TOWARDS A PROCESS FOR TOTAL INFORMATION RISK MANAGEMENT

(Research Paper)

Alexander Borek
University of Cambridge
ab865@cam.ac.uk

Ajith Kumar Parlikad
University of Cambridge
ajith.parlikad@eng.cam.ac.uk

Philip Woodall
University of Cambridge
phil.woodall@eng.cam.ac.uk

Abstract: The importance of information as a resource and competitive factor in today's society and economy is constantly rising. As a consequence, it becomes necessary for organizations to manage the risks that arise from poor information quality (IQ) in the same way other operational and strategic risks are managed. Information is, however, an unique and intangible resource that requires special methods and techniques for managing its related risks. This paper proposes a process for Total Information Risk Management (TIRM) that enables the assessment and treatment of organization-wide information risks in a systematic and effective manner. The TIRM process provides a practical approach that unites the best practices of the IQ and the risk management disciplines. We have tested and refined the TIRM process by extensive application in four in-depth case studies in different industries following a rigorous process development approach.

Key Words: Information Risk Management, Corporate IQ, IQ Management, IQ Business Impact, IQ Costs.

INTRODUCTION

Information has been long recognized as a resource of vital importance to all organizations (Eaton & Bawden 1991), and has been described as *"a valuable entity, independent of the technology that manipulates it"* [36]. Many studies have shown that information quality (IQ) can have a significant impact on decision-making and organizational performance [22],[28],[12],[21],[33]. Poor quality information can bring huge risks to an organization and even lead to serious disasters as shown in the cases of the explosion of the space shuttle Challenger and the shooting down of an Iranian Airbus by the USS Vincennes [11]. It can result in the need for resource-wasting information rework, cause significant process inefficiencies, and lead to poorer decision making and lost future opportunities [32],[31],[8],[9]. A risk-oriented view on IQ would shift the focus from managing IQ to managing the business impact of IQ and would therefore provide an alternative perspective to IQ management, potentially with productivity gains for an organization. This paper advocates that information risks, which, in this context, are risks that arise from poor IQ, have to be managed in a systematic and holistic way building on concepts from IQ management, e.g. [8],[9],[25],[37],[29], and risk management, e.g. [15],[16],[1],[27]. Moreover, it is essential to understand how decision makers integrate information coming from human and information system sources in order to effectively manage information risks. A process for information risk management should address the following three questions: (1) How can information risks

be identified effectively? (2) How can the impact and likelihood of information risks be assessed, evaluated and monitored? (3) How should potential information risk treatment options be evaluated, selected, implemented and monitored? Effective information risk management can help companies to focus on their IQ "pain points", to build more sensible business cases for information risk mitigation initiatives and to guide them in choosing the best IQ improvement options at a given time. This paper proposes a process for Total Information Risk Management (TIRM) that has been carefully designed and tested in the industry to address the research problem. The rest of the paper is organized as followed: First, we present the relevant literature in two disciplines that provides the foundation for the TIRM process, namely IQ management and risk management, and we explicate information risk in the context of TIRM. Furthermore, we explain how we have developed and tested the TIRM process and, then, present the TIRM process in full detail. The paper concludes with a discussion of contributions to theory and limitations and examines ideas for future research on this topic.

RESEARCH BACKGROUND

A process for managing IQ-related risks should take concepts from the risk management discipline into account. Risk is defined by the International Standard Organization (ISO) as the "effect of uncertainty on objectives" [19]. It can be measured, depending on its nature, using either a statistical approach that uses historical data or a subjective probability approach in an informed decision [1],[27]. Moreover, risk is context-dependent as it reshapes when the system changes [23]. Risk management has academically evolved over time from analyzing one event, its probability and consequence to the analysis of multiple events, which led to research about management structures for risk management [23]. Many different risk management processes have been suggested in the literature [16]. Typically, a risk management process contains the steps: (1) identification of risks, (2) assessment/measurement of risks, (3) evaluation, choice and implementation of risk mitigation options, (4) monitoring of risk mitigation [16].

Information as a resource has unique characteristics, since it can be reused repeatedly with no decrease in value, transferred through time and space, refined and reinterpreted, inferred and adapted; and maybe most importantly, it can be synthesized and converted into knowledge – things that are not possible for traditional resources [10]. This has, however, the consequence that general risk management methods are not readily applicable, but have to be adapted to fit information [14]. The term "information risk management" has been used in the context of disclosure of information [4],[20] or the management of "ICT-induced risks" [7]. The Risk Management Guide for Information Technology Systems of the U.S. Department of Commerce argues that the goal of information risk management should be rather "to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization" [34]. Borek et al. argue that the IT business value chain is strongly connected to information resources, its quality and the related risk induced by IQ [5]. Empirical data shows that poor IQ can have a negative impact on organizational success, e.g. [32],[13],[33],[21]. IQ costs and impacts can be classified along different organizational levels [32], or divided into direct (immediate negative monetary effects) and indirect costs [9]. General cost categories can be (1) process failure costs (a process does not perform properly), (2) information scrap and rework costs (IQ is improved manually without addressing the root cause), and (3) lost and missed opportunity costs [8]. The business impact of IQ can be assessed with a handful of techniques, as for example [8],[25],[26], which however are all cost-based approaches and do not provide a complete information risk management process. On the other hand, existing information risk management processes address only a small subset of the range of risks that are caused by IQ (e.g., information security [4],[14]). This paper is an attempt to merge current risk management approaches with existing approaches to manage IQ and its business impact, in order to create a risk management process that enables the effective management of information risks resulting from poor IQ. In the following, we explain what we mean by information risk by providing some basic constructs and a model.

INFORMATION RISK – BASIC CONSTRUCTS AND MODEL

In this paper, each distinct consequence that is caused by an IQ problem and which has a measureable impact on one or more business objectives is called an information risk. We will explain the model and define its constructs in the following. We define *information risk* as the effect of uncertainty on objectives that arises from the use of information resources and their quality. *Information* can result from data in information systems or knowledge made explicit and communicated by humans in both structured and unstructured forms. *Information quality* is defined from a user perspective as the fitness for use of information, in accordance to the IQ literature. It is a multi-dimensional concept with dimensions like accuracy, completeness, timeliness, security etc. [37].

An *IQ problem* arises when information is not fit for the specific purpose of a task and the outcome of the task is potentially influenced by this. One example that we encountered has been that data about the condition of production machines has been incorrect, which had an impact on decisions how to schedule maintenance activities. *Root causes* of an IQ problem are the technological, people or organizational factors that create an IQ problem [24] and, thus, alone or in combination, have the intrinsic potential to give rise to an information risk. In the case of the inaccurate machine condition data, the root causes were two-fold: (a) some sensors were not calibrated correctly and (b) engineering staff made mistakes when they entered the data manually into the system. An IQ problem can have one or more direct consequences and each direct consequence can have one or more intermediate consequences. A *direct consequence* is the immediate effect of an IQ problem, which has a likelihood attached. An *intermediate consequence* is a consequence of a consequence with a (conditional) likelihood attached. Note that intermediate consequences can cause further intermediate consequences. Some of the consequences have an impact on one or more business objectives. *Business objectives* are strongly context-specific and are defined usually by senior management or the executive board. They can be financial goals, e.g. maximizing revenues, but may also include other aspects like product quality, delivery times, customer satisfaction and environmental objectives. The direct consequence in our example scenario was that decisions how to schedule preventive maintenance activities were sub-optimal. The intermediate consequence was in some cases that maintenance activities were executed unnecessary, which wasted money and which, thus, influenced the business objective “cost-effectiveness”. Another intermediate consequence was that maintenance activities were not executed, although they would have been necessary, which could lead to machine failure and, in the worst case scenario, could cause the production to stop, which has an impact on “operational efficiency”. Moreover, this could lead to a late delivery, which might impact the business objective “customer satisfaction”. *Information risk assessment* is the process of identification, analysis and evaluation of information risk. *Information risk treatment* is the process to modify information risk, for example, by removing the risk source, changing the likelihood or consequences of the risk or sharing the risk with a third party. In the next section, we describe the development of the TIRM process.

PROCESS DEVELOPMENT

The goal of this research is to build and evaluate a practical process for effectively managing information risks in an organization. We therefore use a process-based action research approach developed by (Platts 1993), which has already been proven to be both rigorous and effective for designing management processes in various contexts, e.g. the design of performance measurement systems (Neely et al. 2000). Following this approach, the process development occurred in three research phases, see Figure 1.

The first phase was the initial design of the process on the basis of a review of the existing IQ and risk management literature and interviews with managers (operational, strategic and IT) and consultants (management and IT) about information risks in the industry.

In the second phase, the process was tested and refined by application in a semiconductor manufacturer, a steel manufacturer and an electrical utility company. These studies involved spending a considerable amount of time at the companies’ sites to facilitate workshops for stages 2, 3 and 4 of the TIRM process, which are explained in the next section and in Figure 2. Some interviews and workshops were also

conducted over telephone before and after the site visit. After each workshop, a feedback discussion took place to evaluate how the process can be improved and refined. After each application of the TIRM process, we used the gathered feedback and the experiences and insights of the action researcher to improve the process. The process has been evaluated using feedback discussions after each workshop and questionnaires at the end of the process using the three main criteria feasibility, usability, and utility, which are, according to [30], most suitable to evaluate a management process. The questionnaires have been designed based on a number of sub-criteria and questionnaires developed and tested as part of an existing doctoral thesis that also has used the process-based research approach [35]. We have so far received predominately high results regarding all three evaluation criteria: feasibility, usability and utility of the TIRM process.

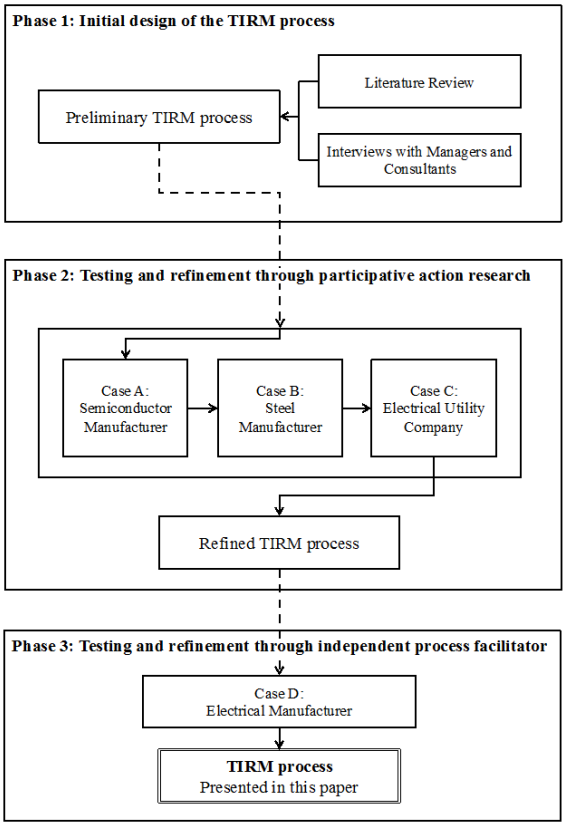

Figure 1. Process Development

In the third research phase, the process was applied in an additional case study in a company that manufactures industrial components. This time, the process has been applied by an independent facilitator to show that the feasibility of the process is not dependent on the knowledge and skills of the researcher [30]. In case study A, we examined five different departments, *viz.*, local maintenance, central engineering, manufacturing IT, planning and purchasing. Case study B comprised quality management, purchasing, maintenance, sales & marketing, strategic management, logistics and planning, production and product design departments. Case study C looked at three core processes in a utility company: (1) processing new customer requests, (2) expanding the existing electricity network and (3) managing and maintaining the existing electricity network. Case study D looked at all processes that are required to manage physical assets in manufacturing, from planning and acquisition to deployment, usage, maintenance and retirement of the assets. In the following, the TIRM process is presented in detail.

TOTAL INFORMATION RISK MANAGEMENT PROCESS

Based on the review of the literature and the industrial interviews, we found that a process for managing information risks in an organization should aim at:

1) Systematically assessing and treating information risks in an organizational-wide scope.
2) Considering information provided by all sources, e.g. IT, documents and humans, external and internal information etc.
3) Being based on a widely accepted risk management standard to assure its acceptance in the industry and that it incorporates current risk management best practices.
4) Building on concepts and assessment and improvement techniques from the IQ discipline.

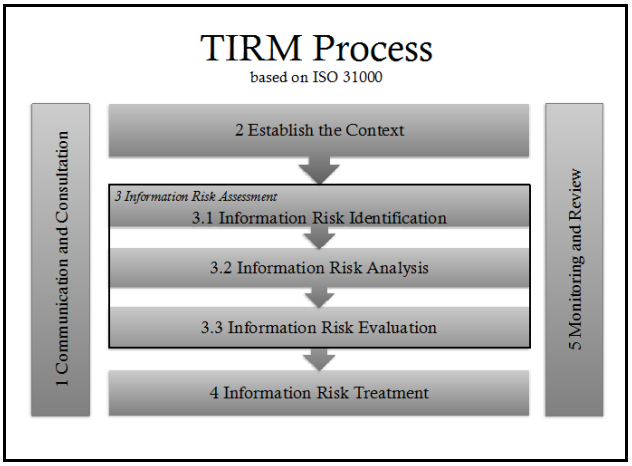

Figure 2. The TIRM Process Overview

Total Information Risk Management (TIRM) is a systematic, holistic approach that builds on formal information risk assessment and management and leans on the concept of total risk management [15]. TIRM aims at managing risks arising from information resources of all possible types and sources, which includes information coming from databases, documents and humans, and information that is external and internal, tacit and explicit, structured and unstructured etc. The TIRM process is based on an internationally widely recognized risk management standard, ISO 31000 [18]. ISO 31000 provides a terminology for risk management, a risk management framework and a risk management process. The TIRM process can be used within the given ISO 31000 framework, but adapts the risk management process specifically for managing information risks by transferring best practices from the IQ discipline. There are five process stages in the TIRM process, which are: (1) communication and consultation, (2) establish the context, (3) information risk assessment, (4) information risk treatment and (5) monitoring and review, as illustrated in Figure 2. Process stages one and five are continuous activities that are executed during the whole process. Each stage of the TIRM process is now described in detail.

Stage 1: Communication and Consultation

Throughout the TIRM process, communication and consultation should take place with all relevant stakeholders, which includes personnel from the business function(s) involved, IT management, risk management, as well as senior executives. As the TIRM process crosses functional boundaries, it is key that senior management is committed to the information risk management initiative. It is also important that the IT management and risk management executives are aware and supportive of the initiative. The goals and benefits of the information risk management program need to be clearly communicated to all people involved in or affected by the TIRM process to gain active support. The validity and plausibility of results from the information risk assessment stage should be cross-checked with relevant stakeholders.

Potential information risk treatment options should be also discussed with all involved parties to better understand their weaknesses, risks and strengths and to get support during implementation.

Stage 2: Establish the Context

Before information risks can be assessed and treated, the organizational context has to be established in discussions with (a) senior general management, (b) IT and knowledge management, (c) risk management, (d) personnel from the business function(s) involved. The external and internal context of the organization needs to be established along with the context of the TIRM process and the risk criteria that should be used to evaluate risks in the organization, as visualized in Figure 3.

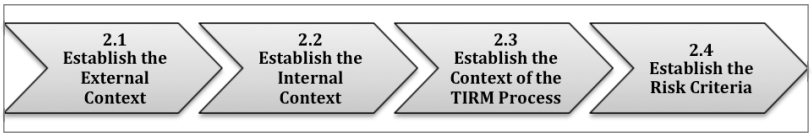

Figure 3. Establish the Context Sub-Stages

Sub-Stage 2.1: Establish the External Context

First, the external context of the organization needs to be established, which can include aspects ranging from "social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local" [18]. The external environment of an organization can have a major influence on how information risks are evaluated. For example, the UK utility industry is a market that is substantially regulated regarding prices and service quality. Information about the age and reliability of physical assets play a crucial role as evidence that investments to modernize the assets are really necessary, which justifies the increase of prices in front of the regulators.

Sub-Stage 2.2: Establish the Internal Context

The internal context looks at governance, organizational structure, policies and objectives of the organization, capabilities, and standards etc. [18].

In particular, it is important to understand the current information management capabilities in the organization, which give context to the information risks that are identified. In our studies, we have used a questionnaire in workshops with operational and IT managers, which builds on the IQ Management Capability Maturity Model developed by [3]. The results in the 13 key performance areas and 48 critical success factors for IQ management of the model can be useful to find the root causes of IQ problems in the information risk treatment stage as they uncover the weaknesses of IQ management in the company.

Sub-Stage 2.3: Establish the Context of the TIRM Process

Additionally, the context for the TIRM process itself needs to be clearly laid out, which depend on the external and internal context of the organization established in 2.1 and 2.2. First, the goals and objectives of the TIRM process need to be defined, which are:

- Understanding the risks that arise through poor IQ for the organization
- Financial evaluation of the business impact of IQ
- Developing effective IQ improvement initiatives based on the identified pain points

The TIRM process requires two special roles, a project sponsor, who needs to be a senior executive equipped with sufficient organizational power, e.g. the CIO or a member of the executive board, and a project manager, who is responsible for the execution of the TIRM process. Moreover, the scope of the process has to be defined, which can be the whole organization or, for example, a specific organizational unit or process group, etc. For each process or task area in the defined scope, at least one representative is chosen, who has sufficient knowledge about this process or task area. It has further to be decided how the IQ assessment should be executed during the information risk assessment stage (see 3.1.3), which can be

either subjective or objective (or a combination), and which IQ dimensions should be selected. Usually, there are other activities and projects that run simultaneously and are relevant to the TIRM process, as for example, a quality management initiative or the rollout of a major enterprise information system. The relationships of the TIRM process to these activities and projects have to be clarified.

Sub-Stage 2.4: Establish the Risk Criteria
Finally, the risk criteria need to be defined. Risk criteria are "the terms of reference against which the significance of a risk is evaluated" [18]. They are "based on organizational objectives, and external and internal context" and can be "derived from standards, laws, policies and other requirements" [18]. Risk criteria include the level at which a risk becomes acceptable or tolerable (e.g. a monetary value), the way likelihood is defined and the timeframe that should be considered.
The TIRM process needs to be integrated and adapted to the overarching risk management process in the given organization. As long as it does not conflict with definitions provided by the TIRM process, all other aspects, e.g. the definitions for likelihood, level of risk and the risk appetite of the organization etc., can be taken from the risk management function in a given organization, if existent, or should otherwise be defined under consideration of the general risk management best practice, e.g. [16].

Stage 3: Information Risk Assessment

Information risk assessment consists of three sub-stages (these can be conducted in a workshop format with the relevant stakeholders). First, potential information risks are identified, then, the identified information risks are analyzed, and finally, they are evaluated against the identified risk criteria (see 2.4), as shown in Figure 4. Next, each sub-stage is described in more detail.

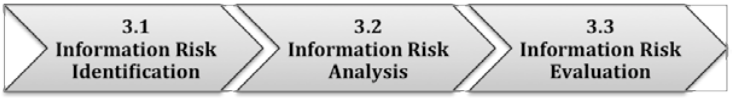

Figure 4. Information Risk Assessment Sub-Stages

Sub-Stage 3.1: Information Risk Identification
Risk identification is the process of finding, recognizing and describing risks. Information risks need to be identified in the scope that has been defined in the Establish the Context stage (see 2.3). The steps for information risk identification are shown in Figure 5.

Figure 5. Information Risk Identification Steps

We found that to identify information risks, it is essential to start with the analysis of which information is used in a process or task area in **step 3.1.1**, because IQ can only be assessed in the context of usage from a user perspective. This step involves measuring the importance of each piece of information for the task and how often it is used. This can be done say, by using a qualitative 4-step Likert scale, e.g. "information is irrelevant", "information is helpful", "information is important", "information is essential". Next, in **step 3.1.2**, information is further examined by studying the information flow within the organization to understand how each item of information is created, processed and accessed. This provides the context for the IQ assessment as it ensures that each information item that is assessed is clearly defined and fully understood. The output of steps 3.1.1 and 3.1.2 are therefore important to proceed with the IQ assessment in **step 3.1.3**. The quality of each information item used is assessed along the IQ dimensions defined in

the Establish the Context stage (see 2.3). IQ can be assessed using existing IQ assessment methodologies, see [2] for a good overview. There are generally two different types of IQ assessment: Subjective assessments, which "reflect the needs and experiences of stakeholders", and objective assessments, which use defined metrics to assess IQ, which can be either task-independent or task-dependent [29]. We have used a subjective IQ assessment in our studies, assessing the quality of each information used for a task in each dimension on a 4-step Likert scale, e.g. from "information is always inaccurate", "information is often inaccurate", "information is sometimes inaccurate" to "the accuracy of information is satisfying". Results that are available from objective IQ assessments, which have been already conducted in the past, can be included in the results of the subjective assessments, for example, by using the DQA methodology [29]. Note that sometimes a process involves external parties that should, when possible, be included in the IQ assessment or in cases when this is difficult, the process or task area representatives inside the organization can assess the IQ from the third party perspective based on the experiences of problems that they could observe in the work with the customers, suppliers etc. For instance, in the new connections process of the utility company, customers receive an offer letter that reveals the costs, requirements and duties for connecting a specific new building to the electricity network. In 10 to 30 percent of cases (average 20 percent), which is when the customer is a private individual or inexperienced developer, the customer does not understand the detailed requirements and hence delays the job considerably.

In **step 3.1.4**, each IQ problem identified has be described in detail, i.e. when and why does it occur in which task, why does it influence the task, how often does the IQ problem appear. In some cases, the results from the information management maturity assessment from sub-stage 2.3 are providing some context for the IQ problem. To understand the IQ problems from the perspective of information custodians, they can be asked directly to examine the problems. Only, when the IQ problem is thoroughly understood, it is possible to determine its consequences accurately. Thus, in **step 3.1.5**, for each IQ problem, the direct and intermediate consequences are identified (note that not every IQ problem needs to have a direct and/or intermediate consequence, in fact, some IQ problems have no consequence at all). A representative of a process or task area does not always have the full knowledge to determine the intermediate consequences of an IQ problem. Sometimes it is, therefore, useful to interview representatives from other processes or task areas that might be affected intermediately by the problem. The output of this sub-stage is a set of IQ problems for each process or activity and identified direct and intermediate consequences, which is further used for information risk analysis. To give an example, an IQ problems that we encountered in one of our cases in a manufacturing company has been that information about materials used for production were incomplete, which made it difficult to find out the details about the materials and to understand which materials are actually the same. The reasons for this were (a) the lack of a unified terminology for materials in the company, which made it hard to find out which material is actually used, and (b) that their ERP system did not allow the entry of sufficient details about materials. This IQ problem happened quite frequently and had the direct consequence that it became very difficult and time consuming to find a cheaper supplier for a material. The intermediate consequence has been that the organization used the old supplier for a material, although there were cheaper suppliers available.

Sub-Stage 3.2: Information Risk Analysis

Information risk analysis follows a four step process shown in Figure 6. **Steps 3.2.1** and **3.2.2** analyze the direct and the intermediate consequences of the identified IQ problems in sub-stage 3.1. Risk analysis examines "the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur" [18]. Note that the causes and sources of risk have been already identified in sub-stage 3.1 of the TIRM process by determining and examining the found IQ problem.

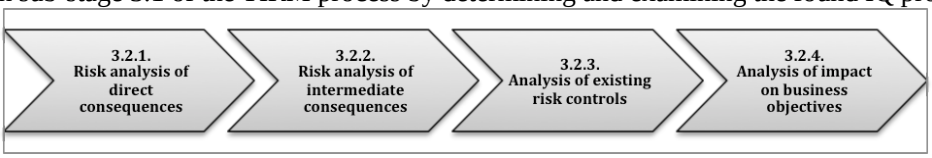

Figure 6. Information Risk Analysis Steps

The likelihood and the consequences of an information risk can be measured quantitatively by taking estimates using a triangular distribution, which requires estimating the lower and upper boundary and the average and, thus, makes it easier for the process or task area representative to make an quantitative estimation of likelihood and consequences. It has been shown that using ranges for subjective measurements can provide relatively solid measurements also for intangible assets like information [17]. In some cases, when quantification is not possible or does not make sense, qualitative descriptions or scales can be used. A typical example would be when the potential consequence is human causality, which can not be easily put into numbers nor might not be ethically appropriate. In case study C, plans of the existing electricity network were in 10-30 percent (15 percent in average) of the cases inaccurate or incomplete, as they are based on historical background plans, which is historical data up to 100 years old. Incorrect and/or incomplete plans of the existing network can lead to safety issues as engineers might work on high voltage cables without knowing it. This could lead 1 to 10 times a year (5 times average) to serious injuries or even death. However, existing controls are in place in form of working procedures, in particular, safety rules that engineers comply to, which reduces the impact to minor injuries in the normal case and serious injuries in the worst case (while the likelihood stays the same). Another consequence is that the job is calculated using wrong cost estimates due to wrong assumptions following from the network plans. This has a high impact on customer satisfaction, as three times a month customers are requested to pay up to 5000 pounds more than planned (500 pounds in average). Moreover, this creates, on average 3 times a year, additional costs of up to 10000 pounds (2000 pounds in average) for the company. Plus, due to inadequate planning, between 1 and 5 times a month (average 3 times), construction work is delayed by 5 days in average (between 0 and 14).

Then, in **step 3.2.3**, we investigate which risk controls are already in place and what the likelihood and consequence of the risk would be without the controls. Risk controls reduce the likelihood or the consequence of the risk and not knowing them could result in a wrong risk analysis and evaluation. Moreover, the value of the risk control becomes more transparent and it can be decided if it is worth keeping the risk control in place. In the example above, risk controls are, for instance, safety procedures that are in place that reduce the likelihood of injuries and deaths.

As risk is the effect of uncertainty on objectives, it is key to look at how the analyzed consequences impact the business objectives. **Step 3.2.4**, therefore, studies the overall impact of each information risk on the business objectives in the organization and evaluates them using qualitative scales (*very low* to *very high*). For instance, fatal injuries of engineering staff due to incomplete and inaccurate plans clearly has a *very high* impact on the organization's objective "our commitment to our staff is to provide them with safe working conditions". On the other hand, charging customers too much due to an incorrect bill of material has a *medium* impact on the objective "to exceed our customers' expectations". This, then, leads to the evaluation of the information risks.

Sub-Stage 3.3: Information Risk Evaluation

Third, a thorough risk evaluation is required, taking the wider context of information risk management into account, e.g. the level of other information risks and their inter-relationships. In particular, it needs to be decided if an information risk is tolerable and if it should be treated, by comparing the level of risk with risk criteria from sub-stage 2.4, and the priorities of different treatments implementations have to be determined [18], which are used in the information risk treatment stage. To illustrate it with an example, the risk of serious injuries due to poor IQ in the organization that we examined has been evaluated as not tolerable and, thus, has required information risk treatment, whereas wrong customer billing is an information risk that has been evaluated as tolerable.

Stage 4: Information Risk Treatment

ISO 31000 describes risk treatment as "selecting one or more options for modifying risks, and implementing those options" [18], as illustrated in Figure 8. Furthermore, information risk treatment is a

cycle that only ends when an information risk becomes tolerable or reaches a level that is satisfying.

3.2 INFORMATION RISK ANALYSIS

	Information 1	Information 2	Information 3	Information 4
Used Information	Plans	Bill of materials	List of Tasks	Materials available in store
Information Risk Title	Safety issues like working on high voltage cable	Customer would complain about pricing	Wrong task is done	Parts are not available when needed
Impact Type	Poorer decisions	Security risk	Poorer decisions	Resources are wasted
Root Dimensions	Accuracy and Completeness	Information Security	Accuracy	Accuracy
Root Cause	Plans do not show safety issues, because background plans are incorrect (historical data up to 100 years old).	Pricing of materials falls into the hands of the customer.	Procedures change over time	Sometimes materials are not replaced when required, which changes the availability of materials.
What is the likelihood of the consquence?	Likelihood of Consequence	Likelihood of Consequence	Likelihood of Consequence	Likelihood of Consequence
	Lower Boundary: 1 / Average: 5 / Upper Boundary: 10	Lower Boundary: 0% / Average: 0,1% / Upper Boundary: 1%	Lower Boundary: 0 / Average: 3 / Upper Boundary: 10	Lower Boundary: 0 / Average: 1 / Upper Boundary: 2
Unit	# per Year	Percent	# per Year	# per Month
Comment			around 2 changes a year, which affect the number of projects stated above.	
What is the consequence?	Consequence	Consequence	Consequence	Consequence
	Lower Boundary: No injuries / Average: Minor injuries / Upper Boundary: Serious injuries	Lower Boundary: 0 / Average: 100 / Upper Boundary: 1000	Lower Boundary: 0 / Average: 300 / Upper Boundary: 3000	Lower Boundary: 200 / Average: 1000 / Upper Boundary: 3000
Unit		Pounds	Pounds	Pounds
Comment	It is very unlikely that people get serious injured or killed	Company might need to explain pricing to the public.		
Controls already in place	Working procedures, in particular safety rules, for example equipment to check high voltage cables,	Take care of the control of the data.	Staff check parts before starting work.	Forwardplanning with procurement. Range of substitute components. Minimum stock levels.
What is the likelihood of the consequence without controls?	Likelihood of Consequence	Likelihood of Consequence	Likelihood of Consequence	Likelihood of Consequence
	Lower Boundary: 1 / Average: 5 / Upper Boundary: 10	Lower Boundary: 0% / Average: 5% / Upper Boundary: 10%	Lower Boundary: 0 / Average: 20 / Upper Boundary: 40	Lower Boundary: 0 / Average: 2 / Upper Boundary: 4
Unit	# per Year	Percent	# per Year	# per Year
Comment	Near misses		around 2 changes a year, which affect the number of projects stated above.	
What is the consequence without controls?	Consequence	Consequence	Consequence	Consequence
	Lower Boundary: Minor injuries / Average: Serious injuries / Upper Boundary: Fatal injuries	Lower Boundary: 0 / Average: 100 / Upper Boundary: 1000	Lower Boundary: 0 / Average: 1000 / Upper Boundary: 10000	Lower Boundary: 200 / Average: 1000 / Upper Boundary: 3000
Unit		Pounds	Pounds	Pounds
Comment	It is likely that people get seriously injured or killed	Company might need to explain pricing to the public.		

Figure 7. TIRM Spreadsheet Tool – Information Risk Analysis

Figure 8. Information Risk Treatment Sub-Stages

In our case studies, we have so far only applied sub-stage 4.1 actively due to constraints regarding time and access. In sub-stage 4.2, we acted where possible as non-participating observers (and not as action researchers anymore). However, the steps in sub-stages 4.1 and 4.2 are based on a rigorous review of the IQ improvement literature, which has been presented in [6] with some minor modifications. Note that not all information risk treatment options require an IQ improvement. For instance, avoiding a risk by not starting the activity that creates the risk can mean in practice that a task, for which out-of-date information is used, is stopped being executed so that the faulty information is not needed anymore.

Sub-Stage 4.1: Select Information Risk Treatment Options

Figure 9. Select Information Risk Treatment Options Steps

In order to find and select appropriate information risk treatment options, a five step process is used, as shown in Figure 9. Often several information risks are based on the same IQ problem. **Step 4.1.1,** therefore, selects the key IQ problems based on the assessed information risks of stage 3, which either have been marked as not tolerable or where it seems most beneficial for the company to make an information risk treatment. In **step 4.1.2**, the root causes of the IQ problems are identified, which is needed to be able to treat the source of the information risks. To identify root causes, we categorize each IQ problem in a table according to the position of the root cause of the IQ problem in the information lifecycle and regarding whether the IQ problem is caused by technology, organization or people factors [24], as shown in the example in Table 1. Additionally, we examine if the root causes of the IQ problem lie within the organization (internal) or outside the organization (external)

Information Lifecycle	***Create***	Process	***Access***	***Use***	***Dispose***
Technology	ERP system does not sufficiently support the data collection process	-	-	-	-
Organization	Data collection is not communicated as a top priority by management	-	-	-	-
People	Insufficient knowledge of sales staff about which and how data should be entered	-	-	-	-
Internal or External	*Internal creation by sales staff*	-	-	-	-

Table 1. Example - Root Cause Analysis of IQ Problems (in Step 4.1.2)

The example shown in Table 1 is taken from case study B with a steel manufacturing company. Information about the technical product requirements from the customers, which are entered into the ERP system by the sales staff, are often incorrect and/or incomplete. This leads between 0 and 5 times a year to a wrong product design, which costs substantial money and makes also the customers unhappy. The IQ problem has its origins during the creation of the information by the sales staff due to three factors: the

sales staff has insufficient knowledge about which and how information should be collected (which is a *people* issue), the collection of this data is not prioritized high enough by the senior management (which is an *organizational* issue), and the enterprise resource planning system does not support sufficiently the data collection process (which is a *technology* issue). The rest of the table is empty as there are no root causes in other parts of the information lifecycle regarding this IQ problem.

Information Lifecycle	***Create***	***Process***	***Access***	***Use***	***Dispose***
Potential Technology Treatment	Modify ERP system so that data users can give feedback if collected information is sufficient and check the correctness already during the data collection stage.	-	-	-	-
Potential Organization Treatment	Head of production and head of sales have to make it a requirement for sales staff to fill out the complete checklist with information that is as accurate as possible.	-	-	When information is used, the sales department should be called to obtain additional clarifying information.	-
Potential People Treatment	Special training for sales staff that shows how they can interpret the customer requirements and capture the data better.	-	-	-	-
Internal or External	*Internal creation by sales staff*	-	-	*Internal usage by technical staff*	-

Table 2. Example - Identification of Potential Information Risk Treatment Options (in Step 4.1.3)

Information Risk Treatment	**Treatment Option No. 1: Additional Training for Sales Staff**
Treated Information Risk	Information Risk 1: Information about the technical product requirements
Description	Additional training for sales personnel regarding technical aspects of the product, which should take place once a year. Current training is mostly focusing on business aspects. In particular, it has to be shown in the training how checklists in the ERP system should be filled out and how customer requirements are interpreted correctly.
Benefits	It is expected that the additional training leads to a 25-35% reduction of the frequency of the occurrence of incorrect and/or incomplete information about product requirements (ca. 50% of the problems arise because customers do not want to share the information and it is assumed based on previous experience that not all problems are resolved by the training). This can bring estimated savings of 15000 to 25000 USD yearly and can avoid customer dissatisfaction. Additional benefits are that the qualification of the sales staff is improved substantially over time, which can lead to more sales in the long term.
Costs	The additional training of the sales staff would generate costs between 4000 and 7000 USD yearly. The costs result from designing and executing the training once a year.
Risks	There is a risk that the training measures are not as effective as estimated and that, therefore, the information risk is not mitigated properly.
Responsible Managers	***Head of Sales and Executive Management***
Benefit/Cost Evaluation	***High***
Recommendation	***Implement information risk treatment option with High Priority***

Table 3. Example – An Evaluated Risk Treatment Option (in Steps 4.1.4 and 4.1.5)

In **step 4.1.3**, alternative information risk treatment options are developed by populating the table created in step 4.1.2 with potential risk treatment options, as illustrated in Table 2. This is a brainstorming activity that can be inspired by previous solutions and experiences but also by successful examples in the literature. The table helps by giving structure to the thoughts in the brainstorming process and also by pointing to the right direction. For instance, as the example used in the table is a data collection problem, it makes it clear that potential solutions have to address this stage of the information life cycle. Only, when solutions are not found in a particular stage, other stages are considered for solutions that are "out of the box". For instance, in Table 2, the organizational treatment during the information usage stage could be that the technical staff calls the sales department to get additional clarifying information about technical product requirements. However, this solution does not address the root of the IQ problem.
In **step 4.1.4**, each potential information risk treatment option found in step 4.1.3 has to be assessed and evaluated regarding the costs, risks and benefits of the option. This is then used in **step 4.1.5**, to decide, which information risk treatment options should be executed and in which priority it should be implemented. It needs also to be determined which managers are held responsible for the implementation. An example of such an evaluation resulting from steps 4.1.4 and 4.1.5 is shown in Table 3.

Sub-Stage 4.2: Implement Information Risk Treatment Options
The output of sub-stage 4.1 is a list of selected information risk treatment options, which have now to be implemented in sub-stage 4.2. The implementation can differ a lot between various risk treatments. For risk treatment that involve IQ improvement, a six step process can be followed, which is presented in Figure 10. **Step 4.2.1** is to build a team that should be responsible with the implementation of the risk treatment. The team should contain members from different functions including IT and operational management. In **step 4.2.2**, when necessary, appropriate software tools are selected that support the implementation of the risk treatment, e.g. data deduplication software or business process modelling software. In **step 4.2.3**, the project team has to analyse the different ways selected information risk treatment options can be implemented and then choose the one that is considered to be the most effective.

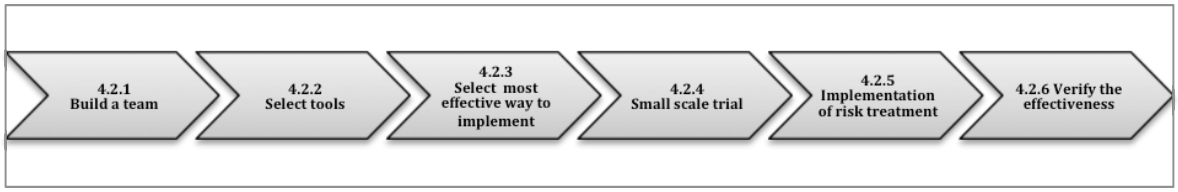

Figure 10. Implement Information Risk Treatment Options Steps

For instance, it is possible to enrich existing data with new data from external providers. It has to be decided which provider should be selected and how the old data should be merged with the new data. In **step 4.2.4**, the risk treatment is implemented, whenever possible, on a small scale to test its effectiveness and, when necessary, to modify the risk treatment to increase its effectiveness afterwards. Eventually, **step 4.2.5** is the actual implementation of the information risk treatment and its effectivness is verified, which leads to stage 5, the monitoring and review of the TIRM process.

Stage 5: Monitoring and Review

The TIRM process has to be monitored and reviewed, either ad-hoc or periodically, to assure that controls are effectively working. Monitoring and review can be also very useful to collect additional information for improving risk assessment, analyze experiences made and to identify changes in the internal and external context [18]. The results from the monitoring and review stage should be recorded and reported. Furthermore, they provide an input for the review of the risk management framework.

CONCLUSION

This paper presents a process for Total Information Risk Management that enables the systematic organizational-wide identification, measurement, analysis and mitigation of information risks. It is build based on the concepts from risk management and the IQ discipline and unites the best practices of both disciplines in a novel approach to manage IQ-related information risks. From a research perspective, there are three major contributions in this paper. First, we have demonstrated that such an information risk management process can be useful, feasible and usable in practice in general by collecting feedback on the final reports that resulted from the TIRM process and by observing that recommendations for information risk treatment options have in some cases already been successfully implemented. Second, we have shown a potential specific way to manage information risks that can be readily applied in the industry by presenting the TIRM process in full detail in this paper. Third, the TIRM process has strong theoretical implications as it shows a clear interface between risk management and the IQ discipline. From a practitioners perspective, our contributions have implications for most of today's organizations, in which it is imperative to understand the business value of IQ and to justify any larger IQ investment from a cost benefit view point. The TIRM process could be a valuable tool for identifying the IQ "pain points" and setting the IQ priorities in an organization, a prerequisite for successful information risk treatment.

A limitation of this research so far is that we could not fully test stage 5 (Monitoring and Review) and sub-stage 4.2, i.e. implement information risk treatment options, due to company access and time restrictions in our case studies. However, as some of the case studies went for more than a year from beginning to end, we could observe that a substantial number of the recommended information risk treatment options have resulted in new projects and a few of them have been already implemented during this time period and have often proven to be very effective. Furthermore, our current software tool that supports the TIRM process is spreadsheet based, which enabled us to rapidly develop and modify it. Spreadsheet-based tools have yet weaknesses regarding usability and the automation of data analysis and integration in comparison, for example, to a more sophisticated Java-based software tool. This had some impact on the usability and feasibility of the TIRM process. We plan to implement a software tool as part of this project in the near future. The TIRM process has been applied in the context of production and utility organizations. It needs to be further tested in more industries and other contexts in future studies.

ACKNOWLEDGEMENTS

This research is funded by EPSRC project "Information Quality in Asset Management", project reference number EP/G038171/1. We would like to thank Valeria Klassen for her work as independent facilitator.

REFERENCES

[1] Barrese, J., and Scordis, N., "Corporate Risk Management.," *Review of Business*, 24 (3), 2003, pp.26–30.

[2] Batini, C., Cappiello, C., Francalanci, C., and Maurino, A., "Methodologies for data quality assessment and improvement," *ACM Computing Surveys (CSUR)*, 41 (3), 2009, p.16.

[3] Baškarada, S., *IQM-CMM: Information Quality Management Capability Maturity Model*.Vieweg +Teubner, 2009.

[4] Blakley, B., McDermott, E., and Geer, D., "Information security is information risk management," Proceedings of the 2001 workshop on New security paradigms, 2001, pp.97–104.

[5] Borek, A., Helfert, M., Ge, M., and Parlikad, A.K., "An information oriented framework for relating IS/IT resources and business value," Proceedings of the International Conference on Enterprise Information Systems (ICEIS), 2011.

[6] Borek, A., Woodall, P., and Parlikad, A.K., "A Risk Management Approach to Improving Information Quality for Operational and Strategic Management," Proceedings of the 18th EUROMA Conference: Exploring Interfaces, 2011.

[8] English, L.P., *Improving data warehouse and business information quality: methods for reducing costs and increasing profits*.John Wiley & Sons, 1999.

[9] Eppler, M., and Helfert, M., "A classification and analysis of data quality costs," Proceedings of the 9th International Conference on Information Quality (ICIQ-04), 2004, pp.311–325.
[10] Fattahi, R., and Afshar, E., "Added value of information and information systems: a conceptual approach," *Library Review*, 55 (2), 2006, pp.132–147.
[11] Fisher, C.W., and Kingma, B.R., "Criticality of data quality as exemplified in two disasters," *Information & Management*, 39 (2), 2001, pp.109–116.
[12] Ge, M., "Information quality assessment and effects on inventory decision-making," Doctoral Thesis, Dublin City University, 2009.
[13] Ge, M., and Helfert, M., "Effects of information quality on inventory management," *International Journal of Information Quality*, 2 (2), 2008, pp.177–191.
[14] Gerber, M., and von Solms, R., "Management of risk in the information age," *Computers & Security*, 24 (1), 2005, pp.16-30.
[15] Haimes, Y.Y., "Total Risk Management," *Risk Analysis*, 11 (2), 1991, pp.169–171.
[16] Hopkin, P., *Fundamentals of Risk Management: Understanding Evaluating and Implementing Effective Risk Management*.Kogan page, 2010.
[17] Hubbard, D.W., *How to measure anything: finding the value of intangibles in business*.John Wiley & Sons, 2010.
[18] International Organization for Standardization, "ISO 31000:2009 Risk Management – Principles and Guidelines on Implementation" 2009.
[19] International Organization for Standardization, "ISO Guide 73:2009 - Risk management -- Vocabulary" 2009.
[21] Jung, W., "An experimental study of the effects of contextual and representational data quality on decision performance," Doctoral Thesis, Claremont Graduate School, 2005.
[22] Jung, W., Olfman, L., Ryan, T., and Park, Y.T., "An Experimental Study of the Effects of Representational Data Quality on Decision Performance," *AMCIS 2005 Proceedings*, 2005, p.298.
[23] Kumar, M., "Risk Management Practices In Global Manufacturing Investment," Doctoral Thesis, University of Cambridge, 2010.
[24] Lin, S., Gao, J., Koronios, A., and Chanana, V., "Developing a data quality framework for asset management in engineering organisations," *International Journal of Information Quality*, 1 (1), 2007, pp.100–126.
[25] Loshin, D., *Enterprise knowledge management: The data quality approach*.Morgan Kaufmann, 2001.
[26] McGilvray, D., *Executing Data Quality Projects: Ten Steps to Quality Data and Trusted Information*.Morgan Kaufmann, 2008.
[27] Miller, K.D., "A framework for integrated risk management in international business," *Journal of international business studies*, 23 (2), 1992, pp.311–331.
[28] O'Reilly III, C.A., "Variations in decision makers' use of information sources: The impact of quality and accessibility of information," *Academy of Management Journal*, 25 (4), 1982, pp.756–771.
[29] Pipino, L.L., Lee, Y.W., and Wang, R.Y., "Data quality assessment," *Communications of the ACM*, 45 (4), 2002, pp.211-218.
[30] Platts, K.W., "A process approach to researching manufacturing strategy," *International Journal of Operations and Production Management*, 13, 1993, pp.4–4.
[31] Redman, T.C., "Improve data quality for competitive advantage," *Sloan Management Review*, 36, 1995, pp.99–99.
[32] Redman, T.C., "The impact of poor data quality on the typical enterprise," *Communications of the ACM*, 41 (2), 1998, pp.79-82.
[33] Slone, J.P., "Information quality strategy: An empirical investigation of the relationship between information quality improvements and organizational outcomes," Doctoral Thesis, Capella University, 2006.
[34] Stoneburner, G., Goguen, A., and Feringa, A., "Risk management guide for information technology systems," *Nist special publication*, 800, 2002, p.30.
[35] Tan, K.H., "A Process and Tool for Manufacturing Action Plan Selection," Doctoral Thesis, Institute for Manufacturing, University of Cambridge, 2002.
[36] Trauth, E.M., "The evolution of information resource management," *Information & Management*, 16 (5), 1989, pp.257–268.
[37] Wang, R.Y., and Strong, D.M., "Beyond accuracy: What data quality means to data consumers," *Journal of management information systems*, 12 (4), 1996, p.33.