Downloaded from orbit.dtu.dk on: May 30, 2024



DTU Library

The Professionalization of Risk Management: What Role can the ISO 31000 Risk Management Principles Play?

Olechowski, Alison; Oehmen, Josef; Seering, W.; Ben-Daya, M.

Published in:
International Journal of Project Management

Link to article, DOI:
10.1016/j.ijproman.2016.08.002

Publication date:
2016

Document Version
Peer reviewed version

Link back to DTU Orbit

Citation (APA):
Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The Professionalization of Risk Management: What Role can the ISO 31000 Risk Management Principles Play? *International Journal of Project Management*, *34*, 1568-1578. https://doi.org/10.1016/j.ijproman.2016.08.002

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

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

The Professionalization of Risk Management: What Role can the ISO 31000 Risk Management Principles Play?

A. Olechowski, J. Oehmen, W. Seering, M. Ben-Daya

Alison Olechowski
PhD Candidate
Massachusetts Institute of Technology
Department of Mechanical Engineering
Email: alisono@mit.edu

Prof. Josef Oehmen
Associate Professor, PhD
Technical University of Denmark
Department of Management Engineering
Email: jooehm@dtu.dk

Prof. Warren Seering
Professor
Massachusetts Institute of Technology
Department of Mechanical Engineering
Email: seering@mit.edu

Prof. Mohamed Ben-Daya
Professor
American University of Sharjah
Industrial Engineering Department
Email: mbendaya@aus.edu

ABSTRACT

Risk management is increasingly seen as a means of improving the likelihood of success in complex engineering projects. Yet the presence of a legitimacy gap, driven by the lack of empirical validation of published best practices, might explain low adoption of risk management on projects. We present an empirical investigation and discussion of the eleven principles of the ISO 31000:2009 Risk Management Standard via a large-scale survey of engineering and product development practitioners. Adhering to the risk management principles at a high level was found to be a significant factor in

better reaching cost, schedule, technical and customer targets, in addition to achieving a more stable project execution. This finding suggests that, rather than a single rigid standard or an ever-changing set of detailed methods, the ISO principles have potential to be the basis for our shared understanding of best practice, and to catalyze the professionalization of project risk management.

Keywords: ISO 31000; project risk management; risk management standard; survey analysis; professionalization of risk management

1 INTRODUCTION

Risk management is increasingly seen as a means of improving the likelihood of success in the complex, multi-functional and challenging task of managing engineering and product development projects. Studies show that project risks affect outcomes in a number of industries (Wallace & Keil 2004; Mishra et al. 2016). Yet studies have shown that risk management practices are poorly adopted by project managers (Kutsch & Hall 2009; Raz et al. 2002; Grant & Pennypacker 2006; Ibbs & Kwak 2000; Papke-Shields et al. 2010). How do project managers decide which risk management practices to engage in, and how can they have confidence in the value of investing in such processes?

Given the increasing ad hoc implementation of risk management practices by project managers, the under-usage of existing methods due to lack of legitimacy, and thus the search for and generation of numerous prescriptive guidelines, we recognize the need for studies that validate methods for project risk management, and lead to professionalization of the field. But we must balance this search for validation of prescriptive methods with the warnings of the contingency point-of-view, and avoid a one-size-fits-all solution.

In this paper we propose the use of risk management principles as an alternative to specific practices or tools. We argue that these principles provide guidance to project managers in establishing a risk management process, while recognizing that each project is different. We seek to explore the potential of one set of such risk management principles in this work. This study will report the results of an empirical study in the engineering and product development context of the effectiveness of the principles included in one promising standard - the ISO 31000:2009 Risk Management guideline.

2 LITERATURE REVIEW

We begin with a discussion of the state of professionalization of project risk management. The establishment of a formal body of knowledge is seen as a critical step towards professionalization of a field (Wirth & Tryloff 1995). This body of knowledge provides a common understanding of industry best practices in the field, allowing for teaching, certification, and common competence improvement. The complex and diverse nature of project management has led to various communities of practice and bodies of knowledge, and it has been a challenge to reach a common and workable understanding of project management best practices (Bresnen 2016). Some research has been directed towards identifying critical success factors in project management, well reviewed by Fortune and White (2006), which include risk addressing, assessment and management.

We can learn about the likely future path to professionalization of risk management from discussions of professionalization of project management (Duncan 1995; Morris et al. 2006; Muzio et al. 2011). We see the same patterns beginning to play out in the project risk management field. There exist a great number of popular guidelines for implementing risk management in engineering project domains (INCOSE 2011; DoD 2006; International Organization for Standardization 2009; Project Management Institute 2008; NASA 2008). These guidelines generally consist of a list of so-called “best practices” in risk management, assumed to be captured from experience and lessons learned over time; however, the guidelines fail to include evidence to support the effectiveness of their prescriptions. What results is an ad-hoc application of risk

management processes, if there is any application at all; there is both a lack of legitimacy and a lack of unity towards one common best practice understanding.

To this point, Kutsch and Hall (2009) argue that despite a great deal of work towards prescriptive risk management guidelines, little work exists to reveal what risk management is actually done (or not done) by project managers, and why. Kutsch and Hall report that one third of the 102 IT project managers in their study conducted no project risk management process on their project at all, because they could not justify the cost of such processes. In a number of other studies of project management maturity, risk management methods are included as a category of competence, and is consistently found to be relatively immature (Ibbs & Kwak 2000; Papke-Shields et al. 2010; Grant & Pennypacker 2006). It appears that even though project managers might be aware that risk management practices exist, project managers fail to implement these practices. Little evidence exists to prove the legitimacy of these methods, and persuade project managers to invest in risk management.

Legitimacy is critical in the decision of an organization to adopt a standard (Brunsson et al. 2012), but is difficult to assess from the standard itself. We can look to the literature to provide legitimacy through empirical studies that investigate both important factors in risk management and if and how risk management leads to project success. We highlight below the limited set of studies that have attempted such evaluations.

2.1 Empirical evaluations of project risk management practices

Agreement on a standard set of risk management methods would not only be a catalyst for professionalization, but would allow for more coordinated and integrated research on the effectiveness of risk management practices.

A meta-analysis of empirical evidence from previous studies of risk management in IT projects seeks to address the question of whether risk management actually contributes to project success (de Bakker et al. 2010). The authors identify that senior management support of and user participation in risk management are highly influential on project success. Further, the authors warn that the knowledge of risks alone (or what they call the “evaluation approach” as opposed to the “management approach”) is not enough to contribute to project success.

In a study of 291 development programs, Oehmen et al. (2014) examined 30 proposed risk management best practices and showed that more than 70% show no significant association with desirable product development or risk management outcomes, with only indirect impact on product and project success in impact measures. These findings suggest that we should take a more critical look at the conventionally recommended risk management practices.

A project management focused study, investigating specific methods extracted from the PMBOK, surveyed 142 practitioners (Papke-Shields et al. 2010). The risk-related methods include “quantitative risk analysis” and “risk register updates,” for example. Of particular interest to this work is the finding that risk-related methods were found to be the least used of 10 knowledge areas. The authors found a significant difference in the

level of use of risk management methods between the successful and unsuccessful projects in the study, suggesting that even though infrequently used, the more risk management, the better project outcomes.

An empirical study based on over 100 product development projects in various industries was reported by Raz et al. (2002). This study found that only a small number of projects used any kind of risk management practices. Those projects that did use risk management, however, were found to have better met time and budget goals.

In another study, this time with evidence from a questionnaire of 84 project managers from the software and high-tech industries, Raz and Michael (2001) start from a list of 38 risk management tools from the literature and identify 28 tools that are used by organizations with better project management performance. Examples of such tools include ranking of risks, risk probability assessment, and checklists.

Mu et al. (2009) propose and validate a risk management framework for new product development which decomposes risk management into three factors: organizational, technological, and marketing. Validation was performed empirically through a survey of Chinese firms. The results show that risk management strategies aimed at those three factors contribute both individually and interactively to the performance of new product development.

A study of seven hundred project managers by Zwikael and Ahn (2011) explores the effectiveness of risk management practices to reduce risks in project management, and to lead to project success. The analysis found that risk was negatively correlated with

project success, but that effective risk management planning could moderate the effect of those risks.

Given the lack of agreement on a collection of best practices for risk management, the previously cited studies tend to cover different sets of tools, methods, or tasks, sometimes at different levels of abstraction. This makes it difficult to take action based on their findings; it would require a project manager to assemble their own method from the various lists of identified practices, rather than adopt an existing unifying guideline or standard. But what this work does largely do is to provide evidence that risk management consisting of some combination of existing practices can lead to better project outcomes.

2.2 The contingency perspective

There is evidence that suggests that standardized methods for project management may increase project success (Milosevic & Patanakul 2005), and it can be argued that standardized processes allow for more accessible and transferable gained experiences and learning in the organization (Perminova et al. 2008). Yet those who maintain a contingency view of project risk question the need for a unifying body of knowledge in risk management. The contingency perspective argues that various project and uncertainty characteristics call for different risk management approaches, and therefore a one-size-fits-all standard risk management practice is not ideal (Teller et al. 2014; Jun et al. 2011; Miterev et al. 2016; Williams 2005; Thamhain 2013).

We suggest in this paper that a set of principles, rather than a set of prescriptive methods, may represent a happy medium between foundational, professionalization-

building knowledge, and contingency based customization. The set of risk management principles studied here is from the ISO 31000:2009 risk management standard. To our knowledge, this set of principles is the only collection of its type published as part of a major standard, aiming to provide high-level guidance regarding the creation, evaluation, selection and implementation of concrete risk management practices.

3 THE ISO 31000:2009 RISK MANAGEMENT STANDARD

The ISO 31000:2009 Risk Management Standard was created to be widely applicable across contexts and projects (International Organization for Standardization 2009). The International Organization for Standardization (ISO) has developed and released a number of highly popular standards, most notably ISO 9000 for quality management, and ISO 14000 for environmental management (Heras-Saizarbitoria & Boiral 2013; Anttila 1992; Su et al. 2015). Given the high reputation and wide acceptance of these other ISO standards, and the growing uptake of risk management efforts that better address the effects of uncertainty in the engineering project process, one can assume that the engineering project community will keenly look into this relatively new standard.

The standard defines risk as “the effect of uncertainty on objectives.” By this definition, risk and uncertainty are fundamentally connected; efforts to reduce or mitigate risk are efforts that address the effects of uncertainty. Interpreting the definition for the engineering project context helps to define the relevant scope of risk management. The objectives of project management are traditionally viewed as quality, cost and time. We have already discussed the great number of uncertainties in managing engineering projects. Effect is defined by ISO to mean the deviation from the expected. Thus, risk on projects is the deviation from expected projects objectives caused by uncertainty.

This definition of risk therefore encompasses a wide-array of previously studied engineering uncertainties and challenges, from part integration risk to customer satisfaction risk to product safety risk to testing equipment availability risk.

In its introduction, the standard lists additional outcomes which are enabled by risk management, including:

- Increased likelihood of achieving objectives
- Establish a reliable basis for decision making and planning
- Minimize losses
- Be aware of the need to identify and treat risk throughout the organization

3.1 Creation of ISO 31000

The ISO 31000:2009 Standard was prepared by the ISO Technical Management Based Working Group on risk management (International Organization for Standardization 2009). Purdy (2010) explains that the working group was made up of experts nominated from 28 countries and various specialist organizations. The consensus-driven process took over four years, and there were over seven drafts of the standard. Drafts are circulated to member bodies for voting, and a 75% approval is required for publication (International Organization for Standardization 2009). The standard cites no other works, and so leaves the genesis of many of its concepts unknown. Some of the ISO 31000 standard is similar to an earlier standard, the AS/NZS 4360:2004 standard for risk management, jointly published by Standards Australia and Standards New Zealand (Standards Australia 2004). However the ISO standard introduces a new definition of risk and eleven risk management principles that were not present in AS/NZS 4360.

The eleven principles are the focus of this work. According to the suggestions of the ISO standard, if the principles are complied with, they will lead to effective risk management. The principles are:

1. Risk management creates value
2. Risk management is an integral part of organizational processes
3. Risk management is part of decision making
4. Risk management explicitly addresses uncertainty
5. Risk management is systematic, structured and timely
6. Risk management is based on the best available information
7. Risk management is tailored
8. Risk management takes human and cultural factors into account
9. Risk management is transparent and inclusive
10. Risk management is dynamic, iterative and responsive to change
11. Risk management facilitates continual improvement

We know little about the creation or intention of these principles. We assume that one approach to generating a set of principles it to aim for a list of mutually exclusive and collectively exhaustive (in describing successful risk management) items, where the latter is more important than the former. For a concept as broad as risk management, we would imagine that this is a challenging undertaking. If an additional requirement is widespread applicability, a certain level of abstraction (as seen in the principles) is understandable.

3.2 Critiques of ISO 31000

A number of authors have critically examined the ISO 31000 standard as a whole. Aven (2011) critiques the uncertainty- and risk- related vocabulary of the standard from a reliability and safety point of view. The author argues that the guide fails to provide consistent and meaningful definitions of key concepts. In a broader critique of the standard, Leitch (2010) concludes that the standard is vague and lacks a mathematical

base. He attributes the vagueness to the process, given that the standard was created from a consensus-based process involving people from all over the world, speaking different languages. Although it is important to conceptually examine the fundamental definitions on which the standard is built, neither of these papers involve actual evidence to evaluate the effectiveness of the ISO 31000 standard, and its potential for impact in industry.

By reviewing past crises from a risk management perspective and retroactively applying ISO 31000, Lalonde and Boiral (2012) explore limitations of implementation and raise questions about the effectiveness of the standard. The authors warn that the adoption of a risk management guideline is not as important as the actions risk managers take. The authors do praise the holistic nature of the guideline. Interpreting their praise with reference to the principles, they point to the inclusion of the positive value-add point of view (principle 1 - risk management creates value) and principle 7 (risk management is tailored) for suggesting that formality will only get you so far.

Addressing the gap in measured effectiveness of the claims of various risk management guidelines, this paper presents an empirical evaluation of the eleven ISO 31000 risk management principles and of their effect on risk management and project management outcomes. We also test the relationships between the principles.

4 SURVEY OF ENGINEERING PRACTITIONERS

The goal of this work is to empirically investigate the effectiveness of the ISO 31000 risk management principles in the engineering industry. As a means of collecting empirical evidence, we conducted a large-scale survey of engineering practitioners (Oehmen et

al. 2014). The survey was distributed to six major aerospace and defense organizations and one government risk management function. To gain responses from a wider variety of practitioners and organizations, the survey was also administered via professional association mailing lists.

Of the 291 respondents who began the survey, 215 respondents completed the final portion of the survey. Respondents were permitted to leave answers blank.

Table I provides additional details on the survey population. Each survey respondent was asked to answer the questions based on a single project which they had completed.

[Table I]

When considering the generalizability of the analysis, it should be noted that half of the respondents were from the aerospace and defense industry, although a wide variety of industries are represented. Similarly, only 6% of the survey respondents were from small organizations (with annual budgets less than 1 million USD).

The survey collected extensive information (171 questions) from each respondent about a past project, specifically regarding project outcomes and risk management process. The survey addressed methods and practices in the areas of risk analysis, risk evaluation, decision-making, and risk monitoring. As previously discussed, this paper will focus on an in-depth analysis of the eleven questions asked about the ISO 31000 risk management principles (see Table II).

Questions on use of practices and outcomes were asked on a five-point symmetric Likert scale, i.e. five discrete options ranging from “never” to “always,” or from “strongly disagree” to “strongly agree”.

The survey included high-level outcome questions which covered the traditional project goals (success with regards to cost, schedule, technical performance and customer satisfaction targets). Outcome questions regarding intermediary risk management outcomes were also included, for example stability of the project and execution of risk identification and mitigation. These outcomes are analogous to those listed in the standard (and presented in the introduction) as being enabled by effective risk management. A complete list of the outcomes considered in this analysis is presented in the following section.

5 RESULTS

Table II presents the responses to the survey questions regarding the ISO 31000 Risk Management principles. The respondents were asked to “Please indicate your assessment of the way risk management was executed [on this project].” The principles were phrased in the active style, for example “Our risk management creates and protects value.” The respondents were asked to respond on a 5-point scale, from “Strongly Disagree” to “Strongly Agree.”

[Table II]

A review of the distributions presented in Table II reveals that the responses tended to be mound-shaped and near-normal, suggesting that traditional parametric data analysis relying on the normal assumption would be valid. However given that there were only

five discrete response options for both the questions regarding the principles and the outcomes, the data is ordinal but not continuous; therefore as a conservative precaution, non-parametric data analysis methods were used in this study. The distributions are generally centered on response 4, “Agree” and show a skewed distribution, with few responses in the low (“Strongly Disagree”) tail.

Table III shows the response distribution to the outcome questions. Note that the target question responses were asked on a different scale than the intermediary outcome questions, but both have been recoded to a 1 – 5 scale for analysis.

The four target questions were asked under the heading: “Please rate the overall program/project success for your organization.” The intermediary outcome questions were asked under the heading: “How strongly do the following statements apply to the overall project/program execution?”

[Table III]

5.1 Exploring the relationships among the principles

We first examine the relationship among the eleven ISO 31000 risk management principles of Table II.

The Goodman Kruskal Gamma is an ordinal measure of the association between two variables (Sheskin 2011). In other words, it is an indication of whether one variable tends to increase with another. The Gamma between each pair of principles is presented in Table IV. Note that the matrix is symmetric since there is no implied causal relationship. For the majority of pairs, the Gamma association is significant (null-

hypothesis: Gamma = 0) at the α = 0.05 level. Where there is no significance to the association, we leave the matrix entry empty.

[Table IV]

Examination of the associations in Table IV shows two groups of more highly associated principles, as highlighted by the thicker box border. The principles within these group, or clusters, associate highly with one another, while associating less strongly with the principles outside of their group.

The first cluster (cluster A) includes the following four principles:

- Creates and protects value (Principle 1)
- An integral part of all organizational processes (Principle 2)
- Part of decision making (Principle 3)
- Facilitates continual improvement (Principle 11)

The second cluster (cluster B) is composed of the following six principles:

- Explicitly addresses uncertainty (Principle 4)
- Systematic, structured and timely (Principle 5)
- Based on the best available information (Principle 6)
- Tailored (Principle 7)
- Transparent and inclusive (Principle 9)
- Dynamic, iterative, and responsive to change (Principle 10)

The strength of the clusters is evidenced by the fact that all associations over 0.5 are contained within either cluster A or cluster B, with the exception being the association between principles 7 and 8. Further, neither cluster contains any associations lower than the highest association outside of the cluster.

This clustering was formally confirmed via variable clustering based on a principle component analysis using the SAS VARCLUS algorithm (SAS Institute Inc. 2014).

Formal clustering suggested that principle 8 “Risk management takes human and cultural factors into account” be included in cluster B, however we choose to exclude it from the cluster to highlight the fact that its associations are considerably weaker than those of the rest of cluster B. We recommend future work towards building on our understanding the role of individuals and culture in project risk management (Liu et al. 2014).

5.2 Testing the effect of each principle on outcomes

We now analyze the data to see which if any variables correlate significantly with the outcome variables and therefore project success.

We first use an ordinal logistic regression and resulting Whole Model Test, Lack of Fit statistics, and R^2 values (Sheskin 2011) to statistically check whether the models are sufficient, i.e. that the eleven principles explain the project outcomes in some significant way. Details of these tests are included in the Appendix, with statistics in Table A. The results confirm that it is meaningful to investigate the effects of the individual variables in the model (the eleven principles) on outcomes.

We test the effect of each risk management principle on each outcome variable using the Effect Likelihood Ratio test (Sheskin 2011). The effect likelihood ratio is calculated using the chi-square statistic. It is a test for a difference between a model including all variables (all eleven principles), and one with the variable (principle) of interest removed. The test measures how much more likely the outcome data is to be from the model consisting of all eleven principles, or of the model without the principle of interest (i.e. the remaining 10 principles). If the p-value is non-significant (in this case greater

than α=0.05) there is no statistical significance for the variable of interest to be included in the explanatory model, and therefore we interpret the principle to not have a statistically significant effect on the outcome. Table V lists the calculated p-values for each outcome model. Significant p-values are bolded.

This analysis indicates that only some of the eleven principles are meaningful in explaining any one of the outcomes. It should also be noted that the significant variables were not the same consistent set for each of the outcomes; however, each of the eleven principles except #8 was found to be a significant factor in at least one of the seven outcomes.

[Table V]

Although the ordinal logistic model does generate parameter estimates for a full 44 term model, we will not examine these estimates in detail since the goal of this analysis is to look for those variables which standout as significant. We expect that given the complexity of the engineering endeavor, it is unlikely that a model of the ISO principles alone would be accurate enough to be fully explanatory.

6 DISCUSSION

We discuss the results of the survey analysis in two parts: first implications of the associations between the 11 ISO risk management principles, and next a discussion of the revealed relationship between the principles and project outcomes.

6.1 Implications of the clustering of the principles

This is the first study that empirically reveals the relationship between individual risk management tools, methods or principles. The observation of two clusters of risk

management principles supports the assertion that there are two fundamentally different types of principles included in the standard. The low cross-association between the clusters suggests that the two groups of principles make up independent conceptual structures, and are not first-order dependent. Therefore when designing a risk management framework, or improving the current system, it is possible to drive these two structures independently and simultaneously.

The first cluster (A) addresses the extent to which risk management is embedded in the project process and the organization; risk management is an integral part of all organizational processes; it is part of decision making; it facilitates continual improvement, and it creates and protects value. The second cluster (B) is composed of those principles related to characterizing the risk management process: the process is systematic, structured, and timely; it is based on the best available information and explicitly addresses uncertainty; it is tailored; it is transparent and inclusive, dynamic, iterative and responsive to change. Each of these principles could be interpreted as a guideline for the design of the risk management process. They are requirements for effective risk management. A high level of fidelity to each of these principles indicates an efficient and mature risk management process in the organization. The results for cluster B suggest that a high quality and sophisticated risk management process will lead to strong outcomes on basic project and process metrics. Cluster A suggests that positive outcomes can also be achieved through ensuring that the risk management process is integrated with decision-making, continuous improvement, and the rest of the engineering organization.

6.2 Implications of the relationship between the principles and project outcomes

The statistical significance (Whole Model Test p-values less than 0.05, see the Appendix) of all eleven ISO 31000 Risk Management Principles indicates that the set of principles as a whole is appropriate for project risk management. The standard states that “for risk management to be effective, an organization should at all levels comply with the principles” (ISO 2009b) and the results in this paper support this statement regarding the outcomes that have been tested. The eleven principles together have impact not only on effective risk management but also on the stability of the program and the overall achievement of cost, schedule, performance and customer satisfaction targets.

It is not surprising that the collective wisdom of the many professionals involved in the creation of the ISO 31000 standard is powerful. As is the case in many aspects of the engineering project process, methods and tools have developed from the craftsman tradition; if something works for one project, it is kept for the next. Over time, processes are refined through trial and error; they do not necessarily receive academic validation or empirical testing. In this instance, the analysis shows agreement between the experience-based insights of the risk management community and empirical evidence from industry.

The principles are generally high-level (for example “Risk Management creates and protects value”), and could be seen as descriptors of an effective risk management process rather than specific risk management practices to implement. It is perhaps for this reason that they prove to be significantly important to project success; they are, in fact, a set of risk management performance measures already, and their significance in

modeling more high-level project outcomes is an indication of risk management's positive impact on engineering projects.

The reported low (<0.5) R^2 values (see Table A in Appendix) for the models indicate that these principles do not entirely or exhaustively explain the project outcomes, as would be expected. There are innumerable additional factors that influence an engineering project – both controllable and uncontrollable – and these would be impossible to completely capture in a survey. For that reason, the fact that the models created from the eleven principles alone were found to be statistically significant is intriguing and suggests that the relationship between engineering project success and risk management deserves to be further explored.

Analysis of the significance of the individual principles indicates that each principle had a significant contribution to at least one outcome, and each outcome was significantly affected by at least two principles. No principle was significant for all outcomes. The principle "risk management is part of decision making" has a significant effect in five of the seven outcomes. This implies that risk management analysis and results are a valuable input to the decision-making process in project management, not simply valuable as a separate risk and mitigation catalog. Project management, product development and process decisions can all benefit from feedback from risk management.

Additionally, three risk management process based principles (explicitly addresses uncertainty, tailored, transparent and inclusive) each have a significant effect in three

outcome models. Besides decision-making, one integration related principle - integral part of all organizational processes – shows a significant effect in three outcomes.

Comparing these results to those highlighted in the paper's introduction, we see agreement with the conclusion of de Bakker et al. that senior management support of and user participation in risk management are highly influential on project success (de Bakker et al. 2010). We argue that these two factors are reflected in the principle "transparent and inclusive" which was found in this study to have a significant effect on positive project outcomes.

Further, de Bakker et al. (2010) warn that the knowledge of risks alone (or what they call the "evaluation approach" as opposed to the "management approach") is not enough to contribute to project success. We find evidence to support this perspective, given the positive role of the principles "part of decision-making" and "an integral part of all organization processes," both principles calling for action and not simply raising awareness (i.e. such as the principle "based on the best available information").

Another comparison to prior literature – that of Raz and Michael (2001)– reveals agreement with our findings. The risk management tools evaluated in their study are more specific than the principles investigated in this study; however, there are obvious mappings between the set of tools associated with better performing project management, revealed in the Raz and Michael study, and the principles in ours. For example, checklists, risk impact and probability assessments, and revision of risk assessments lead to risk management that is "systematic structured and timely";

subcontractor management, customer satisfaction surveys, and critical risk reporting to senior management ensure that risk management is “transparent and inclusive”.

The significant relationships among principles and outcomes should inform the risk management professional of where to focus initial resource efforts. It is important to clearly define where risk management can be shared with all stakeholders in order to be a part of decision-making and organizational processes at all levels. The risk management process must be tailored to the project and organization, while also being transparent and inclusive to all those stakeholders. Risk management must consider and explicitly address its foundation of uncertainty.

If the organization is looking for a particular outcome as a key driver for risk management, they can adjust their risk management focus appropriately. For example, if the stability of the project is important, the risk management process should be designed to be transparent and inclusive, facilitate continuous improvement of processes and practices, and be a part of decision-making. Similarly, if the product’s cost target is of high importance, risk management focus should be placed on basing the analysis on the best available information, and ensuring the risk management is an integral part in all organizational processes.

The principle “risk management takes human and cultural factors into account” does not show a significant effect on any of the outcomes. It is possible that the true effect of this principle has not been captured in the seven outcomes in this study. Further analysis is necessary to better understand this principle’s role.

6.3 Limitations and future work

The following limitations are important to consider when interpreting these results. The survey is taken post-project and so recollection of program details may not be accurate. The analysis relies on self-reported outcomes (including outcome success and failure) that could be biased by the experience of the respondent. The responses reflect the perceptions of the respondents, which was not necessarily the reality of the project. The survey was self-administered online; to address potential misinterpretation of the questions, clear descriptions and examples were included throughout the survey and opportunities were given to comment on ambiguity of individual questions.

There is the potential for self-selection bias, where those who chose to respond to the survey did so because of an already strong opinion about risk management, and others avoided the survey. A preliminary check to avoid a bias in the analysis due to various factors (e.g. industries, roles, project size) was performed for this analysis and showed no obvious influence of any particular group.

Although the sample included a diverse mix of engineering projects, the statistical findings from this data set are not necessarily generalizable beyond this sample. The sample was strongly composed of large, aerospace and defense organizations and thus may not generalize outside of that population.

The empirical correlations presented in this work are informative and suggest actionable findings. However it is important to remember that these statistical correlations do not necessarily indicate causation. Further work should investigate the cause-and-effect

relationship between project outcomes and these principles. Qualitative validation would add significant power to these findings.

7 CONCLUSIONS

Risk management is increasingly seen in industry as a tool for improving engineering project success, but practices remain ad-hoc and non-standardized. Yet there is evidence to suggest that a one-size-fits-all approach to risk management best practice is not the right choice, given the complexity and diversity of modern projects. The new ISO 31000 risk management standard was introduced with the promise of universal applicability and included eleven principles for effective risk management. The high-level principles show the potential to be a compromise between a unifying standard and a collection of ad-hoc tools and methods. This study empirically evaluated the ISO standard via those eleven principles, both investigating their inter-relationship and testing their effect on project outcomes.

This paper reveals insights from various analysis perspectives. When we explored the relationship among the eleven ISO 31000 risk management principles the principles were found to cluster into two distinct association groups: one related to the capabilities of the risk management process itself, and the other related to the strength of the interfaces between the risk management process and the other functions of the project and organization. The emergence of these two main clusters suggests the importance of a sophisticated, mature risk management process that does not stand on its own, but is integrated well into the rest of the project and organization.

Empirical evidence from the statistical analysis suggests that the ISO 31000 is indeed a promising guideline for the establishment of risk management in the engineering management community. Adhering to the risk management principles at a high level was found to be a significant factor in better reaching cost, schedule, technical and customer targets, in addition to achieving a more stable project execution. We believe that this provides evidence of the potential for the principles to form the basis of a project risk management body of knowledge and to have a strong impact on the professionalization of the risk management function.

An investigation of the power of the eleven risk management principles to explain positive project outcomes revealed evidence that there is a link between quality risk management and successful projects. These findings agree with the limited prior work in related fields of IT, software and high-tech projects. This finding provide legitimacy to the standard, and suggests that risk management motivated from the ISO 31000 guideline can lead to project success.

In testing the relationship between each principle and positive project outcomes, we revealed the significant positive effect of the principle “risk management is part of decision-making.” This finding reinforces the idea that risk management should be a core part of the full engineering project management process, and can act as a tool for structured, careful decision-making.

Overall, the results presented here suggest that like its predecessors the ISO 9000 and 14000 standards, the ISO 31000 standard for risk management has the potential to be developed into a highly-adopted and impactful body of knowledge and standard of

practice for the project risk management community. We propose the principles as an alternative to a single rigid standard or a set of ad-hoc practices. We believe the principles can form a foundation on which a shared understanding of best practice and an increase in the collective competence can be built. We hope this study inspires future work on the development of clear methods for the adoption and implementation of the ISO principles.

Acknowledgments

The authors would like to thank the King Fahd University of Petroleum and Minerals in Dhahran, Saudi Arabia, for funding the research reported in this paper through the Center for Clean Water and Clean Energy at MIT and KFUPM under R11-DMN-09. We are also very grateful to the members of our industry focus group, benchmarking partners, professional organizations and academic partners that helped us develop, test and disseminate the survey, most notably AFIT, Futron, INCOSE and NDIA.

Appendix

An ordinal logistic regression (Sheskin 2011) was performed in order to build a model of each of the outcomes (see Table III for a list of all outcomes). We use the non-parametric ordinal logistic regression because the data is not continuous but is ordered. All eleven principles are included in each model as independent variables, with an outcome question as the dependent variable.

With these eleven-variable models created, we first examine the Whole Model Test statistic (analogous to the ANOVA test for continuous variables) to see whether there is statistically significant evidence to suggest that the risk management principles explain

the outcome (Sheskin 2011). The p-values for this test are presented in Table A. For each of the outcomes analyzed here, the Whole Model Test showed statistical significance, indicating that the eleven principles do in fact explain the outcome in some way.

We then check the Lack of Fit statistic (sometimes called the Goodness of Fit test), which indicates whether there is enough information contained in the variables of the model, or whether higher-order terms (for example interaction or polynomial terms) should be added to the model. A Lack of Fit p-value smaller than $\alpha = 0.05$ indicates that additional variables should be considered. The p-values for the Lack of fit test are presented in Table A, along with R^2 values. R^2 values range from 0 to 1 and are a statistical measure of the degree of outcome variation explained by the variation in the eleven ISO principles.

[Table A]

The models for each outcome variable of interest in this work show Whole Model Test p-values smaller than $\alpha = 0.05$, and Lack of Fit test p-values larger than $\alpha = 0.05$, indicating that the models are sufficient and that it would be meaningful to investigate the effects of the individual variables in the model, in this case, the eleven principles, as discussed in section 5.2.

The R^2 values are low, which is likely a reflection of the fact that the target achievement of a project is dependent on so many variables, and in this analysis we have only captured eleven. We do see, however, that the Whole Model Test p-values of the high-level project target outcomes (the first four in Table A) are larger than the intermediary

outcomes (the final three in Table A), meaning that the principles have less explanatory power on the high-level project outcomes.

REFERENCES

Anttila, J., 1992. Standardization of quality management and quality assurance: a project viewpoint. *International Journal of Project Management*, 10, pp.208–212.

Aven, T., 2011. On the new ISO guide on risk management terminology. *Reliability Engineering and System Safety*, 96(7), pp.719–726.

de Bakker, K., Boonstra, A. & Wortmann, H., 2010. Does risk management contribute to IT project success? A meta-analysis of empirical evidence. *International Journal of Project Management*, 28(5), pp.493–503.

Bresnen, M., 2016. Institutional development, divergence and change in the discipline of project management. *International Journal of Project Management*, 34, pp.328–338.

Brunsson, N., Rasche, a. & Seidl, D., 2012. The Dynamics of Standardization: Three Perspectives on Standards in Organization Studies. *Organization Studies*, 33, pp.613–632.

DoD, 2006. *Risk Management Guide for DoD Acquisition* 6th ed., Washington, D.C.: United States Department of Defense, Office of the Secretary of Defense.

Duncan, W.R., 1995. Developing a project-management body-of-knowledge document: the US Project Management Institute's approach, 1983-94. *International Journal of Project Management*, 13(2), pp.89–94.

Fortune, J. & White, D., 2006. Framing of project critical success factors by a systems model. *International Journal of Project Management*, 24(1), pp.53–65.

Grant, K.P. & Pennypacker, J.S., 2006. Project management maturity: An assessment of project management capabilities among and between selected industries. *IEEE Transactions on Engineering Management*, 53(1), pp.59–68.

Heras-Saizarbitoria, I. & Boiral, O., 2013. ISO 9001 and ISO 14001: Towards a Research Agenda on Management System Standards*. *International Journal of Management Reviews*, 15(1), pp.47–65.

Ibbs, C.W. & Kwak, Y.H., 2000. Assessing Project Management Maturity. *Project Management Journal*, 31(1), pp.32–43.

INCOSE, 2011. *Systems engineering handbook* 3.2.2 ed. C. Haskins, ed., San Diego: INCOSE.

International Organization for Standardization, 2009. *ISO 31000:2009(E)*, Geneva.

Jun, L., Qiuzhen, W. & Qingguo, M., 2011. The effects of project uncertainty and risk management on IS development project performance: A vendor perspective. *International Journal of Project Management*, 29(7), pp.923–933.

Kutsch, E. & Hall, M., 2009. The Rational Choice of Not Applying Project Risk Management in Information Technology Projects. *Project Management Journal*, 40(3), pp.72–81.

Lalonde, C. & Boiral, O., 2012. Managing risks through ISO 31000: A critical analysis. *Risk Management*, 14(4), pp.272–300.

Leitch, M., 2010. ISO 31000:2009--The new international standard on risk management. *Risk analysis*, 30(6), pp.887–92.

Liu, J., Meng, F. & Fellows, R., 2014. An exploratory study of understanding project risk management from the perspective of national culture. *International Journal of Project Management*, 33(3), pp.564–575.

Milosevic, D. & Patanakul, P., 2005. Standardized project management may increase development projects success. *International Journal of Project Management*, 23(3), pp.181–192.

Mishra, A., Das, S.R. & Murray, J.J., 2016. Risk, process maturity, and project performance: An empirical analysis of US federal government technology projects. *Production and Operations Management*, 25(2), pp.210–232.

Miterev, M., Engwall, M. & Jerbrant, A., 2016. Exploring program management competences for various program types. *International Journal of Project Management*, 34(3), pp.545–557.

Morris, P.W.G. et al., 2006. Exploring the role of formal bodies of knowledge in defining a profession – The case of project management. *International Journal of Project Management*, 24(8), pp.710–721.

Mu, J., Peng, G. & Maclachlan, D.L., 2009. Effect of risk management strategy on NPD performance. *Technovation*, 29, pp.170–180.

Muzio, D. et al., 2011. Towards corporate professionalization: The case of project management, management consultancy and executive search. *Current Sociology*, 59(4), pp.443–464.

NASA, 2008. Agency Risk Management Procedural Requirements. *Risk Management*.

Oehmen, J. et al., 2014. Analysis of the effect of risk management practices on the performance of new product development programs. *Technovation*, 34(8), pp.441–453.

Papke-Shields, K.E., Beise, C. & Quan, J., 2010. Do project managers practice what they preach, and does it matter to project success? *International Journal of Project Management*, 28(7), pp.650–662.

Perminova, O., Gustafsson, M. & Wikstrom, K., 2008. Defining uncertainty in projects - a new perspective. *International Journal of Project Management*, 26(1), pp.73–79.

Project Management Institute, 2008. Project Risk Management. In *A Guide to the Project Management Body of Knowledge (PMBOK GUIDE)*. Newtown Square, PA: Project Management Institute.

Purdy, G., 2010. ISO 31000:2009--Setting a new standard for risk management. *Risk analysis*, 30(6), pp.881–6.

Raz, T. & Michael, E., 2001. Use and benefits of tools for project risk management. *International Journal of Project Management*, 19(1), pp.9–17.

Raz, T., Shenhar, A.J. & Dvir, D., 2002. Risk management, project success, and technological uncertainty. *R&D Management*, 32(2), pp.101–109.

SAS Institute Inc., 2014. The VARCLUS Procedure. In *SAS/STAT 13.2 User's Guide*. Cary, NC: SAS Institute Inc.

Sheskin, D.J., 2011. *Handbook of Parametric and Nonparametric Statistical Procedures* 5th ed., Boca Raton, FL: Chapman & Hall/CRC.

Standards Australia, S.N.Z., 2004. AS/NZS 4360:2004.

Su, H.-C., Dhanorkar, S. & Linderman, K., 2015. A competitive advantage from the implementation timing of ISO management standards. *Journal of Operations Management*, 37, pp.31–44.

Teller, J., Kock, A. & Gemünden, H.G., 2014. Risk Management in Project Portfolios Is More Than Managing Project Risks: A Contingency Perspective on Risk Management. *Project Management Journal*, 45(4), pp.67–80.

Thamhain, H., 2013. Managing Risks in Complex Projects. *Project Management Journal*, 44(2), pp.20–35.

Wallace, L. & Keil, M., 2004. Software Project Risks and Their Effect on Outcomes. *Communications of the ACM*, 47(4), pp.68–73.

Williams, T., 2005. Assessing and moving on from the dominant project management discourse in the light of project overruns. *IEEE Transactions on Engineering Management*, 52(4), pp.497–508.

Wirth, I. & Tryloff, D.E., 1995. Preliminary comparison of six efforts to document the project-management body of knowledge. *International Journal of Project Management*, 13(2), pp.109–118.

Zwikael, O. & Ahn, M., 2011. The effectiveness of risk management: an analysis of project risk planning across industries and countries. *Risk Analysis*, 31(1), pp.25–37.