An Enterprise Risk Management framework for evaluation of eMaintenance

Peter Söderholm
Trafikverket (Swedish Transport Administration)
Risk Manager
Box 809, SE-971 25 Luleå, Sweden
+46 (0)920 353 85
peter.soderholm@trafikverket.se

Ramin Karim
Luleå University of Technology
Division of Operation and Maintenance Engineering
SE-971 87 Luleå, Sweden
+46 (0)920 49 23 44
ramin.karim@ltu.se

ABSTRACT

Maintenance is one approach to manage risk by a reduction of the probability of failure of technical systems and/or the consequences of their failure. However, history has shown that erroneous maintenance also can lead to reduced quality, incidents and accidents with extensive losses. Today, eMaintenance promises great opportunities for a paradigm shift from a rather narrow condition-based maintenance approach with focus on technical system health to a true risk-based maintenance approach that considers organisational excellence. This is achieved by proper information logistic solutions that address the needs of all stakeholders of the maintenance process, which are possible due to new and innovative Information & Communication Technology (ICT). However, all opportunities are also linked with some threats, which seldom are highlighted in the case of eMaintenance. In this paper, a risk management framework for evaluation of eMaintenance solutions is proposed. The framework is based on a combination of international standards (e.g. ISO 31000, ISO/IEC 27000, and IEC 60300-3-14) to achieve integrated Enterprise Risk Management (ERM) and enable a linkage of eMaintenance to strategic goals of an organisation. The framework is illustrated in the context of the Swedish Rail Administration.

Keywords

Enterprise Risk Management (ERM), eMaintenance, information logistics, information security, ISO 31000, ISO/IEC 27000, IEC 60300-3-14, railway.

1. INTRODUCTION

Banverket (the Swedish Rail Administration), as all other authorities in Sweden, should be managed efficiently, take care of the state's resources, obey present laws and obligations, and present its performance in a reliable and fair manner; see SFS(2007:515) at Riksdagen (2010).

More specifically, Banverket is responsible for ensuring that the entire rail sector (railways, light rail systems and the underground) is developed in accordance with the transport policy objectives determined by the Swedish Parliament. The overarching transport policy objective is to guarantee provision of transport systems for citizens and businesses throughout Sweden which is socio-economically efficient and sustainable in the long term. (Banverket, 2009)

As infrastructure manager, Banverket is responsible for investment and maintenance of the national Swedish railway infrastructure. In 2008, Banverket's costs for railway maintenance were about five billion Swedish crones (SEK), which is an increase with 100 percent since 2002.

The volume and content of maintenance is decided upon during the long time planning, which also includes new investments in infrastructure. The present maintenance plan for railway infrastructure was decided upon in 2004 and is valid until 2015. Recently, the latest planning period was ended, which covers 2010-2021. One prerequisite for efficient maintenance management is that the information about maintenance needs and costs are reliable and sufficient. Otherwise, there might be an erroneous estimation of the needs and available resources can be used erroneously. Some of Banverket's challenges related to maintenance planning are:

- assessment of maintenance actions and their effect with regard to strategic goals;
- knowledge about the linkage between maintenance actions and the effect on travellers and cargo customers;
- knowledge about which factors that affect the need of maintenance;
- model and criteria for prioritisation of maintenance actions;
- overarching condition measures for different asset types;
- central information systems with relevant information.

The core of these challenges is shared with other sectors dealing with complex and critical technical systems, e.g. the aviation and process industries (see, e.g. Söderholm, 2005; Karim, 2008; Candell, 2009; and Ahmadi, 2010).

These challenges can to some extent be met by eMaintenance, which aims at the provision of information logistic solutions to all stakeholder of the maintenance process through utilisation of new and innovative Information & Communication Technology (ICT) (see, e.g. Lee, 2003; Levrat et al., 2008; Karim et al. 2008a, 2008b, 2009). However, in order to achieve a true risk-based maintenance approach that considers overarching strategic goals of an organisation, it is also necessary to apply principles, frameworks, processes, methodologies and tools from the risk management area.

The purpose of this paper is to describe a risk management framework for evaluation of eMaintenance solutions, to enable a linkage of eMaintenance to strategic goals of an organisation and

ISBN 978-91-7439-120-6

thereby facilitate an achievement of opportunities and an avoidance of threats.

2. STUDY APPROACH

Based on the stated purpose, the following research question was formulated: How can a risk management framework be used to evaluate opportunities and threats of eMaintenance solutions with regard to strategic goals of an organisation? Based on the criteria given by Yin (2003), a case study was selected as an appropriate research strategy to answer the stated research question. Due to accessibility and available resources, it was decided to study the current practices within Banverket, which also enabled the use of action research (see discussion in, e.g. Patel & Tibelius, 1987; Gummesson, 2000). Hence, the paper describes some of the context and practices of risk and dependability management within Banverket from a strategic point of view. However, during 2010 Banverket was phased out together with Vägverket (the Swedish Road Administration) and the Swedish Institute for Transport and Communications Analysis and their functions moved to the new governmental authority Trafikverket (the Swedish Transport Administration). Hence, due to one author’s involvement in the development work, there was a great opportunity to also study the development of risk management and its intended practices within Trafikverket, which mainly are based on the best practices within Banverket and Vägverket respectively. Empirical data has been collected through action research, interviews, document studies and observations. The analysis is based on relevant theories and practices, e.g. within risk, quality, dependability and information logistics. Finally, the paper has been reviewed by key informants and roles in order to verify its content. Some of the case study findings have also been tentatively validated through similar experiences from other eMaintenance-related case studies performed within the aviation and process industries.

3. REQUIREMENTS ON RISK MANAGEMENT

In Sweden all authorities have to identify hazards within their area of responsibility that can lead to damages or losses; see SFS(1995:1300) at Riksdagen (2010). Furthermore, the authorities have to estimate associated risks and their present and potential costs. Each authority shall make a risk evaluation and take proper actions for risk reduction or control. In addition, there are other external requirements related to risk management that Banverket and Vägverket have to obey by, e.g. regarding: environment; work environment; accidents prevention; fire and explosive hazards; electric power safety; security and peacetime crisis management; and internal control; see e.g. JvSFS (2007:2), SFS(2006:942), SFS(2007:604) at Transportstyrelsen (2010) and Riksdagen (2010). Hence, from a strategic point of view, a risk can be classified as any event or circumstance that has impact on the following (COSO, 2004; ESV, 2008):

- objectives that are aligned with and support the mission;
- operations with an effective and efficient use of resources;
- reliable operational and financial reporting;
- compliance with applicable laws and regulations.

In this complex context, Enterprise Risk Management (ERM) is a vital approach for an organisation to fulfil requirements and achieve its objectives.

4. PROPOSED RISK MANAGEMENT FRAMEWORK

One reason for the scattered practice of risk management within an organisation is that it has been developed over time and within many different areas in order to meet varied needs. However, the adoption of consistent processes within a comprehensive ERM framework strives to achieve integrated risk management that are effective, efficient and coherent across an organisation.

ERM provides principles and a framework that includes processes, methodologies and tools used by organisations to manage threats and seize opportunities related to the achievement of their objectives and value creation for its stakeholders. (CAS, 2003; COSO, 2004; ISO, 2009)

The proposed risk management framework promotes integrated ERM through an integration of risk-related areas such as: internal control, traffic safety, security, information security, health and safety, environment, quality, continuity management, work environment, dependability management, code of conduct, compliance, and insurance (see Figure 1).

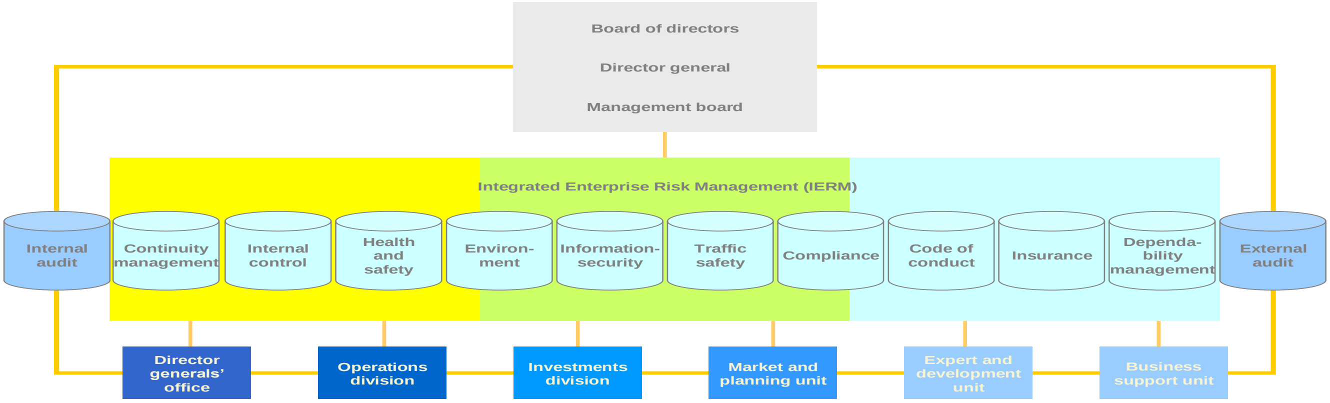

Figure 1. Proposed Integrated Enterprise Risk Management (IERM) framework, illustrated in the organisational structure of Banverket.

4.1 Principles and Framework

The proposed ERM framework adapts the "Plan-Do-Check-Act" (PDCA) model since it is a common framework for the ISO management standards covering important risk-related areas (see e.g. ISO 31000, ISO/IEC 27000, ISO-PAS 22399, OHSAS 18000, ISO 14000 and ISO 9000). Furthermore, the PDCA model can also be seen in the maintenance process described in IEC 60300-14, which has been used in the context of eMaintenance (see e.g. Karim et al. 2008a, 2008b, 2009). Even though the model is used in slightly different ways, its role is to highlight the importance of continuous improvement. Within ISO 27000 the PDCA model is applied to structure all Information Security Management System (ISMS) processes, where information security requirements and expectations of the stakeholders act as input, and necessary actions and processes produces information security outcomes that meets those requirements and expectations.

As an overarching standard for the proposed ERM framework the principles of ISO 31000 is selected, together with its definitions, which can be found in ISO Guide 73. The reason is that ISO 31000 is intended to harmonise risk management processes in existing and future standards. As a consequence, existing ISO-standards will adapt their risk-related vocabulary to ISO 31000 once they are updated. Hence, the use of ISO 31000 will support an integration of diversified risk-related areas. However, even though ISO 31000 provides a common approach to standards dealing with specific risks and sectors, it does not replace those standards. See Figure 2 for some standards that support an integrated ERM framework, with special emphasis on the context of eMaintenance.

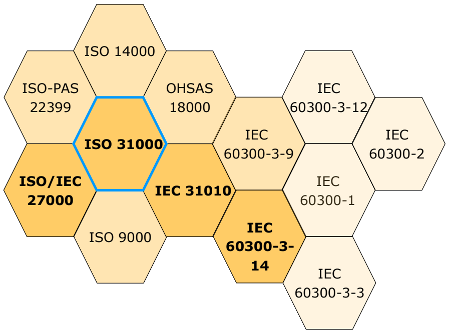

Figure 2. Integration and harmonisation of risk-related areas in different standards, with special focus on the context of eMaintenance.

Even though it is necessary to integrate different risk-related areas to achieve integrated ERM, it is not sufficient. The ERM framework should also support an integration of the risk management process into the organisation's overall governance, strategy and planning, management, reporting processes, and policies. To achieve this integration it is necessary to consider the management principles of the organisation. In the case of Banverket these management principles are primarily by objectives and results, and secondly by mission, where the latter can be divided into projects or administration. There are also other important management principles, e.g. management by rules due to the safety criticality of railways. These management principles are also reflected in the different types of risks described in Section 3. Hence, there are mainly four areas that Banverket's risk management framework should cover:

- Management system, i.e. the performance, effectiveness, and applicability of included processes, methodologies and tools.
- Objectives and results that are deployed from a strategic Banverket level to an individual employee level.
- Projects that range from 'large' investment projects (a budget of more than four billion SEK) to uncomplicated projects at an office.
- Administration (e.g. operation and maintenance) of everything from infrastructure assets to specific software tools.

To manage the deployment and escalation of risks throughout the different hierarchies of Banverket, different types of support are necessary, e.g. management models and software adapted for the balanced scorecard logic. One physical artefact that manifests this integration at Banverket is the document called 'Banverket's overall threats and opportunities analysis'. This document is based on threats and opportunities identified at Banverket's different divisions and units, which are evaluated at each organisational level and aggregated to the management board for final evaluation on a strategic level. The analysis is presented for the board of directors, which decide upon it and use it as one input to judge if they with reasonable insurance can state that they have sufficient internal control. The risks and controls of the analysis, as well as their suitability, are reviewed and updated by the risk owners at each quarter and by the board of directors on a yearly basis.

In addition, risk management also has to be integrated with intangible aspects such as organisational culture and values. One support to this integration is to apply methodologies and tools from the risk management area that support the values, see e.g. Hellsten & Klefsjö (2000), Akersten & Klefsjö (2003) and Söderholm (2004). A physical artefact that is intended to convey the board of directors' risk appetite is Banverket's risk management strategy, which includes principles and criteria for risk management to be used within the authority, but also by entrepreneurs and suppliers of Banverket, and thereby align the risk management culture and practice.

4.2 Process, Methodologies and Tools

Risk management may be as a process that are connected to the PDCA-framework and includes activities such as identification, analysis, evaluation, and treatment of risk (ISO, 2009). See Figure 3.

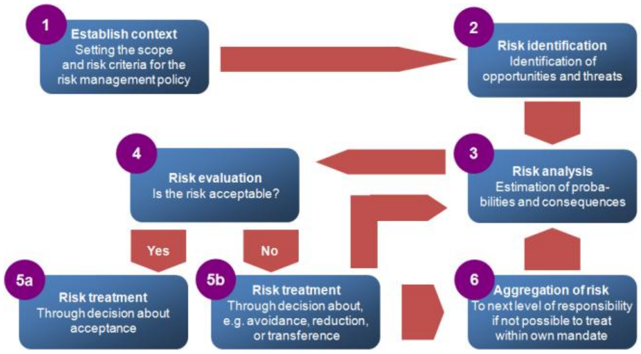
1
Establish context
Setting the scope and risk criteria for the risk management policy
2
Risk identification
Identification of opportunities and threats
4
Risk evaluation
Is the risk acceptable?
3
Risk analysis
Estimation of proba-bilities and consequences
Yes
No
5a
Risk treatment
Through decision about acceptance
5b
Risk treatment
Through decision about, e.g. avoidance, reduction, or transference
6
Aggregation of risk
To next level of responsibility if not possible to treat within own mandate

Figure 3. Risk management framework and process (adapted from ISO, 2009).

The evaluation aims at determining whether the risk should be modified by risk treatment in order to satisfy the risk criteria of an organisation. Throughout this process, the organisation communicate and consult with stakeholders, and monitor and review the risk and the controls that are used to modify the risk to make sure that no further risk treatment is necessary. (ISO, 2009a)

It should be noted that there are different roles responsible for activities within different phases of the process. These roles can be divided into two levels, i.e. a managerial level and an operational level. The managerial level is responsible for decisions related to phases 1, 4, 5 and 6, while the operational level are responsible for work related to phases 2 and 3. See, discussion in e.g. Palm (2008) and Ahmadi et al. (2010).

The process approach is common for the standards. Hence, risk management includes a process, as well as information security. However, also maintenance may be viewed as a process as described in IEC 60300-3-14, which is used by Karim et al. (2008a, 2008b, 2009) within the context of eMaintenance to emphasise information logistic aspects instead of technology. From an information security perspective, one aspect of the process approach is that the users are encouraged to emphasise the importance of (adapted from ISO/IEC 27000):

- understanding an organization's information security requirements and the need to establish policy and objectives for information security, which should be derived form the organisation's strategic goals;
- implementing and operating controls to manage an organisation's information security risks in the context of the organisation's overall business risks, and thereby be aligned with the controls of other risk management functions (e.g. dependability management);
- continuous improvement, based on objective measurement.

Examples of some methodologies and tools that can be used to support the risk management process can be found in 'IEC/ISO 31010: Risk management - Risk assessment techniques'. Other examples of supporting tools are copies of the standards them selves, primarily ISO 31000, ISO/IEC 27000, ISO-PAS 22399, OHSAS 18000, ISO 14000 and ISO 9000. These standards and guidelines was used by both Banverket and Vägverket, and the management system of Trafikverket is expected to be certified for ISO 9000, ISO 14000, ISO/IEC 27000 and OHSAS 18000.

On a more detailed level, the risk matrix for threats is one tool that Banverket uses in their risk management process for activities such as risk identification, risk analysis and risk evaluation. Presently there is a development of a risk matrix for the whole of Trafikverket, where criteria for assessment, acceptance, and escalation shall be decided upon by the board. Hence, this matrix will be included in the risk management strategy and reflects the risk apatite of the organisation and aligns its application of risk management, which contributes to integrated ERM. In order to further support integrated ERM, the consequence areas of the matrix reflects different risk-related areas, e.g. economy, reputation and image, health and safety, environment, and dependability. These areas can be seen as an expansion of the perspectives included in the balanced scorecard; see, e.g. Kaplan & Norton (1996).

The risk criteria included in the risk matrix are terms of reference against which the significance of a risk is evaluated. The criteria are based on organisational objectives, and external and internal context and requirements, e.g. standards, laws, and policies. A further development of the risk matrix is to make a mirror image of the threats' part into a part that illustrates opportunities. In this way both threats and opportunities are highlighted in the risk management process. This emphasis of bath threats and opportunities is also in line with the definition risk given in ISO 31000, which defines risk as the "effect of uncertainty on objectives", where an effect is a deviation from the expected, i.e. positive and/or negative (ISO 2009a, 2009b). However, this risk definition represents a fundamental change from most earlier risk-related standards (besides ISO-AS/NZS, 2009 and COSO, 2004), which emphasis the negative impact of risk, see e.g. earlier DoD, IEC, IEEE, ISO, and ITU standards. A further development would be to extend the most critical threats to cover crisis management, since the risk matrix developed so far is intended to evaluate risks in the context of 'normal' circumstances. See Figure 4.

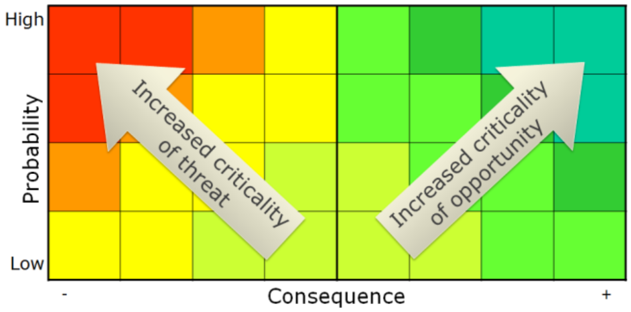
High
Low
Probability
Consequence
-
+
Increased criticality of threat
Increased criticality of opportunity

Figure 4. Risk matrix with threats and opportunities.

Here, it should be noted that risk evaluation from a traffic safety perspective often emphasise the negative consequence part of a risk. Hence, potential events with severe consequences are managed even though their probability is judged to be very small. This also highlights an important difference in the view of risk between different application areas; see, e.g. Rasmussen & Svedung (2000). For example, road traffic experiences relatively many accidents, where each accident has a relatively low level of consequences. Rail and air traffic experiences a smaller number of accidents than road traffic, where the accidents on the other hand tend to have more severe consequences. Finally, there are also application areas, such as nuclear power plants, where the number of accidents is very low, but where an accident may have very severe consequences. In the case of Trafikverket, it will be a major challenge to merge two different risk and safety cultures (i.e. road and rail traffic) and ensure that one culture is not affected by the other in a negative way, see Anderzén & Davidsson (2010).

When considering information security, it can be described by the triad Confidentiality, Integrity and Availability (CIA), which describes characteristics of information. An augmentation of the triad can include characteristics such as auditability/accountability, authenticity and reliability (see e.g., ISO/IEC 27000). The bow tie diagram of Figure 5 illustrates the relationship between information characteristics and strategic consequence areas.

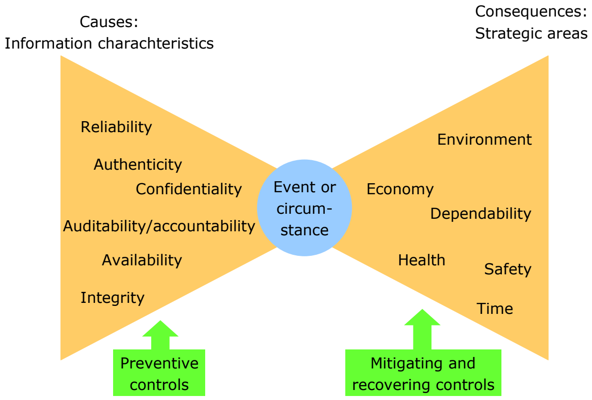

Figure 5. Bow tie diagram of information characteristics and strategic consequence areas.

The bow tie diagram is a fundamental model that is used as a tool within both Banverket and Vägverket to support activities in the risk management process, e.g. in the identification of threats and opportunities related to specific risks, but also in the selection of appropriate controls (e.g. influenced by the risk's position in the risk matrix). The logic of the bow tie diagram is also used in risk-based approaches within the dependability area; e.g. Reliability-Centred Maintenance (Nowlan &Heap, 1978; IEC, 1999) and MSG-3 (ATA, 2007).

4.3 Stakeholders of information

From a risk-perspective, there are three groups of stakeholders that should be considered, i.e. the Three Lines of Defence (TLD), see also Figure 5:

- the risk owners: day-to-day running of the operation and the front-office (cf. the two roles of the risk management process described in relation to Figure 3);
- the risk management functions: continuous monitoring of the business; and
- the audit: periodic checking of risk owners and risk management functions.

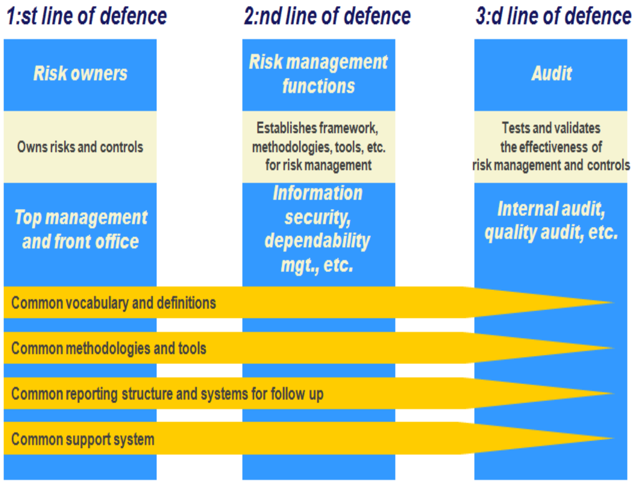
1:st line of defence
2:nd line of defence
3:d line of defence
Risk owners
Risk management functions
Audit
Owns risks and controls
Establishes framework, methodologies, tools, etc. for risk management
Tests and validates the effectiveness of risk management and controls
Top management and front office
Information security, dependability mgt., etc.
Internal audit, quality audit, etc.
Common vocabulary and definitions
Common methodologies and tools
Common reporting structure and systems for follow up
Common support system

Figure 6. Three Lines of Defence (TDL) as stakeholders of information logistic solutions.

To achieve integrated ERM it is necessary to avoid that the various forms of risk functions are carried out by different teams within separate risk silos (cf. description in relation to Figure 1). Integrated ERM relies on an overall enterprise-wide risk management framework and a collaborative process that pulls together and leverages all the various risk functions within an organisation (cf. discussion in relation to Figure 3). From a strategic eMaintenance perspective, this primarily includes risk functions such as internal control, information security and dependability management. However, the other risk management functions should also be involved.

While retaining overall responsibility for risk in predefined areas, the different risk functions can draw on each others' experience. This collaborative approach can also reduce wasteful duplication and promote information and knowledge sharing. This collaborative approach should ideally seek to identify the potential synergies between the various risk functions and help strengthen the overall risk management framework. However, the risk functions cannot delegate any of their monitoring tasks to internal audit as this would compromise the internal audit's position as an independent third line of defence (which includes monitoring of the risk management function).

4.4 Hierarchy of stakeholders, services and systems

Today's society is dependent on an increasing volume of transportation of both goods and passengers. This leads to steadily increase in the need of transportation volumes, as well as in requirements on economy, dependability, safety, and sustainability of the transports. To fulfil these needs and requirements, different modes of transportation have to be integrated and both their systems-of-interest (i.e. infrastructure and vehicles), enabling-systems (e.g. traffic control systems, traffic information systems, tracking systems, Built-in Test Equipment BITE and Computerised Maintenance Management Systems CMMS), and enabling services (e.g. information logistics, support, and maintenance) have to be streamlined and integrated to provide timely and effective transportation services.

One example of a national effort intended to achieve this desirable transformation of the transportation sector is the development in Sweden, where the integration of all modes of transportation are intended to be facilitated through the development of the Swedish Transport Agency and the Swedish Transport Administration.

The agency is working to achieve good accessibility, high quality, secure and environmentally aware rail, air, sea and road transport. The agency has the overall responsibility for drawing up regulations and ensuring that authorities, companies, organisations and citizens abide by them. (STA, 2009)

The administration is a public authority that takes on responsibility for long-term planning of the transport system for road, rail, maritime and air traffic. The administration is also responsible for the construction, operation and maintenance of public roads and railways (STM, 2009).

From a lifecycle perspective a system might be viewed as a system-of-interest or as an enabling-system. A system-of-interest is a system whose lifecycle is under consideration within a given context, while an enabling-system is a system that complements a system-of-interest during its lifecycle stages, but does not necessarily contribute directly to its function during operation (ISO/IEC, 2008). Analogously, a service might from a lifecycle perspective also be categorised as a service-of-interest or as an enabling-service, since a service is a set of functions offered to a user by an organisation (IEV, 2008). By this convention, transportation is a service-of-interest, while traffic control information is one example of an enabling-service. When regarding transportation as a service-of-interest, the mode of transportation is secondary and depends upon the context of the service consumer. This context is affected by available resources (e.g. time and money), capabilities of the transportation systems (e.g. speed and accessibility) and state of the surrounding environment (e.g. accidents and weather conditions). See Figure 7.

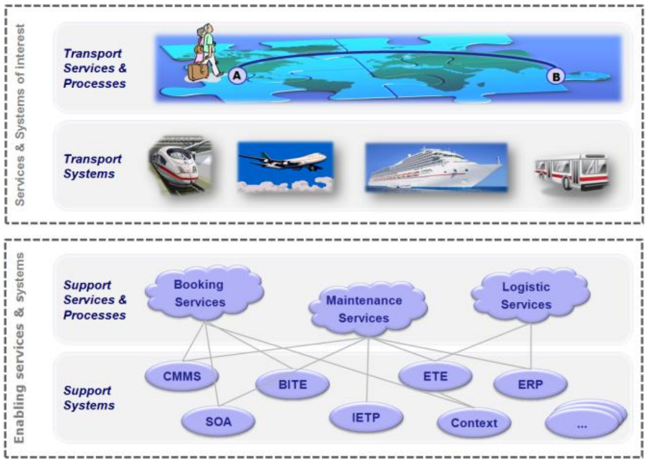

Figure 7. Relations between some different transportation systems and services.

One category of enabling-services is maintenance-related, which can be used to provide the service consumer with information that is related to maintenance and adapted to the consumer's current situation and needs. Maintenance-related information can be used to increase the effectiveness and efficiency of the transport services and system, but also to provide the consumer of the transport services situation-adapted information. For example, information about scheduled maintenance activities on an item within a transport system, e.g. vehicle and rail, can be used within the maintenance process to enable opportunistic maintenance in order to reduce the negative impact on current or planned transports as much as possible. Simultaneously, the same information can be correlated to spatial data in order to provide better decision-support for a route planning service aimed at the consumer of the transport service. Hence, the provision of information services can be considered as essential enabling-services that complement the transport services and contribute to increased satisfaction of the service consumer.

By application of an integrated ERM approach it is possible to apply a top-down approach that departs from overarching requirements on a service-of-interest, e.g. on accessible transportations that considers health, safety and environment. These requirements can in turn be used to identify systems-of-interest, enabling services, enabling systems and related requirements. Thereby, it is also possible to identify and integrate different risk management areas that address different aspects of the proposed hierarchy of systems, services and stakeholders (see Figure 7).

As one illustrative example, the winter of 2010 was unusually long and cold in Sweden, which had a negative impact on the rail traffic. Hence, travellers were faced with transportation services that experienced extensive delays and cancelled trains. One aspect that the travellers judged as very unsatisfactory was the information that they received related to their planned journey. Hence, real time traffic information is a service that the end customers, e.g. travellers and cargo customers, considers as very valuable.

The unsatisfactory traffic situation during the winter exemplifies the benefits of integrated ERP. For example, continuity planning is pivotal to ensure adequate quality of the service of interest by being able to manage long and harsh winter conditions, e.g. through an identification of risks, threats and vulnerabilities throughout all levels of the hierarchy. One important part in this context is technical systems (both systems-of-interest and enabling systems), which is the focus of dependability management. Simultaneously, information is one pivotal service (both as service-of-interest and enabling service), which relies on ICT. Both these aspects are in focus within the area of information security. Simultaneously, the ICT is becoming increasingly integrated, which means that it may have direct impact on traffic safety, which traditionally is another area of risk management that considers the impact on all levels, but ultimately the service-of-interest level. See further discussion in Somerville, 2007.

5. CONCLUSIONS

The establishment of eMaintenance solutions affects several processes and levels in an organisation, not only the operation and maintenance processes and different maintenance echelons. Furthermore, an eMaintenance solution affects: the ICT-environments, in which it will exist; existing applications; and involved actors and stakeholders. In addition, an eMaintenance solution often affects the structure of the system-of-interest, e.g. by increased system complexity since it may lead to the implementation of additional items (e.g. sensors and software), which need to be managed by the maintenance process. Furthermore, the benefits of an eMaintenance solution paradoxically also add to the complexity of the system by an extended integration of different underlying systems, processes and services, see Figure 7. For example ICT is to an increasing extent integrated into systems that directly affect traffic safety, which can also be linked to other ICT-environments that traditionally are not safety critical. Hence, when establishing an eMaintenance solution it is essential that both threats and opportunities are managed in the early phases of the establishment. The reason is to increase the possibility to achieve positive consequences and avoid negative ones. In fact, any eMaintenance implementation related to critical applications can be stopped, or delayed, if it does not consider relevant risk aspects from the very beginning. Hence, information security should be a central and integrated part of each eMaintenance project through which linkage to other relevant risk-related areas can be achieved.

This paper proposes an Integrated Enterprise Risk Management (IERM) framework that includes principles, processes, methodologies and tools that can support organisations to proactively manage threats and seize opportunities related to the achievement of their objectives (Figures 1 and 4). The framework is based on a set of existing contributions (e.g. provided by ISO and IEC) that can be applied for eMaintenance purposes (Figure

2). The reason is that these standards represent well established and proven practices that are agreed upon by an international community. The framework adapts a process-oriented (Figure 3), explanatory (Figure 5), stakeholder-focused (Figure 6) and top-down approach (Figure 7).

It can be concluded that the framework should be applied both during normal operation and when some change is present in the context of an organisation. A change can be an event or circumstance that result in the need to develop, modify, or implement an eMaintenance solution as a response to the change.

Furthermore, it can be concluded that the risk analysis should consider all levels of the proposed hierarchy (Figure 7) and deploy the requirements of the stakeholders down to the system level. By this approach it is possible to identify and combine the strength of different risk-related areas at appropriate hierarchical levels.

Another conclusion is that the risk identification should start with the requirements of the stakeholders and consider both opportunities and threats. The identification starts with the requirements of the stakeholders and relates these to both the present situation and the desired situation at which the development, modification, or implementation aims.

An additional conclusion is that the identification of threats and opportunities should be iterative. The identification should start at the stakeholder level and proceed downward in the hierarchy. However, opportunities and threats identified at lower level should in turn be aggregated upward in the hierarchy to see if additional threats and opportunities are identified at the higher levels.

It can also be concluded that during the risk evaluation, the consequences of threats and opportunities of possible eMaintenance solutions should be related to the stakeholders' requirements and their risk appetite. The result is a list of ranked risks that have negative or positive consequences.

Furthermore, it can be concluded that the ranking of risks will affect the eMaintenance solution and its inherent services. The reason is that the list together with the risk apatite will act as decision support as how to treat the risk, e.g. by accepting, reducing, avoiding or transferring it.

6. ACKNOWLEDGMENTS

We would like to thank Banverket and Trafikverket for supporting this work both intellectually and financially.

7. REFERENCES

[1] Ahmadi, A; Gupta, S.; Karim, R.; Kumar U. (2010). Selection of maintenance strategy for aircraft systems using multi-criteria decision making methodologies. Accepted for publication in: *International Journal of Reliability, Quality & Safety Engineering*.

[2] Ahmadi, A. (2010). *Aircraft Scheduled Maintenance Programme Development*. Doctoral Thesis, Luleå University of Technology, Luleå, Sweden.

[3] Akersten, P.A. & Klefsjö, B. (2003). Total Dependability Management. *Handbook of Reliability Engineering*. Springer, London, 559-565.

[4] Anderzén, I. and Davidsson, G. (2010). Riskanalys avseende Järnvägens trafiksäkerhet med anledning av bildandet av Trafikverket (Risk analysis of railway safety with regard to the estaishment of the Swedish Transport Administration). Banverket, Borlänge. (In Swedish)

[5] ATA (2007). *MSG-3: Operator/Manufacturer Scheduled Maintenance Development*, Washington, D.C.: Air Transport Association of America.

[6] Blanchard, B. S. (2004). Logistics Engineering and Management. Fourth edition, Prentice-Hall, Englewood Cliffs, New Jerssey.

[7] Candell, O. (2009). *Development of Information Support Solutions for Complex Technical Systems using eMaintenance*. Doctoral Thesis, Luleå University of Technology, Luleå, Sweden.

[8] Candell, O. and Karim, R. (2008). "e-Maintenance - information driven maintenance and support", In Proceedings of FAIM.

[9] CAS (2003). Overview of Enterprise Risk Management. Casualty Actuarial Society (CAS).

[10] COSO (2004). Enterprise Risk Management - Integrated Framework: Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission. September 2004.

[11] Ding, W. and Marchionini, G. (1997). "A Study on Video Browsing Strategies". Technical Report. University of Maryland at College Park,.

[12] Gummesson, E. (2000). *Qualitative Methods in Management Research*. (2nd ed.), Thousand Oaks: Sage.

[13] Hellsten, U. and Klefsjö, B. (2000). TQM as a Management System Consisting of Values, Techniques and Tools. *The TQM Magazine*, 12(4), 238-244.

[14] IEC (1990). 60050 (191): Dependability and quality of service. International Electrotechnical Commission, Geneva, Switzerland.

[15] IEC (1999). *60300 (3-11): Application Guide - Reliability Centred Maintenance*, Geneva: International Electrotechnical Commission.

[16] IEEE 610.12 (1990). IEEE Standard Glossary of Software Engineering Terminology, Software Engineering, IEEE.

[17] IEV (2008). International Electrotechnical Vocabulary (IEV). Available at: http://www.electropedia.org/, accessed: 18 August 2008.

[18] ISO (2009a). 31000: Risk management - Principles and guidelines.

[19] ISO (2009b). ISO Guide 73:2009, Risk management – Vocabulary.

[20] ISO/IEC (2007). 27001:2005, Information technology - Security techniques - Information security management systems - Requirements

[21] ISO/IEC (2008). "15288: Systems engineering - System life cycle processes", International Organization for Standardization and International Electrotechnical Commission, Geneva, Switzerland.

[22] ISO/IEC (2010). ISO/IEC 31010, Risk management - Risk assessment techniques.

[23] ISO-AS/NZS (2009). 31000: Risk management - Principles and guidelines.

[24] Kajko-Mattsson, M., Grace, L.A. and Smith, D.B. (2007). "Roles for Development, Evolution and Maintenance of SOA-Based Systems". In Proceedings of SDSOA, IEEE.

[25] Kaplan, R. S. and Norton, D. P (1996). "Using the Balanced Scorecard as a Strategic Management System," Harvard Business Review (1996):

[26] Karim, R. (2008). *A Service-Oriented Approach to eMaintenance of Complex Technical Systems*. Luleå University of Technology.

[27] Karim, R. ; Candell, O. and Söderholm, P. (2009). Development of ICT-based maintenance support services. In Journal of Quality in Maintenance Engineering, vol. 15, nr. 2, pp. 127 – 150

[28] Karim, R. ; Kajko-Mattsson, M. ; Söderholm, P. ; Candell, O. ; Tyrbern, T. ; Öhlund, H. and Johansson, J. (2008b). Positioning embedded software maintenance within industrial maintenance. In IEEE International Conference on Software Maintenance : ICSM 2008. IEEE, pp. 440 – 443

[29] Karim, R. ; Kajko-Mattsson, M. and Söderholm, P. (2008a). "Exploiting SOA within emaintenance". In Proceedings of the 2nd international workshop on Systems development in SOA environments": International Conference on Software Engineering. Session: SOA supporting business process management (BPM). New York, NY : IEEE, 2008. pp. 75-80.

[30] Lee, J. (2003). E-manufacturing-fundamental, tools, and transformation. *Robotics and Computer-Integrated Manufacturing*, vol. 19, no. 6, pp. 501-507.

[31] Levrat, E., Iunga, B. and Crespo Marquez, A. (2008). E-maintenance: review and conceptual framework. *Production Planning & Control*, vol. 19, no. 4, June 2008, pp. 408-429.

[32] Nowlan, F.S. and Heap, H.F. (1978). *Reliability-Centered Maintenance*, Springfield, Va.: National Technical Information Service (NTIS), US Department of Commerce.

[33] Palm, T. (2008). Försvarsmaktens gemensamma riskhantringsmodell (The shared risk management model of the Armed Forces). Totalförsvarets forskningsinstitut, Stockholm. (In Swedish)

[34] Patel, R. and Tibelius, U. (1987). *Om osäkerhet vid insamlandet av information, in Grundbok i forskningsmetodik*. eds. R. Patel and U. Tibelius, Lund: Studentlitteratur.

[35] Rasmussen, J. and Svedung, I. (2000). Proactive Risk Management in a Dynamic Society. Räddningsverket (Swedish Rescue Services Agency), Karlstad, Sweden.

[36] Riksdagen (The Swedish Parliament) (2010). *Svensk författningssamling*, available at: http://www.riksdagen.se/webbnav/index.aspx?nid=3910

[37] Sommerville, I. (2007). *Software Engineering*. Addison-Wesley.

[38] STA (2009). "Swedish Transport Agency", Available at: http://www.transportstyrelsen.se/en/, accessed 2009-11-18.

[39] STM (2009). "Swedish Transport Administration", Available at: http://www.trafikverket.se/, accessed 2009-11-18.

[40] Söderholm, P. (2004). Continuous Improvements of Complex Technical Systems: A Theoretical Quality Management Framework supported by Requirements Management and Health Management. *Total Quality Management & Business Excellence*, 15(4), 511-525.

[41] Söderholm, P. (2005). *Maintenance and Continuous Improvement of Complex Systems: Linking stakeholder Requirements to the Use of Built-in Test Systems*. Doctoral Thesis, Luleå University of Technology, Luleå, Sweden.

[42] Transportstyrelsen (The Swedish Transport Agency) (2010). *Järnvägsstyrelsens författningssamling*. Available at: http://www.transportstyrelsen.se/Regler/Regler-for-jarnvag/Jarnvagsstyrelsens-forfattningssamling/

[43] Yin, R.K. (2003). *Case Study Research: Design and Methods*, 3rd ed., Sage, Thousand Oaks, CA.