised approach is a prerequisite for being able to implement future improvements across the whole organisation. A level 3 organisation also has clearly defined roles and responsibilities concerning IT dependability. The fourth level, called Quantitatively Managed, is similar to level 3, but also requires that the centrally coordinated approach is supported by extensive quantitative data collection. Regular measurements and testing with special usage scenarios in mind can make IT dependability statistically predictable and allow for strategic improvements in IT dependability. The Continually Improving level, which is the fifth and final level of the maturity model, is reached by an organisation that can use the feedback obtained from the practices from level 4 to continually improve not only their IT systems, but also their own IT management procedures. IT systems will then be naturally included in risk and vulnerability analyses and their dependability will be regularly re-evaluated.

To define the levels in more detail the levels can be compared on 22 attributes. Of course all these attributes are in some way related and none of them can be changed completely independent of the others. Nevertheless they each add their own focus to the maturity model and stress a special aspect of an organisation's maturity.

The 22 attributes can be divided in 4 categories: Outcomes, IT management, Cooperation and Organisational Issues. A detailed summary of these attributes can be found in Table 1 and the attributes in each category are also described in the following subsections. The attributes are ordered in such a way that those attributes that are most strongly related are placed next to each other.

### 6.1 Outcomes

The first category of attributes is different from the three other categories in that it contains those attributes that can not directly be influenced by an organisation, but only indirectly. These attributes should mainly be considered as the consequence of an organisation's maturity, while the other categories are the causes of the maturity level. At the same time the outcome attributes are also the most important because the main goal of this maturity model is improving the outcomes of the IT dependability. This category also contains those attributes that are the most visible to stakeholders outside of the organisation.

The outcomes category contains 9 attributes: Actions taken, Problems that can be identified, Basis for improvements, Nature of improvements, Successes,

**Table 1.** Overview of the 22 attributes of the maturity model across the 5 maturity levels

| | | | Level 1: Initial | Level 2: Managed | Level 3: Established | Level 4: Quantitatively Managed | Level 5: Continually improving |
|---|---|---|---|---|---|---|---|
| Outcomes | 1 | Action | Reactive | Responsive | Preventive | Predictive | Pro-active |
| | 2 | Problems that can be identified | Failures | Technical system faults | Insufficient reliability, too high dependence and interdependencies | Faults in risk analysis | Faults in risk analysis procedures |
| | 3 | Basis for improvements | Fixing failures | Personal judgement | Standards | Quantitative risk analysis | Safety culture |
| | 4 | Improvements | Few, changes can be both positive and negative | For some systems, not sustained | For all systems, sustained | Regular, organised | Continuous |
| | 5 | Successes | Not repeatable | Repeatable | Sustainable | Measurable | Source for organisational learning |
| | 6 | Success factor | Luck, Competence of key personnel | Personal competence of system managers | Central coordination | Cooperation, Measurements | Continuous improvement effort by everyone |
| | 7 | Role of IT in emergency situations | Cause of problems | Varying between systems | Under control, backup solutions available | Predictable behaviour | Valuable asset |
| | 8 | Dependability problems | Accepted, create chaos | Solved on individual basis | Possible problems identified and prevented | Possible problems predicted and prevented in a prioritised way | Continuously prevented |
| | 9 | IT dependability | Low | Mixed | Stable | Controlled | Continually improving |
| IT management | 10 | Results of IT incident management | None | Improvement for one system | Improvement for all systems | Improvements in procedures | Improvement in organisational culture |
| | 11 | IT incident management | Ad-hoc | System-based | Formal incident management procedure | Basis for learning | Basis for deeper learning |
| | 12 | IT dependabiltiy management | Sporadic, Technical focus | Single initiatives, Techincal focus | Basic level, linked to requirements | Detailed level | Continuously improved |
| | 13 | Dependability Requirements | Unknown | For some systems | Documented | Measurable | continuously updated |
| Cooperation | 14 | Service Levels | None | For some systems | Basic service level for entire organisation and for all systems | SLAs with measurable service levels for all systems | Continuously evaluated SLAs |
| | 15 | IT dependability analysis and emergency planning | separate activities, not combined | Activities with a shared goal, contact for some systems | Input for each other | Measurable values exchanged, direct connection | Naturally combined activities |
| | 16 | Presence of IT dependability in emergency plans | not included | Included for some systems | Risk and vulnerability analysis for all IT systems included in plans | Measurable values included, regularly tested | Naturally included, continuously improved |
| | 17 | Relationship IT personnel - emergency managers | Conflict | Personal relations | Cooperation between departments | Cooperating, with shared risk and reward | Partnership |
| Organisational Issues | 18 | Involvement | Nobody | Individual system managers and some stakeholders | All internal stakeholders | All internal stakeholders, some external stakeholders | All stakeholders, internal and external |
| | 19 | Responsibility | 'Someone else' | Individual System managers | (delegated by) IT safety manager | Shared by System, Process, IT, and Safety managers | Everyone |
| | 20 | Management Mechanism | Sanctions | Warnings | Instructions | Guidelines | Education |
| | 21 | Organisational learning | None | Reactive ("Don't do that again") | Following rules ("Do like this"), Open loop | Following policy ("Think like this"), Single loop learning ("Improve what you do") | Double loop learning ("Improve the way you think") |
| | 22 | Resource allocation | Reactive, Ad hoc | To individual projects | Divided equally over the whole organisation | Divided in prioritised way | Optimized for best results |

Success factor, Role of IT in emergency situations, Attitude towards dependability problems and IT dependability.

These 9 attributes together describe the dependability experienced by an organisation at each maturity level, and how the organisation deals with these results.

A level 1 organisation will typically experience many problems with IT dependability and will focus most of its effort on trying to fix the problems as they appear. Because of the lack of an organized approach, some problems will not get solved and implemented changes can cause problems for other parts of the organisation. This will lead to a lot of frustrations, and although many of the minor problems will not come as a surprise, a serious failure in a critical system during an emergency situation can still do a lot of damage.

An organisation at level 2 will employ a system-by-system approach towards IT dependability allowing it to respond effectively to most of the problems and even to prevent some problems that only affect one system. Lessons learned from problems they experience will often lead to improvements in the affected system only as there is no centralised approach to IT dependability. This method of working leads to a higher dependability than in level 1, but places a large amount of responsibility on each system manager and much will depend on his skill and experience in dealing with the risks of IT dependability problems.

An organisation at level 3, on the other hand, uses a basic centralised approach towards IT dependability. The same basic techniques for risk and vulnerability analysis are applied to all systems and many dependability problems can systematically be prevented. Because of the coordination between different systems, also problems with interdependencies can be detected and dealt with. The main success factor from level 3 on will be the quality of the centrally coordinated dependability measures being used across the whole organisation. This will also make it easier for the organisation to efficiently share important resources such as backup facilities and emergency power supplies between all critical systems.

A level 4 organisation will supplement the basic centralised approach from level 3 with a large-scale systematic data collection and analysis concerning IT dependability. This will make IT dependability more predictable. The data collection will make it possible to measure improvements and their effects and to prioritise the usage of IT dependability resources. A level 4 organisation will also have an improved cooperation between all involved stakeholders which is an important factor for the IT dependability.

Finally a level 5 organisation will continuously work on evaluating and improving its IT dependability. The safety culture in an organisation at level 5 will even make it possible to regularly identify possibilities for improvement in their risk analysis procedures. At level 5, IT dependability is generally working very well and the level of success that can be achieved depends mostly on whether a continuous improvement effort can be sustained throughout the organisation. This makes that IT systems will not only be a source of risks or problems in emergency situations but also a valuable asset that can be depended upon.

### 6.2 IT Management

The second category of attributes collects those attributes that are directly related to IT management. Unlike some other maturity models, this maturity model does not seek to cover the complete field of IT management, but focuses exclusively on those aspects that are most important for IT dependability in emergency management. This category contains the following 4 attributes: Results of IT incident management, IT incident management, IT dependability management and Dependability requirements. A level 1 organisation lacks organised IT incident management, and the dependability requirements of most systems will typically never have been analysed. At level 2 incident management is handled for each system separately and for many systems there will be no explicit link to risk analysis or emergency management. A level 3 organisation is expected to have a centralised IT incident management system allowing information sharing between different parts of the organisation. Further centralised guidelines for IT dependability management will require the main dependability requirements for each system to be explicitly documented and available to all stakeholders. From level 4, IT incidents can be analysed in detail and can lead not only to direct improvement in all systems but also to improvements of the procedures used for IT dependability and even lead to improvement in the safety culture of the organisation at level 5. At the two highest levels of maturity dependability requirements for all systems should contain detailed measurable values and these requirements should be updated in the case of changes in the systems' functionality or usage.

### 6.3 Cooperation

A third set of attributes concerns the cooperation between the different parties involved in IT dependability. This is in the first place IT personnel, system managers, the system's users and also the personnel responsible for conducting risk and vulnerability analyses, for example emergency managers. The 4 attributes in the category are: Service level agreements, IT dependability analysis and emergency planning, Presence of IT dependability in emergency plans and Relationship IT personnel - emergency managers. A level 1 organisation will typically lack service level agreements or any other documents clearly linking IT dependability and emergency management. The frustrations and conflicts between different parts of the organisation will hinder a necessary cooperation on these important issues. In a level 2 organisation some of these issues will be taken care of for some systems, while there will be many problems with other systems, mostly depending on whether there are good contacts between the system manager of each system and the IT department. A level 3 organisation is expected to have basic, standardised service level agreements in place for all systems. Further, dependability estimates for all systems will be used as input for emergency management and the requirements discovered while making emergency plans will be used as input in the prioritising the IT dependability activities. From level 4 an organisation's SLA's should contain clear, quantitative dependability goals and

measurements. The link between dependability requirements and risk and vulnerability analyses for all systems should be explicitly documented. By clearly defining the responsibilities of all parties in detail, all successes will be shared success and when problems should arise the blame cannot just be shifted around as is often the case on the lower levels of maturity. Finally, in a level 5 organisations there is a real partnership between the different departments cooperating on IT dependability and continuously striving to improve their cooperation.

### 6.4 Organisational Issues

A last category of attributes collects those issues that concern the whole organisation and how it is managed. There are 5 attributes in this category: Involvement, Responsibility, Management Mechanisms, Organisational learning and Resource allocation.

In a level 1 organisation, in the worst case, nobody is actively involved with IT dependabilities and most stakeholders will feel the responsibility lies with someone else. After an incident, often the blame is shifted around and no learning takes place. In a level 2 organisation, the responsibility for IT dependability lies explicitly with the individual system managers who deal with the issue as they see fit. Therefore learning about IT dependability will mostly happen on an individual basis and improvements will depend on whether the system manager can find the resources to invest in IT dependability for each system. In a level 3 organisation, all the responsibility lies in the first place with central IT safety manager who is responsible for the coordination of IT dependability procedures. The IT safety manager distributes detailed dependability instructions and directions that are meant to be followed strictly by all stakeholders. This coordination allows the organisation to learn as a whole from past failures and successes. In a level 4 organisation, the detailed service level agreements for each system will make it possible for the responsibility to be shared by all actors in the IT dependability process. Through the detailed feedback from the collected data in a organisation at level 4, the organisation can achieve organisational learning by adapting its centralised procedures and guidelines based on measured outcomes. System managers are expected to be experienced enough to be able to apply the centralised guidelines and tools to manage IT dependability without detailed instructions. In level 5 organisations, not only the dependability guidelines are regularly updated, but also the way the organisation learns is continuously re-evaluated. This is called double-loop learning. In a well functioning level 5 organisation everyone will be aware of their own part of the responsibility for IT dependability and resources for improvements in IT dependability can be distributed in a prioritised way.

## 7 Transition from One Level to the Next

To further clarify the different levels of the maturity model, this section explains the main elements of the transition process from one level to the next. Although

not every organisation will be at level 1 initially, and not every organisation will aim for level 5, the levels are meant to be taken successively without skipping over any level. A transition from level 2 to level 4 can only be achieved by first implementing level 3.

### 7.1 From Level 1 to Level 2

There are no requirements for the first level of maturity, and at this level it is common that there are some critical IT systems for which there is no control over the dependability. For an organisation to rise to level 2 the responsibilities for each system need to be well defined. Usually this will mean that the coordination for all dependability issues is done by the system manager for each system who organises the work with dependability in the way that suits each particular situation best. The main advantage with this approach is the clear definition of responsibilities which makes that the main problems can be discovered and solved. The main disadvantage is that it is nearly impossible for the organisation to evaluate the quality of the dependability analyses done by the system managers since they each use their own methods.

### 7.2 From Level 2 to Level 3

To go from level 2 to 3, an organisation needs to standardize the way all system managers deal with IT dependability. First an organisational standard needs to be defined and then all system managers need to be instructed in this standard. The standard can be compiled based on national or international standards or on some of the procedures that were already previously used for some IT systems with good results.

### 7.3 From Level 3 to Level 4

While level 3 is mostly concerned with qualitative data about the dependability of IT systems, level 4 also requires the use of substantial amounts of quantitative dependability goals and measurements. A level 3 organisation might for example classify the availability requirements of a system according to a simple scale, Low-Medium-High, but a level 4 organisation is expected to use more detailed, numeric values. Setting up a central system to collect all service level agreements and to facilitate the analysis of all this data is a requirement for the transition from level 3 to 4.

### 7.4 From Level 4 to Level 5

Level 5 is characterised by a continuous effort to improve the processes in the organisation. This is only possible if the processes are well understood throughout the whole organisation and even across the borders of the organisations to include suppliers and network operators. To go from level 4 to 5 all procedures

from level 4 need to become completely institutionalised throughout the organisation and all stakeholders need to be working together in a natural way. This way the data collected can form the basis for deeper, double-loop learning for the organisation. This means the lessons learned are not only used to improve the organisation's dependability practices but also to optimise the improvement process itself.

### 7.5 Commitment Required

It should be clear that there is a large difference between the commitment and resources required of an organisation to reach each level of dependability. Level 1 represents the lowest commitment to IT dependability. Becoming a level 2 organisation only requires a serious commitment from the individual system managers who needs to drive IT dependability forward and need to collect input from all other personnel involved. Reaching level 3 maturity requires a regular commitment from all personnel involved with IT dependability to maintain a basic level of IT dependability across the whole organisation. Level 4 is very similar, but requires a larger effort for data collection and analysis. Reaching and sustaining level 5 maturity definitely requires the largest overall commitment to IT dependability, although in practice all efforts for IT dependability should feel more as a natural part of the daily workings of the organisation than as a special effort for IT dependability.

## 8 Relation to Other Maturity Models

As mentioned before, the maturity model presented in this paper is based on a number of maturity models from related fields. Table 2 illustrates how the attributes in the IDEM3 model correspond to similar concepts in these maturity models. For most attributes, similar maturity levels as in IDEM3 can also be found in one or more of these maturity models. The compatibility of the IDEM3 model with each of these models not only makes it easier to combine the usage of this model with the other models, it also increases the validity of each of the attributes and therefore of the whole model. IDEM3 does not in any way try to be an alternative for any of the models presented below, but has a different, very specific focus that is not explicitly present in any of the other models.

Of course, not all attributes can be matched with corresponding areas in all other maturity models. This can be for a number of different reasons. First of all, each of the maturity models referred to here has its own scope, which only partly overlaps with the scope of this maturity model. Therefore there are, for example, no attributes concerning IT management in maturity models from the area of design safety. When an attribute is clearly outside the scope of a certain maturity model, this is marked in Table 2 as n.a., not applicable. Secondly, there are some attributes that are not explicitly mentioned in certain maturity models, for example, organisational learning in all but one of the models. Such attributes are nevertheless generally compatible with these models, they were

| | | | Luftman | COBIT | CERT REF | DCMM | Safety Culture | Comments |
|---|---|---|---|---|---|---|---|---|
| Outcomes | 1 | Action | n.a. | n.a. | concepts used, but not as exact | =Approach | - | idea taken from DCMM |
| | 2 | Problems that can be identified | n.a. | n.a. | - | - | - | Own input |
| | 3 | Basis for improvements | n.a. | n.a. | n.a. | ~ Practice used in decision making | = part of Safety Culture | Adapted from DCMM, original from UKOOA |
| | 4 | Improvements | n.a. | n.a. | - | - | - | from CMMI |
| | 5 | Successes | - | - | discussed in organisational characteristics, but different levels | in level descrtiption | - | from CMMI |
| | 6 | Success factor | - | - | similar idea in level description | - | - | adapted from CERT |
| | 7 | Role of IT in emergency situations | ~ business perception of IT value | - | n.a. | n.a. | n.a. | adapted from Luftman |
| | 8 | Dependability problems | n.a. | - | discussed in organisational characteristics, but different levels | - | = part of Safety Culture | idea taken from SCMM |
| | 9 | IT dependability | n.a. | n.a. | in organisational characteristics | n.a. | n.a. | adapted from CERT res |
| IT management | 10 | Results of IT incident management | - | - | - | n.a. | n.a. | Own input |
| | 11 | IT incident management | - | DS8 | Incident Management and Control, no levels | n.a. | n.a. | Own input |
| | 12 | IT dependabiltiy management | n.a. | DS4, DS5 | in organisational characteristics | n.a. | n.a. | adapted from CERT res |
| | 13 | Dependability Requirements | n.a. | - | in organisational characteristics + Resiliency Requirements | Key process area | n.a. | adapted from CERT res |
| Cooperation | 14 | Service Levels | = part of Competency/value measurements | DS1 | - | n.a. | n.a. | idea taken from Luftman |
| | 15 | IT dependability analysis and emergency planning | = part of Competency/value measurements | part of PO9 | in organisational characteristics | n.a. | n.a. | idea taken from Luftman |
| | 16 | Presence of IT dependability in emergency plans | = part of Competency/value measurements | part of PO9 | in organisational characteristics | n.a. | n.a. | idea taken from Luftman |
| | 17 | Relationship IT personnel - emergency managers | = Partnership | P04.15, no levels | n.a. | n.a. | n.a. | idea taken from Luftman |
| Organisational Issues | 18 | Involvement | ~ part of Scope | consistent with PO4 | attribute discussed in organisational characteristics, but different levels | - | similar idea present | adapted from Luftman |
| | 19 | Responsibility | n.a. | consistent with PO4 | attribute discussed in organisational characteristics, but different levels | - | = part of Safety Culture | adapted from SCMM |
| | 20 | Management Mechanism | - | - | - | Even more levels present | - | Selection of DCMM, original source not found |
| | 21 | Organisational learning | - | - | - | Key process area | - | idea taken from DCMM |
| | 22 | Resource allocation | - | PO05 | in organisational characteristics + Financial Resource Management | n.a. | n.a. | adapted from COBIT |

**Table 2.** Traceability of the attributes of the maturity model to other maturity models [12], [7], [11], [13], [2]

just not selected as process areas or explicitly used in the description of the different maturity levels. This is marked in Table 2 with a minus sign (-).

## 9 Evaluation of the Maturity Model

IDEM3 is the result of a long development process during which many of the details of the model have regularly been updated. The model has been evaluated and validated in a number of ways. First of all, the case studies [5] provide an empirical grounding [16] and the relationships with in well-established maturity models are a strong external theoretical grounding [16] of the maturity model.

For a further external validation, IDEM3 has, at a number of different occasions, been presented in detail to researchers and practitioners with long experience in the field, such as representatives of the Swedish Civil Contingencies Agency. At each of these presentations the model has received a positive reception, and many practitioners, both from the field of IT dependability and emergency management have expressed an interest in putting the ideas of this model into practice. Their comments and recommendations, both on the form and the details of this model, have all been taken into account in the version presented in this paper.

Further, the model is currently being used to assess certain aspects of IT dependability at two Swedish hospitals and to formulate improvement suggestions. First results of this assessment and the improvements suggested by the model were very positively evaluated by the participating organisations. These four rounds of evaluations give us confidence that the model in its current form can be an effective tool in improving an organisation's IT dependability in emergency management. The final validation of this model, in the form of a large-scale implementation of this model at a number of organisations, is currently taking place. The practical evaluation of a complete maturity model is in no way an easy task, and proving that the model leads to an efficient improvement in an organisation's IT dependability requires a huge research effort.

## 10 Conclusions

This paper has shown that process improvement based on a maturity model can help organisations close the critical gap between IT dependability management and emergency management. The IDEM3 maturity model contains 22 attributes in four categories: Outcomes, IT Management, Cooperation and Organisational Issues. The model is based upon a number of established maturity models from related fields and upon a number of problems identified in an earlier case study.

The maturity model is not a quick fix that will solve all of an organisation's IT dependability problems. The main value of the maturity model is that it offers a way for an organisation to quickly capture its strengths and weaknesses in how it combines IT management and emergency management. IDEM3 can help an organisation to involve all stakeholders in this process improvement effort and to visualise it progress. The model has been evaluated and improved based

on feedback from experts and professionals in the field, and is currently being evaluated by case studies in the field of application.

## References


1. Santos, R.S., Borges, M.R.S., Gomes, J.O., Canós, J.H.: Maturity levels of information technologies in emergency response organizations. In Briggs, R.O., Antunes, P., de Vreede, G.J., Read, A., eds.: Collaboration Researchers' International Workshop on Groupware (CRIWG). Volume 5411 of LNCS., Springer, Heidelberg (2008) 135–150
2. Fleming, M.: Safety culture maturity model. Offshore Technology Report, 2000/049, HSE Books, Norwich, UK (2001)
3. Zimmerman, R., Restrepo, C.: Information technology (IT) and critical infrastructure interdependencies for emergency response. In: Proceedings of the 3rd International Information Systems for Crisis Response and Management (ISCRAM) Conference. (2006)
4. SEMA: Basic Level for IT Security. SEMA recommends 2003:2. Swedish Emergency Management Agency (2003)
5. Weyns, K., Höst, M.: Dependability of IT systems in municipal emergency management. In: Proceedings of the 2009 Information Systems for Crisis Response and Management (ISCRAM) conference. (2009)
6. Office of Government Commerce: Information Technology Infrastructure Library, Version 3. (2007)
7. ISACA: Control objectives for information and related technologies (COBIT) (3rd ed.). (2000)
8. International Organization for Standardization: ISO-IEC 27002: Information technology - Security techniques - Code of practice for information security management. (2005)
9. Frühwirth, C.: On business-driven IT security management and mismatches between security requirements in firms, industry standards and research work. In Bomarius, F., Oivo, M., Jaring, P., Abrahamsson, P., eds.: PROFES. Volume 32 of Lecture Notes in Business Information Processing., Springer (2009) 375–385
10. Konrad, M., Chrissis, M.B., Ferguson, J., Garcia, S., Hefley, B., Kitson, D., Paulk, M.: Capability maturity modeling at the SEI. Software Process: Improvement and Practice **2** (1996) 21–34
11. Caralli, R.A.: Introducing the CERT resiliency engineering framework improving the security and sustainability processes. Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA (2007)
12. Luftman, J.: Managing the Information Technology Resource: Leadership in the Information Age. Prentice-Hall (2003)
13. Strutt, J., Sharp, J., Terry, E., Miles, R.: Capability maturity models for offshore organisational management. Environment International **32** (2006) 1094–1105
14. Bhamidipaty, A., Lotlikar, R., Banavar, G.: RMI: a framework for modeling and evaluating the resiliency maturity of IT service organizations. IEEE International Conference on Services Computing (SCC 2007) (2007) 300–307
15. SEI: Capability Maturity Model Integration, Version 1.2. Volume CMU/SEI-2006-TR-008(2008). Carnegie Mellon Software Engineering Institute (2008)
16. Ågerfalk, P.J.: Grounding through operationalization - constructing tangible theory in IS research. In: European Conference on Information Systems (ECIS) 2004 Proceedings. (2004)