PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

INTRODUCING A THEORETIC MODEL AND AN EMPIRIC NORM FOR INFORMATION RISK MANAGEMENT IN DECISION MAKING

Stefan Schwerd, Richard Mayr
University of Latvia, Latvia
E-mail: stefan@schwerd.eu, mail@richardmayr.de

Abstract

Nowadays computer mediated communication (CMC) and the high volume of computed and stored information is getting a business on its own. Information is collected, aggregated, analyzed and used to create real business advantage and value but also risks within companies and also outside on the markets in a high volume. On the other hand, single individuals still need to deal and interpret this sheer mass of increasing information continuously. The change in information management and handling triggers the ongoing changes in decision makings on the operational level as well as on the strategic level. Information is a good sold itself and triggered an own industry of information brokerage. It opens the question of trust and correctness into the information itself but also into the information source and opens a complete new, not modelled yet discipline of Information Risk Management. Currently no model exists in science to measure Information Risk Management where as there is a highly increasing demand to measure case-based applicability and success of Information Risk-Management (IRM) activities in a broader context. The authors propose a new model for IRM and derive a qualitative prove of variables/measure and a quantitative empiric-norm as a base for further perception comparison with specifically targeted groups.
Keywords*: information risk management, management theory, decision making, enterprise risk management.*

Introduction

The central point of this research work was based on various observations in midsized and big enterprises in various businesses around the globe IRM was not considered as being an upcoming management topic. On the other hand, it was observed, that current literature and research does not offer an empiric model or empiric-norm for "Information Risk Management". Especially in the context of decision making processes this could lead to a serious intentional or unintentional drift, where the base of Information is the base for the decision quality. With this, there is currently no formalized way of comparison or benchmarking of companies or dedicated groups e.g. for average "mid-managers" on their level in the light of IRM. So, the main goal of this research work is:

H0: development of a model and a robust and statistically proven empiric norm for Information Risk Management in the context of decision making, including the factorization and definition of measurement variables for Information Risk Management

Developing a model in an area that has not been researched and finding appropriate measures required a broad research work of multiple connected disciplines such as e.g. "communication", "social- and pedagogic", and "computer-science". Figure 1 gives an overview of

ISSN 2029-6932 (Print) ISSN 2538-712X (Online)

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

initially literature-researched scientific fields and their relations and builds the initial frame and context for identifying variables and measures for IRM.

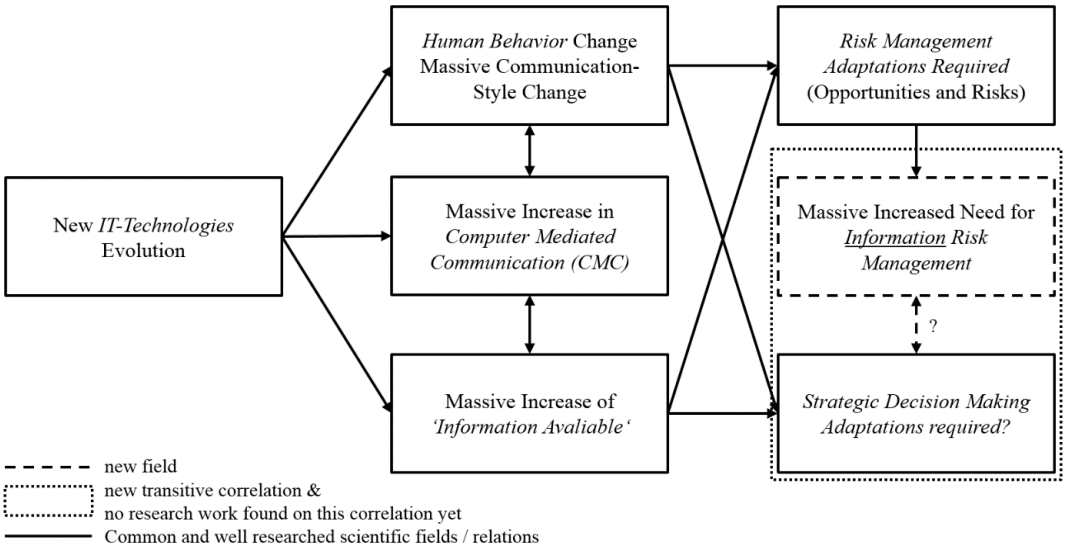

Figure 1: Information Technology impact on Risk-Management – a transitive view.

The focus for the initial model development was done in the context of decision making or in other words, the new measurement model for IRM should be targeting the quality / improvement of strategic decision-making processes.

Methodology of Research

General Background of Research

The initial question on how to measure the quality and characteristics of "Information Risk Management" mechanism, a choice of several operationalized measurable variables and indicators are preselected based on a broad literature research. The Table 1 shows the resulting 4 variables and in a cross table style also the authors/references which have been considered the individual measures/variables – besides the later statistical results described later.

In the area of Social- and Psychological Research, which describes the perception and the behavior, the "buy-in" theory of participation in IRM contexts associates' user acceptance with users' psychological involvement that develops during their participation. In other words, as users participate in IRM activities, they begin to view the focal system as personally important and relevant, and are therefore likely to be more accepting of the system than they would otherwise be had they not participated. On the other Hand, John D'Arcy (2015) describes situations where security requirements increase workload for employees and, as a result, create added time pressure for them to complete job duties. For example, employees who do not have administrative access to their work computers may have to spend valuable time completing paperwork and waiting for an IT professional to install needed software or download needed materials. As a result, employees should work harder and faster to compensate for the overload caused by this security requirement. These conditions are known causes of frustration and stress. Employees have also lamented that many security requirements force them to adapt their work procedures (e.g., not sharing passwords with co-workers) which can be stress inducing.

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

With this a first overarching interim result is the real of IRM-"AWARENESS" of the employees. It could be seen as one of the key indicators of IRM as such and for all further identified measures. This includes not only the theoretical knowledge of IRM at all levels of the organization but also the willingness to follow combined with a proactive "all day" attention.

Enterprise Risk Management Systems - prominent example are insurance companies - where the risks of clients are economically transferred to. The basic methods are well researched and with the upcoming era of high performing computers the mathematical models became very detailed including thousands of variables. But also, with this ability to process in real-time billions of data, a new risk became more prominent – the risk of having correct information at the time needed in a secure way available. In newer days' systems take economic decisions in milliseconds, esp. in the banking and brokerage area. No human is re-calculating the equations. Including also the legislative circumstances like data privacy or SOx. Authors in ERM agree that a focal point for the future is also the human being, being still an essential part of the whole ERM/IRM discussion in a fully automated and computerized world. Other than IT Systems human capabilities are not scalable ad infinitum. Changes in organizational structures and interpersonal relationships are the consequence and are projecting into the quality of information. The systems-specifications, the data-models already are reflecting this human limitation as they are created by humans. A whole business was created about information as a good sold to ensure competitive advantage to clients using this aggregated or even detailed profiling for their primary business.

The aim of Enterprise Risk Management is to detect, eliminate, avoid or transfer (Auer, M. 2008) risk and their economic impact for the company (Cruz, 2002). With increasing media-presence and new media it becomes more and more important to open a coherent and effective framework that includes necessary steps and processes for integrating Reputation Risk management into an organization's overall ERM approach which is intended to support corporate strategic success (Gazert, Schmit, 2016). In particular reputation creation, enhancement, and protection are critical to an organization's success, yet highly challenging given the wide ranging and somewhat opaque nature of the concept. These qualities call for a strong ERM approach to reputation that is holistic and integrative, yet existing knowledge of how to do so is limited. Gazert and Schmit address risk strategy, risk assessment, risk governance, and risk culture as key elements of ERM - adding to common strategies the integrated Reputation Risk Management that applies across industries. In contrast to previous work, Gazert et al (Gazert, Schmit, 2016) offer a broader perspective on the underlying causes and consequences of reputation damage based on empirical evidence and insight from the academic literature and provide additional detail in identification of reputation determinants, antecedents, and drivers. Results in a study by Fiordelisi et al. (2011), for example, indicate that substantial reputational loses follow after operational loss events and that the highest reputational damage is caused by the operational risk type "fraud". Methods of preventing operational losses mainly comprise the monitoring and optimization of processes as well as the initialization of training for the employees and business continuity management. These methods only influence the probability of operational losses, but not the magnitude of single operational loss events (Auer, 2008). On top, internal operational loss (…) is often limited as operational risk includes human errors and, thus, the willingness of employees to inform about operational loss events will be one crucial success factor (Kalhoff, Maas, 2004). Bowling (2005) describes a meta-strategy to approach to be considered when implementing an ERM-Strategy:

- Focus on strategy and business objectives
- Think broadly about the expansive range of risks facing your organization
- Recognizing that ERM is not a quick process but a multi-year journey

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

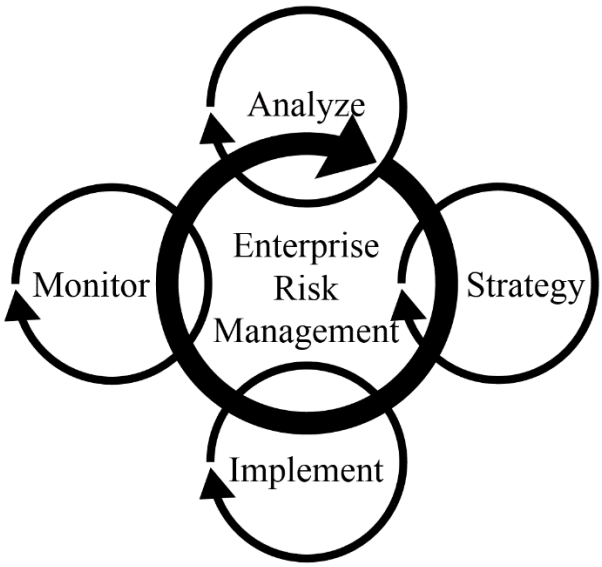

Figure 2: Enterprise risk management model.
Source: Bowling, David M. 2005. Success Factors for Implementing Enterprise Risk Management (pp.26)

In Figure 2 Bowling describes the fundamental and anytime ongoing four steps of Enterprise Risk Management. Starting with an overall analysis, building a strategy based on the analyses results, implementing this strategy while continuously monitoring and analyzing the efforts done but also the changes outside in the market but also internal changes iteratively.

David Bowling (2005) proposed a model for the implementation in hierarchy of steps to be followed which became in the meantime an accepted business organizations' standard - see Figure 3.

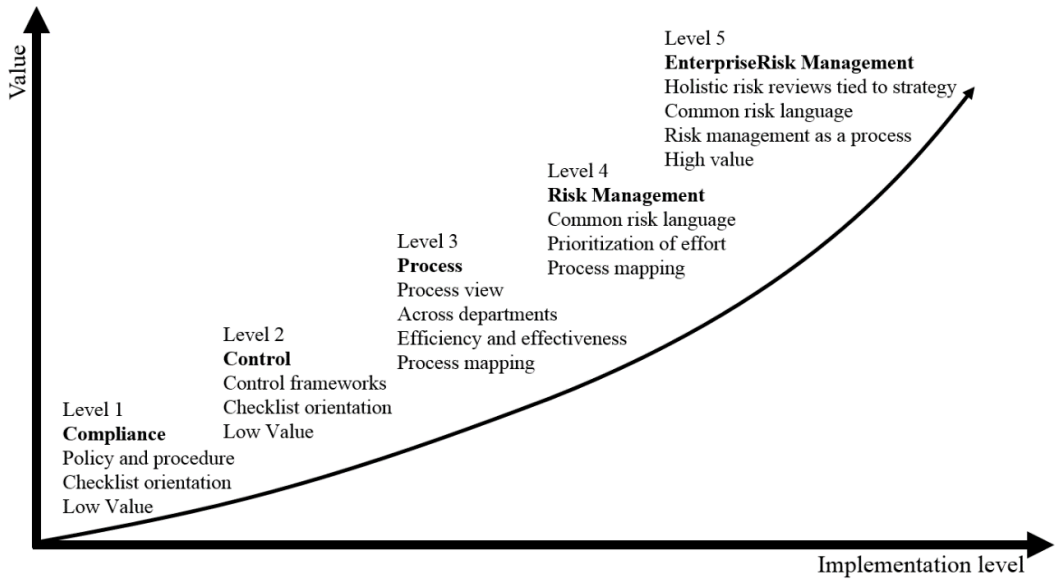

Figure 3: The Journey to ERM.
Source: Bowling, David M. 2005. Success Factors for Implementing Enterprise Risk Management (p.54)

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

This is also confirmed by Kaplan and Mikes (Kaplan, Mikes, 2012) who showed the four most important dimensions: Enterprise risk management consists of active and intrusive processes that (1) are capable of challenging existing assumptions about the world within and outside the organization; (2) communicate risk information with the use of distinct tools (such as risk maps, stress tests, and scenarios); (3) collectively address gaps in the control of risks that other control functions (such as internal audits and other boundary controls) leave unaddressed; and, in doing so, (4) complement - but do not displace - existing management control practices. Each of the taxonomy's (Kaplan, Mikes, 2012) three risk categories - "preventable," "strategic," and "external" - has a different source, a different degree of controllability, and a different approach for identification, mitigation, and management

Out of this review of current models the following essentials according risk management are elaborated from a modelling perspective but also from a human interrelation and implication perspective concluding with the implications of information business itself.

Methodologically/Technically, holistic Risk Management consists itself of 3 steps:

1. Risk Identification - Information Classification
2. Protection of Risk-Areas
3. Active Controls of Risk-Areas

In mid-sized and big enterprises, the effective implementation of Standards and Controls is key for any kind of compliance reporting done by internal and external auditors. When responding to a specific business risk, an auditor should search for relevant and reliable audit evidence and list the accounts and assertions to test in response to that risk. Cognitive research has found that experts / specialists have more complete knowledge and memory organization than novices have a more complete problem representation, which they bring to an unstructured industry task (Hammersley, 2006). IRM was over a long time a not structured task. In the beginning a holistic view on all Information Assets needs to be in place to further classify and segregate the "important to look at" assets from the irrelevant. Further on an appropriate protection of this information assets needs to be established as well as an "over time controlling" of these security measurements.

Intermediate Resume of Literature Review

Information Risk Management could be seen as a meta-discipline for all common risk management models which needs to be considered on top - as the core of any decision-making process is the availability and correctness of information that on which the decision is based. The currently additional appearing risk (1) the change in the information culture, (2) the information is available almost everywhere in real-time via the internet, without any prove of correctness and context, and (3) the technical ability to store, transfer, aggregate, and compute mass data far beyond human capabilities requires specific attention in scientific theory but even so in practical economy.

A summary table of the literature review is attached in the appendix, pointing out the various authors and areas of Risk Management that are to be considered for this research work.

Scientific Design – Methodology

Especially the development of the variables is in focus of this article, as there is no current measurement model for *Information Risk Management* at all / holistically developed yet. The overall approach to determine the measurement variables consists out of a four-step-approach.

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

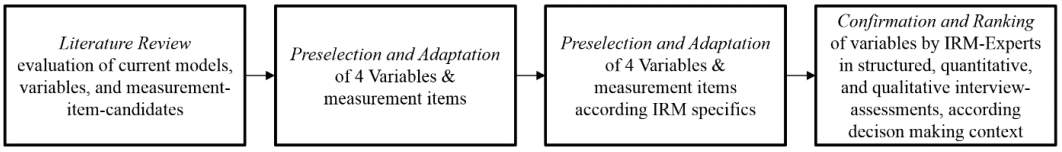

Figure 4: Four-Step-Process: Determining latent exogenous variables.
Source: Author

Identifying the Measurement Variables for Information Risk Management

As described in the previous chapter by Burack (1966) the basic-/ meta- model for any organizational supervision process are the following 3 steps to be undertaken from a pedagogical view: (1) Give clear instructions, based on the knowledge and applicability for employees, (2) Ensure, that instructions are fully understood, concepts are clear, and the purpose why it has to be done is intellectually accepted (and supervise in case of questions), and (3) Check and measure success to identify risks and gaps to adapt and to ultimately reach the organizational goal. Transfer-ring this approach on the topic on IRM, the following 3 Variables could be examined and further on measured:

- *Information Classification*: The need for clear rules and governance on how information is classified and what this means for the company as baseline for any further decisions, it should be clearly defined and transparent to everybody.
- *Information Protection*: The need on protecting the information on an adequate level based on the Information Classification, in all instances (paper based, electronically stored, verbally communicated etc.) - clearly defined and transparent rules should be implemented.
- *Information Controls*: The need of a formalized control-framework to oversee and check the level of fulfillment and herewith the overall risk-situation, to enable corrective and preventive actions, and where needed sanctions.

As discussed in earlier there is a strong need for ongoing and continuous involvement of everybody to apply to specific needs in the direct work surrounding and adapt changes accordingly based on an own broad knowledge - this rep-resents the essential difference - *active participation role* - of everybody in contrast to a strict order taking role in the current observed models. Here the author postulates also a dynamics and bi-directional demand-management. IRM Experts may span the frame of the meta-concept, but will not be able to consider all implications in a special department, because these are based on the organizational setup, formal and informal rules, communication style internally and externally and all this in a highly volatile and dynamic ongoing change. In essence, the IRM Concept rules of a dedicated group or department are as individual, as the communication/organization-needs are. Concluding this discussion that the individuals in the groups need to have a high *IRM-Awareness* level - which is hereby the 4th identified latent exogenous variable to measure the level of IRM (-readiness) in companies.

As mentioned previously, there is no proven scientific model with operationalization / measurement items proposed yet. Consequently, the measurement characterization items identified by the author of this dissertation need to be proven separately. First a transfer from common models out of the literature review was conducted.

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

Proving the Proposed Variables

To prove the proposed variables, an expert interview was conducted to identify and rank the measurement items and consequently the variables themselves in the light of decision making improvement (chosen latent endogenous variables are not discussed in this article). Overall 41 measurement criteria were identified which characterize (load) the 4 chosen variables.

Structured Expert Interviews – Quality and Reliability of Method and Results

Linderman et al. (2011), Mayer (2008), Gläser and Laudel (2009) performed significantly contributing meta-studies on the development of the Expert-Interview-Method. All three agree that the so called Expert Interviews could be conducted in a qualitative and quantitative way - depending on the scientific questions and the limitations in this field. It could also be segregated in structured interviews with dedicated pre-prepared questions, and a story line along the answers are constructed in a SMM (sense making methodology) way. In qualitative interviews situations are openly discussed and recorded. Especially for structured interviews the following four entry conditions need to be considered:

1. The operating range of questions needs to be well balanced - risk of too limited view or specialization is not necessary
2. Specific and well-defined contextual semantic expressions need to be used - ensuring the precision of the result
3. Balanced effectiveness - Ensuring the correct balance of detail-level amongst question areas, value-related ratings/classification needs to be transparent to the interviewee
4. Expert-Context - proving the areas of expertness to ensure applicable questioning Gläser and Laudel (2009) distinguished between two groups of types of questions, (1) *Content based Questions*, and (2) *Functions Based Questions*.

A structured questionnaire - in paper - was examined prior to the interviews containing only *fact-based questions* and *reality based questions* intentionally to eliminate most method-based weaknesses by design. Functions-aspect based questions were formally not asked and recorded. A quantitative result could be examined by questioning the basic impact of operationalization-criteria to the variables and ranking the impact strength, the author of this article chose a "Likert-5 scale" per question. The advantage of using a structured questionnaire is to eliminate uncontrolled answers, it is even seen as advantage if the investigator is present during answering (Friedrichs, 1990). Another advantage of fixed questionnaires is to use well defined wording and sequence of the questions, and indicate a clear scale of meaning and understanding of the answers range. By this, questions can be formulated accurate to generate answers to the hypothesis precisely and exclusively without leaving too much room for different interpretation. In this sense, the author only formulated closed and fully standardized questions (Closed questions are pre-formulated questions - equal for any interviewee). For this case scholars have developed a vast amount of theories which are plausible, proved, and tested about the rules and scales to be used (Friedrichs, 1990). Most prominently the so called "Likert-Scale" is used to measure the attitude of an individual concerning a specific object in a specific situation. All statements are formed in a positive or negative way. The idea of the Likert-scale is the fact that the more strongly the test subject refuses a statement, the further his attitude differs from the formulation of the statement itself.

On-top to the common way of measuring the level of agreement or disagreement, in the expert-interviews also the area of significance for the four variables as a measurement item was questioned per question-set with a simple multiple choice.

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

It must be noted, that Likert-Scaled answers are interpreted as equidistant ranges, in the case of a Likert-5-Scale the equidistance of each answer is equal to 20% of the total possible range. The interviewees were actively reminded about this fact - also in the opening of the interviews there was a clear agreement, that in case the applicability for the chosen area of significance would differ in case of multiple selection from each other, it would be actively noted - in none of the interviews this was the case.

Execution of Expert-Interviews

In summary 10 *Information-Risk-Management-Experts* were interviewed in personal F2F interviews. The selection of IRM Experts was conducted on their publicly known professional experience and career. In the interviews, the confirmation about the used terminology was done verbally at any stage of the interviews to ensure high data quality and preciseness. In the following table the mapping (in column 3 up to column 7) of the developed questions (including literature reference) to the variable is done. As well it the interview results (mean) are shown in the last column.

Table 1. Measurement to variable mapping to results and literature references overview.

Criteria – recursively derived from other scholars scientific investigation fields– adapted to IRM-topic by author	Initial Literature Source, from which the IRM adapted measurement criteria are derived from (by author)	Awareness	Information Classification	Information Protection	Information Controls	Mean (normalized)
To be transparent to the executive board, a register of ALL CRITICAL information assets and all related risks should be in place and up to date at any time	Ashok, P. 2015; Gatzlaff, K. 2010; Banker, M. 2015; Garg, A. 2003	X	X			0,82
Because of the rules and guidelines are formally in place and could be read at any time, it is important to actively train employees affected by the business controls	Spears, J. 2010; I SO /IEC 2000; Furnell, S.2008	X	X			0,96
An EXTERNAL information crisis would cause a significant negative impact to the company (e.g. Information Breach, stolen intellectual property)	Chen, Y. 2001; Xiang, Y.2013	X	X			0,92
Regarding "Information Risk Management" it is important to have a "crises Team" implemented – being able to respond immediately to any threats	Fiordelisi, F. 2011; Kalhoff, A. 2004	X		X	X	0,84
It is important to distinguish between information, that could be stored on public storage locations and information that should be stored on restricted storage locations	Bowling, S. 2005	X		X		0,92
Formal "business controls" need to be agreed and sponsored by the executive board of the company to ensure that they are taken serious and are executed	Kaplan,A. 2015 Auer, M. 2008	X			X	0,94
A lack of transparency in particular on "Information Risks" on executive management level could be a reason for not fully implemented "Information Risk Management" Awareness / Preparedness	Kalan, A. 2015; Kaplan, A. 2012; Iyer, G. 2000	X			X	0,86

To ensure, that the controls are executed in an appropriate way, this should be part of the "role description" of the employees affected	Wiemann, J.M.1989; Hargie, O. 1986	X		X	0,78
To ensure better awareness /preparedness in "Information Risk Management" within companies, it is important to have a formally implemented communication and decision map (defined communication streams and mandates for decision making in crises)	Kruglanski, A. 1996; Auer, M. 2008	X		X	0,9
"Time/Costs" constraints could be a reason for not fully implemented "Information Risk Management" Awareness / Preparedness	Kaplan, A. 2012	X		X	0,88
The value of risk analysis results increases with the company affiliation of the employee	Short, J. 1976; Maxwell, G.M. 1985	X			0,68
An INTERNAL information crisis is less negative impacting the company than an EXTERNAL information crisis	Marshall, G.W. 2007	X			0,74
An INTERNAL information crisis would cause a significant negative impact to the company (e.g. loss of relevant information, non-integer information etc.)	Chen, Y. 2001; Xiang, Y.2013	X			0,76
To ensure better awareness /preparedness in "Information Risk Management" within companies, it is important to do good "Information Security and/or Management" awareness programs to all associates	Ashok, P. 2015; Gatzlaff, K. 2010; Banker, M. 2015; Garg, A. 2003	X			0,9
"New-joiners" should be trained automatically if applicable for their new role	Marshall, G.W. 2007	X			0,88
Smaller groups are more effective in risk assessment then bigger groups	Boos, M, 2000	X			0,8
To ensure better awareness /preparedness in "Information Risk Management" within companies, it is important to have a formal "Learning and Training System" in place	Marshall, G.W. 2007	X			0,78
Regarding "Information Risk Management" it is important to ensure, that the executive board is playing "a significant role" in this (general management buy in – e.g. as part of the crises etc.)	Chen, Y. 2001; Xiang, Y.2013	X			0,88
The "NSA Affair" (disclosure of many secrets by Mr. Snowden in Summer 2013) proved that "Information Risks" are not only relevant for Military and Government	PwC 2015; Gatzlaff, K.2010	X			0,98
However classified information should be only accessible by limited number of people	Campbell, K. 2003		X	X	0,9
Also for critical applications it is possible to outsource this to 3rd party vendors – unauthorized information theft is covered/avoided by contractual terms and conditions	Campbell, K. 2003; Ashok, P.2015		X	X	0,64
It is important that these professionals do have a good inside in the local organization and processes and are not only "headquarters functions"	Campbell, K. 2003; Ashok, P.2015		X		0,94
It is good to involve these professionals in the classification process with a formal approval of all classifications to also ensure the "mandatory involvement"	Campbell, K. 2003; Ashok, P.2015; Diakopoulos, 2015		X		0,68
A consistent and sustainable "information classification" scheme is KEY to identify Information related risks at all (e.g. Confidentiality/ Integrity/Availability/Privacy/Legal requirements)	Campbell, K. 2003; Ashok, P.2015; Diakopoulos, 2015		X		0,88
In general, there is a strong need to have an overview on enterprise level on all classified information asset types (the types only, not the instanced assets themselves!)	Ashok, P.2015; Diakopoulos, 2015		X		0,8
There is a high need to have a number of professional people (e.g. Information Risk Managers) helping the information asset owners with the classifications to ensure an enterprise wide well balanced and calibrated classification over all asset types	Ashok, P.2015; Diakopoulos, 2015		X		0,86

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

It is important to distinguish in particular between these different dimensions (e.g. Confidentiality/Integrity/Availability/Privacy/Legal requirements)	Utz, S. 2001; Bt. Fakhiri, N. 2015; Spears, J. 2008	X			0,8
It is important to have exact definitions on how to classify each of this dimensions (e.g. for confidentiality: public use, internal use, confidential, strictly confidential)	ISO/IEC 2000; Utz, S. 2001; Bt. Fakhiri, N. 2015; Spears, J. 2008	X			0,86
The "information asset owner" should be the person to define the group of people which should have access to the information	Cruz, M.G. 2002; Gazert, N. 2016; Kaplan, A. 2012		X	X	0,78
Formal "business controls" (like SOX, etc.) help to manage "Information Risk Management" activities in an appropriate way in big enterprises	Kaplan, A. 2012; Fiordelisi, F. 2011		X	X	0,76
It is essential for companies, that IT department provides an up to date IT security back-bone (anti-virus, Intrusion detection, etc.)	Diakopoulos, N. 2015; Campbell, K. 2003		X		0,96
For mobile devices there is NO need to encrypt the hard drive because all employees are trained and reliable in handling critical information (to avoid unauthorized information access in case of theft)	Diakopoulos, N. 2015;		X		0,9
Employees should not have "local administrative" accounts on their PCs	Sirirat, S. 2015; Diakopoulos, N. 2015; Campbell, K. 2003		X		0,88
If office doors are not locked in big companies, it is important NOT to leave classified information on the work desks	Posey, C. 2016; Meyer, J.P. 1997		X		0,96
To avoid unauthorized access to PCs, it is important to lock the PCs logically (Screensaver with password) and physically (fix the PC to the desk with e.g. a steel cable)	Diakopoulos, N. 2015		X		0,88
IT department should implement an automated "backup" for specific local (on local PC) folders to avoid data-loss in case of hardware-crashes etc.	Banker, M. 2016		X		0,82
Formal rules and guidelines (Standard Operating Procedures and e.g. "how-to" guidelines) need to be in place to ensure that "business controls" are understood and executed in the correct way	Kaplan, A. 2012			X	0,82
A review on the fulfillment-level could also be done by the people being responsible for the execution	Feldman, M. 2015; Near, J.P.2016			X	0,68
A reason for not fully implemented "Information Risk Management" Awareness / Preparedness could be that there are no significant risks at all (as an outcome of a formal evaluation within the company)	Conceptually inspired by Goedel, K. 1931			X	0,74
A good "tracking system" on the fulfillment level of the "business controls" should be in place	Elbashir, M. 2011			X	0,86

Source: Author's results based on IRM-Expert Interviews

The suggested implications resulting out of the literature review could be seen as fully supported, no contradictive statement was perceived, both methodically and result-based. For variable IRM-Awareness in total 19 questions/criteria were identified and ranked, for variable IRM Information Classification in total 12 questions/criteria were identified and ranked, for the variable IRM-Information-Protection in total 12 questions/criteria were identified and ranked, and for the variable IRM-Information-Controls in total 13 questions/criteria were identified and ranked.

Statistical Method

An individual rating / ranking per measurement criteria could be statistically done, based on the 10 answers given in the interviews by the 10 selected IRM-Experts. It could be ar-

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

gued that the statistical sample on which the results are based on are the numerous decisions (themselves) that the IRM-Experts did themselves or were involved or have observed in their capacity of experts. Thus, a parametric result-calculation (mean and deviation) could be seen as meaningful. Further, it could be observed that the distribution of the results are very homogenously (detailed calculations and results see in annex) also proving the semantical validity of the results represented by the IRM-Experts. Resulting, the normalized mean was calculated (with the standard-distribution) serving as the EMPRIRC-NORM.

Results of Research

Implicitly with proving and ranking the measurement criteria of the four variables, the significance and individual characteristics are also confirmed as well as their significant relevance for characterizing Information Risk Management as such. Secondly, in a qualitative approach, the chosen variables are also confirmed to be seen as a well-fitting selection mirroring decision-making-improvements in the light of IRM-characteristics (qualitative proof of variable candidates).

Table 2. Expert's interview resulting IRM measurement variables' mean.

Variable	Mean Empiric Norm	Normalized mean
IRM Awareness	0,8536	1
Information Protection	0,8533	0,9996
Information Classification	0,8383	0,9820
Information Controls	0,8276	0,9696

Source: author's calculations based on structured IRM-Expert Interviews in Phase 1

It could be summarized, that all chosen variables describing Information-Risk-Management are confirmed also quantitatively, as the audience are Experts with a high level of preciseness and knowledge in the field of information risk management. Also, it must be noted, that 10 Expert interviews were conducted, as mentioned previously, a number of even 3-4 Experts is acceptable for any meaningful investigation. With this the number of Experts is at comparably high level. Finally, the empiric-norm is calculated as IRM-Experts mean. Also, it could be summarized, that all chosen measurements / operationalization of the variables describing Information-Risk-Management transitively and are confirmed qualitatively (transitively) by the IRM Experts as well.

This was the first time that a set of IRM-Experts were interviewed and gave a ranking (mean) of proven variables and measures. The ranking shows some difference in the importance of the different variables in the light of decision making processes - the range of values is between 0,853 and 0,827 showing a comparably homogenous confirmation of the chosen variables as confirming to be characterizing Information Risk Management.

Discussion

Four main variables for describing and measuring Information Risk Management were identified and qualitatively proven (1) IRM-Awareness, (2) IRM-Protection, (3) IRM-Classification and (4) IRM-Control. All four variables shown where proven quantitatively on a comparably high level. Whereas esp. IRM-Awareness is seen as the highest ranked criterion by the IRM Experts – it reflects interestingly also the basis of any pedagogic- or learning theories, where the initial step is to raise attention for the need of the target group, and generate the basic understanding.

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

Also, interesting that the IRM-Protection is seen on an almost similar level. This shows the gender of the overarching goal to "protect" against damage – in a broader scope – to protect against non-optimal decisions. The third criterion proven is the call and need for Information classification. It is seen as the base of any ranking. The target audience needs to make clear differences between the levels of classifications, to also balance and derive the level of investment into protection-measures. In literature, the notion of "crown-jewels" is used to illustrate the question, if e.g. senior executives know about their most valuable assets (here it could be transferred as "information-assets") and further raise the question on having an appropriate protection implemented. The forth criterion identified is the IRM-Controls. Once the other three measures are implemented, it is key to continuously check and improve the measures – also according their economic value. In other words, this represents the willingness of an organization to actively control in an ongoing way the implemented measures and adapt where necessary.

With this further group-comparisons can be conducted. The empiric norm is the baseline to measure the perception on how Information Risk Management contributes to the improvement of decision making. Other groups like senior managers or mid-level managers could be asked for their perception, the results could be compared with this empiric norm to identify deficiencies and gaps, but also areas of conformity - out of this practical organizational changes and remediation activities can be derived. Also, cultural differences in the perception can be elaborated based on this empiric norm. It might be figured out, that there are different levels of perception of Information Risk Management in different cultural spheres. Also, differences in industries are possible, e.g. highly regulated or high-tech industries might have a different level of perception than low knowledge or agricultural areas.

Conclusions

There is a high need to measure Information Risk-Management in a standardized way / model to guarantee comparability amongst different target groups, but also over time with in same target groups to measure also progress, derive corrective and preventive actions, and finally be economically successful in current information and media driven economy.

Future investigations to reference back to this newly generated empiric norm. It must be noted, that his empiric norm was generated for the specific case of Information Risk Management Perception in the light of decision making processes. This means it is not context-fee and could not be taken for other without adaptations. But on the other hand, this is not limited only to decision making, the basic scientific approach and method could be redone for any other context the same way. This means, that besides the empiric norm itself this scientific work also offers a general method to generate potential other empiric norm for other correlations around Information Risk Management.

Annex

Table. Overview on overall statistical results IRM-Expert-Interviews.

Latent Exogenous Variable	Information (IRM) Awareness	Information Classification	Information Protection	Information Controls
No. of valid Experts interviews	10	10	10	10
No. of confirmed measurement criteria	19	12	12	13
Mean over all per variable (normalized)	0,817	0,791	0,817	0,742
Standard deviations per varialbe total (over all measurement items per variable)	0,150	0,184	0,162	0,180
Variance per variable total (over all measurement items per variable)	0,114	0,169	0,134	0163

Source: Author's results

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

References

Ashok, P. (2015). Plug the value leak: Fix your drilling data. *World Oil*, *263* (10), 21-24.

Auer, M. (2008). *Operationelles Risikomanagement bei Finanzinstituten* [Operational risk management in financial institutions]. Weinheim: Wiley-VCH Verlag GmbH & Co.

Ayyub, B. M. (2014). Systems resilience for multihazard environments. *Definition, Metrics, and Valuation for Decision Making, Risk Analysis, 34* (2), 340–355. DOI: 10.1111/risa.12093.

Banker, M. (2015). Cybercrime will cost businesses over $2 trillion. *JUNIPER Research Ltd., 27* (6), 29.

Barney, J. B., & Zhang, S. (2009). The future of Chinese management research. A theory of Chinese management versus a Chinese theory of management. *Management and Organization Review, 5* (1), 15–28. DOI: 10.1111/j.1740-8784.2008.00102.x.

Biehl, M., Cook, W., & Johnston, D. A. (2006). The efficiency of joint decision making in buyer-supplier relationships. *Annals of Operations Research, 145* (1), 15–34. DOI: 10.1007/s10479-006-0023-x.

Biocca, M. (2005). Risk communication and the precautionary principle. *Human and Ecological Risk Assessment: An International Journal, 11* (1), 261–266. DOI: 10.1080/10807030590920097.

Boos, M., Jonas, K. J., & Sassenberg, K. (Eds.) (2000). *Computer-mediated communication in organizations*. Göttingen: Hogrefe.

Bowling, D. M. (2005). Success factors for implementing enterprise risk management. *Bank Accounting & Finance (08943958), 18* (3), 21-66.

Bt Fakhri, N. F. (2015). Information security aligned to enterprise management. *Middle East Journal of Business, 10*, 62-66.

Burack, E. H. (1966). Technology and Some Aspects of Industrial Supervision: *A Model Building Approach. Academy of Management Journal, 9* (1), p43–66.

Chang, C. (2015). Responses to conflicting information in computer-mediated communication. Gender difference as an example. *New Media & Society, 18* (1), 5–24. DOI: 10.1177/1461444814535344.

Cruz, M. G. (2002). *Modeling, measuring and hedging operational risk*. West Sussex: Wiley.

Choi, J. J., Mao, C. X., & Upadhyay, A. D. (2013). Corporate risk management under information asymmetry. *Journal of Business Finance & Accounting, 40* (1-2), 239–271. DOI: 10.1111/jbfa.12008.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements. A coping perspective. *Journal of Management Information Systems, 31* (2), 285–318. DOI: 10.2753/MIS0742-1222310210.

Derek B. C., & Richard, V. C. (2003). Opportunities, precepitations and criminal decisions: A reply to Worthley's critique of situational crime prevention. *Crime Prevention Studies, 16*, 41–96.

Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Communications of the ACM, 59* (2), 56–62.

Elbashir, M. Z., Collier, P. A., & Sutton, S. G. (2011). The role of organizational absorptive capacity in strategic use of business intelligence to support integrated management control systems. *The Accounting Review, l86* (1), 155–184.

Feldman, M. (2015). Certifying and removing disparate impact. In *Proceedings of the 21 st ACM International Conference on Knowledge Discovery and Data Mining*, 259–268.

Fiordelisi, F., Soana, M. G., & Schwizer, P. (2011). Reputational losses and operational risk in banking. *Working paper, University of Rome III.*

Friedrichs, J. (1990). Methoden empirischer Sozialforschung [Methods of empirical social research]. *Opladen, 14*, 172.

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security, 4*, 6-9.

Garg, A., Curtis, J., & Harper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security, 1* (2/3), 74-83.

Gatzert, N., & Schmit, J. (2016). Supporting strategic success through enterprise-wide reputation risk management. *The Journal of Risk Finance, 17* (1), 26-45. https://doi.org/10.1108/JRF-09-2015-0083.

Gläser, J., & Laudel, G. (2009). Experteninterviews und quanlitative Inhaltsanalyse. *Instrumente rekonstruierender Untersuchungen*. VS Verlag für Sozialwissenschaften | Springer, p. 130.

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

Greenwood, W. T. (1974). Future management theory. A "Comparative" evolution to a general theory. *Academy of Management Journal, 17* (3), 503–513. DOI: 10.2307/254653.

Hargie, O. (1986). *A handbook of communication skills*. Worcester: Billing and Sons.

Haws, K., Davis, S., & Dholakia, U. (2016). Salad = success and fries = failure? Conceptualizing and assessing self-control outcome measures in food decision-making research. *Journal of Consumer Behaviour, 15* (2), 99–116. DOI: 10.1002/cb.1560.

Holtgrewe, U. (2014). New technologies. The future and the present of work in information and communication technology. *New Technology, Work and Employment, 29* (1), 9–24. DOI: 10.1111/ntwe.12025.

Huang, K., Dyerson, R., Wu, L., & Harindranath, G. (2015). From temporary competitive advantage to sustainable competitive advantage. *British Journal of Management, 26* (4), 617–636. DOI: 10.1111/1467-8551.12104.

Iyer, G., & Soberman, D. (2000). Markets for product modification information. *Marketing Science, 19* (3), 203–225.

Kalhof, A. H., & Haas, M. (2004). Operational risk – management based on the current loss data situation. In: Cruz, M. (Ed.), *Operational risk modelling and analysis: Theory and practice*. Navarra: Risk Books, 11.

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review, 90*, 48-60.

Kruglanski, A. (1996). Motivated social cognition: principles of the interface. In E. T. Higgins & A. W. Kruglanski (Eds.), *Social psychology: Handbook of basic principles* (pp. 493-520). New York: Guilford.

Linderman, A., Baker, J., & Bosacker, S. C. (2011). Surfacing and transferring expert knowledge: The sense-making interview. *Human Resource Development International, 14* (3), 353–362.

Marshall, G. W., Michaels, C. E., & Mulki, J. P. (2007). Workplace isolation: Exploring the construct and its measurements. *Psychology & Marketing, 24* (3), 195–223.

Maxwell, G. M. (1985). Behavior of lovers: Measuring the closeness of relationships. *Journal of Social & Personal Relationships, 2*, 215–238.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13* (3), 334-359.

Pfeiffer, T., & Schneider, G. (2010). Capital budgeting, information timing, and the value of abandonment options. *Management Accounting Research, 21* (4), 238–250. DOI: 10.1016/j.mar.2010.07.001.

Power, D. J. (2008). Understanding data-driven decision support systems. *Information Systems Management, 25* (2), 149–154. DOI: 10.1080/10580530801941124.

Posey, C., Roberts, T. L., & Lowry, P. B. (2016). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32* (4), 179–214.

PwC Reporting (2015). Cost of UK cybersecurity breaches doubles. *Information Management Journal, 49* (4), 10.

Schultz, C., Salomo, S., Brentani, U., & Kleinschmidt, E. J. (2013). How formal control influences decision-making clarity and innovation performance. *Journal of Product Innovation Management, 30* (3), 430–447. DOI: 10.1111/jpim.12009.

Short, J., Williams, E., & Christie, B. (1976). The social psychology of telecommunications. *Wiley*.

Spears, J. L. (2010). User participation in information system security risk management. *MIS Quarterly, 34* (3), 503.

Srisawang, S. (2015). Factors affecting computer crime protection behavior practices. In: *Conference Proceedings: IT and open innovation PACIS 2015*. Singapore.

Utz, S., & Sassenberg, K. (2001). Attachment to a virtual seminar: The role of experience, motives, and fulfillment of expectations. In U. D. Reips & M. Bosnjak (Eds.), *Dimensions of internet science* (pp. 323-336). Lengerich: Pabst.

Wagner, H. T., Beimborn, D., & Weitzel, T. (2014). How social capital among information technology and business units drives operational alignment and IT business value. *Journal of Management Information Systems*, *31* (1), 241–272. DOI: 10.2753/MIS0742-1222310110.

Wiemann, J. M., & Kelly, C.W. (1981). Pragmatics of interpersonal competence. In C. Wilder-Mott & J. H. Weakland (Eds.), *Rigor and imagination: Essays from the legacy of Gregory Bateson* (pp. 283-298). New York: Praeger.

PROBLEMS
OF MANAGEMENT
IN THE 21st CENTURY
Vol. 12, No. 1, 2017

Xiang, Y., & Sarvary, M. (2013). Buying and selling information under competition. *Quantitative Marketing and Economics, 11* (3), 321–351.

Received: *April 24, 2017* Accepted: *June 28, 2017*

Stefan Schwerd	Dipl. Inf. (Univ.), MBA (Univ.), Country Head Information Security and Risk Management Germany at a global pharmaceutical company, 83607 Holzkirchen, Germany. PhD Student, University of Latvia, Riga, Latvia. E-mail: stefan@schwerd.eu
Richard Mayr	Dipl. Inf. (FH), CEO at a field force automation company, 83026 Rosenheim, Germany. PhD Student, University of Latvia, Riga, Latvia. E-mail: mail@richardmayr.de