Development and application of a new maturity model for project risk management in the automotive industry

by Jose Irizar and Martin Wynn
Email addresses: Jose.Irizar@ gmail.com; MWynn@glos.ac.uk

Abstract

The management of risk is an integral part of the project management process and project failure is an area of concern in many organisations. This chapter explains and discusses a new maturity model for the assessment and management of project risk in the automotive industry. The research design was two-fold. First, a case study analysis in a major German automotive company was undertaken to develop the maturity model, the approach being qualitative and inductive, using data provided by in-depth interviews. Second, this model was then applied in two major projects currently underway in the company – one involving the implementation of a cloud-based ERP system, and the other the program management function responsible for product development and launch. The model adds to existing risk management maturity models and is unique in being specific to the automotive industry. It can be used by risk and project managers, and can be adapted to other industry sectors.

Keywords – Risk Management, Project Risk Management, Risk Identification, Risk Assessment, Risk Allocation, Maturity Model, Automotive Industry

1. INTRODUCTION

The significance of managing risk has come to the fore in recent years in the context of cybersecurity and the rapid growth of the associated risks to organisations and society at large (Olakunle & Win, 2022). However, project risk management has been a fundamental discipline in most industry sectors for several decades, and can be defined as the process that dynamically minimizes risk levels by identifying and ranking potential risk events, developing a response plan, and actively monitoring risk during project execution (Zwikael & Ahn, 2011). Although risk management has become a significant element of some of the most widely deployed industry standard methodologies, there is no universally agreed method for managing risk. Yet, as a recent industry report notes, "risk management has never been more important. Projects are under more pressure to deliver, and the costs of failure are higher than they have ever been"

(Project Management.com, 2019, p.8). Application of integrated risk management methods can support early risk identification and assessment, thereby improving project outcomes and avoiding delays and cost overruns (Zayed, Amer, & Pan, 2008).

This research focuses on the development and application of a new maturity model for the assessment, monitoring and management of project risk capability in the automotive industry, specifically in a European context. Following this brief introduction, the next section explores relevant literature in this field, followed by a detailed explanation of the research methodology employed. Section 4 then presents the maturity model as built and verified, but also applies the model to two in-company projects. This provides an illustration of how the model can be used, in a manner that can be built upon by other researchers and practitioners. The final section draws together key themes covered in the chapter and assesses the contribution to research and practice.

2. LITERATURE REVIEW

Risk Dimensions

Holzmann (2012) views risk management as comprising five main activities, encompassing risk identification, risk assessment, risk allocation, and risk control. Other authors (Bannerman, 2008; Harwood, Ward, & Chapman., 2009) see risk appetite or treatment as an important dimension for overall risk management. This research combines elements drawn from these sources to focus on four main dimensions of risk management: risk identification, risk assessment, risk allocation and risk appetite; and it does not see risk in a purely negative context, but also recognises the potential of positive risks or opportunities.

Risk identification is considered to have the highest impact on the effectiveness of project risk management and involves the detection and classification of all known and - as far as is possible - unknown, risks, thus producing the foundation upon which the overall risk management process can be established (Chapman, 2001). Risk identification is also perceived as the most influential risk management activity (de Bakker, Boonstra, & Wortmann, 2011; de Bakker et al., 2012), and particularly in complex projects is seen as an area in need of improvement (Harvett, 2013). Risk identification can be performed in a number of ways, such as filling in questionnaires, consulting experts or available documentation from previous projects, doing brainstorming sessions, or conducting interviews.

Risk assessment is the stage in the risk management process at which each identified risk is assessed for its probability or likelihood of occurrence, and its impact - in terms of time, cost and quality - on either the project phase or the entire project, should it occur (Patterson, 2002). Risk assessment entails the study of the probability of occurrence and any associated consequences. Generally speaking, two broad categories of risk assessments have been used - qualitative risk assessment and quantitative risk assessments (Dawotola, Gelder, & Vrijling, 2012). Qualitative risk assessment makes use of descriptive scales for the assessment of probabilities, such as risk scores. These scores or rankings are subject to interpretation and therefore entail an inherent level of subjectivity (Dawotola et al., 2012). The application of qualitative risk assessment suffers some serious limitations, mainly the subjectivity of the values estimated. Qualitative risk analyses are flawed in the sense that they can produce wildly different results (Emblemsvåg & Kjølstad, 2006).

Risk matrices are one of the most popular risk assessment methodologies employed across many industries, providing the graphical output that enables the communication of risk assessment. The development of risk matrices (RMs) has taken place in isolation from academic research in decision making and risk management – risk matrices produce arbitrary decisions and risk-management actions. These problems cannot be overcome because they are inherent in the structure of RMs (Thomas, 2013). Their theoretical basis is superficial and the validity of the qualitative information they employ is highly suspect. Assessments of the likelihood of occurrence and their impacts suffer all the shortcomings associated with subjective assessment (Wall, 2011).

Risk allocation is a major task in the overall risk project management process (Harvett, 2013), and is based on the recognition that different parties have different objectives and perceptions of project risk, as well as varying capabilities for managing associated sources of uncertainty. Chapman and Ward (2007) consider risk allocation (or risk ownership as it is sometimes termed) a relevant phase within their formal process framework SHAMPU (Shape, Harness, And Manage Project Uncertainty). It involves allocating responsibility for managing project uncertainty to appropriate project parties. These allocations are fundamental because they can strongly influence the motivation of parties and the extent to which project uncertainty is assessed and managed by each party.

Risk allocation is related to the more general concept of business ownership which has seen a range of business functions take responsibility for various aspects of project delivery. In the

past IT or engineering functions often owned exclusively the risk in their related projects. Now, it is often the case that the function in charge of the project helps business partners to take ownership of specific risks and assists them in making assessments and in following compliance mechanisms by themselves (Chobanova, 2014).

Project *risk appetite* (sometimes called *risk treatment* or *risk propensity)* reflects an organisation's attitude and strategy towards risk. It encompasses how risk is managed and whether exposure to risk should be reduced, or the impact of risk should be mitigated, transferred, externalized or accepted. These responses can be supported by a framework providing risk factor dependencies and priorities (Aloini et al., 2012). Harwood et al. (2009) see risk propensity as the organizational behavioural tendency towards taking reasonable risks, by recognising, assessing and managing risks. A risk-averse organisation is seen to have low risk appetite, and will take only those risks that are judged to be tolerable and justifiable.

A balanced treatment of risk would focus both on risk and reward. An overemphasized focus on risk versus reward may have considerable influence on strategic decisions such as entering new markets, developing new products or targeting new mergers and acquisitions (TowerGroup, 2014). Resultant executive inaction may lead to loss of potential revenue growth. Education and training in project risk management with subsequent additional experience in the organization can produce a better understanding of risk and reward. Risk management can then be understood as a protection shield, not an action stopper. Manager and employees learn through education and training to take and manage risks, not to avoid them. The organization will treat risk appropriately and not try to circumvent it.

Existing Maturity Models

The maturity concept has featured in a range of models used for assessing organizational capabilities encompassing the collective skills, abilities and expertise of an organization. Maturity can be understood as a measure of organizational performance, and such models have been developed to assess a range of organisational capabilities, including e-Government (Wynn et al., 2021), e-business (Wynn et al., 2013) and blockchain deployment (Bazaeea et al., 2020; Wang et al., 2016), and Artificial Intelligence utilisation (Vaish et al., 2021). There are two approaches to organizational maturity that can be applied in the development of such models. The Organisational Project Management Maturity Model (OPM3) measures organisational maturity based on the level of best practices deployment, while the Capacity Maturity Model Integration (CMMI) assesses maturity based on organisational process

effectiveness (Man, 2007). Further, organisational capabilities may refer to both processes and projects (Maier et al., 2012). Assessing an organization's project risk management maturity level can help develop its project capability and performance. Risk management maturity reflects the organization's s211understanding of its risk portfolio and its attitude towards those risks. Organizations intending to implement or improve their project risk management need a framework against which they can benchmark their current practice (Zou et al., 2010), and maturity models can be used to identify the priority areas in need of improvement, and remedial actions can then be taken to increase performance (Hopkinson, 2012; Ciorciari & Blattner, 2008).

Hillson (1997) was an early proponent of risk maturity models. His approach consisted of four attributes (culture, process, experience and application) and four levels of maturity. His model (Table 1) is not industry specific and does not focus on risk in projects, but is a general organisational approach to risk. Yeo and Ren (2009) developed and tested a five-level maturity model (initial, repeatable, defined, managed, and optimizing) with three key capability areas: organization culture; risk management process; and risk management knowledge and technology, based on research of Asian offshore and marine projects. Similarly, Zou et al's. (2010) risk management maturity model was industry specific, in this case the construction industry in Asia and Australia. It had four maturity levels (initial, repeated, managed and optimized), and encompasses risk identification, risk assessment and risk appetite - but not risk allocation - in projects.

	LEVEL 1 - NAIVE	LEVEL 2 - NOVICE	LEVEL 3 - NORMALISED	LEVEL 4 - NATURAL
DEFINITION	Unaware of the need for management of risk. No structured approach to dealing with uncertainty. Repetitive & reactive management processes. Little or no attempt to learn from past or to prepare for future.	Experimenting with risk management, through a small number of individuals. No generic structured approach in place. Aware of potential benefits of managing risk, but ineffective implementation, not gaining full benefits.	Management of risk built into routine business processes. Risk management implemented on most or all projects. Formalised generic risk processes. Benefits understood at all levels of the organisation, although not always consistently achieved.	Risk-aware culture, with proactive approach to risk management in all aspects of the business. Active use of risk information to improve business processes and gain competitive advantage. Emphasis on opportunity management ("positive risk").
CULTURE	No risk awareness. Resistant/reluctant t to change. Tendency to continue with existing processes.	Risk process may be viewed as an additional overhead with variable benefits. Risk management only used on selected projects	Accepted policy for risk management. Benefits recognised & expected. Prepared to commit resources in order to reap gains.	Top-down commitment to risk management, with leadership by example. Proactive risk management encouraged & rewarded.
PROCESS	No formal processes.	No generic format processes, although some specific formal methods may be in use. Process effectiveness depends heavily on the skills of the in-house risk team and availability of external support.	Generic processes applied to most projects. Formal processes, incorporated into quality system. Active allocation & management of risk budgets at all levels, Limited need for external support.	Risk-based business processes. "Total Risk Management" permeating entire business. Regular refreshing & updating of processes. Routine risk metrics with constant feedback for improvement

EXPERIENCE	No understanding of risk principles or language.	Limited to individuals who may have had little or no formal training.	In-house core of expertise, formally trained in basic skills. Development of specific processes and tools.	All staff risk-aware & using basic skills. Learning from experience as part of the process. Regular external training to enhance skills.
APPLICATION	No structured application. No dedicated resources. No risk tools.	Inconsistent application. Variable availability of staff. Ad hoc collection of tools and methods.	Routine & consistent application to all projects. Committed resources. Integrated act of tools and methods.	Second-nature, applied to all activities. Risk-based reporting & decision-making. State-of-the-art tools and methods.

Table 1. Attributes of Hillson's Risk Maturity Model (Hillson, 1997)

An extension of Hilson's maturity model is Hopkinson's (2012) Project Risk Maturity Model, which establishes a framework for assessing risk management capability against recognised standards. Hopkinson's model offers a working model to assess risk management capacity and applies it to an equipment procurement case study. Crawford (2006) identified some key issues for developing and applying project management related maturity models. One is the intrinsic subjectivity associated with the determination of an organisation's maturity. Crawford also concluded that, rather than necessarily striving to achieve the next level of maturity, organizations should instead determine their minimum level of maturity at which optimum value can be achieved (Crawford, 2006). Maier et al. (2012) established a roadmap to develop maturity grids for assessing organizational capabilities. They review existing maturity models and conclude that they offer a contemporary representation of different conceptualizations of organizational practices and capabilities that are viewed as important for success.

Provisional Conceptual Framework

Whilst some of these maturity models are of value in certain industry contexts, there is no maturity model specifically geared to project risk management in the automobile industry. This research addresses this gap by building and verifying a maturity model for the automotive industry in Europe. The initial conceptual framework for this model builds upon the four dimensions of risk discussed above – identification, assessment, allocation and appetite. These can be defined as:

Risk identification: The process by which the project team detects prospective events which might affect the project and documents their characteristics (Holzmann, 2012).

Risk assessment: The stage in risk management at which the identified risk is assessed for its probability (likelihood) of occurrence and its impact, in terms of time, cost and quality (Patterson & Neailey, 2002).

Risk allocation: The assignment of the responsibility for managing specific project risks or uncertainty to appropriate project individuals or parties (Harvett, 2013).

Risk appetite: The organizational (or individual) behavioural tendency regarding how to take reasonable risks (Aloini et al., 2012).

The research attempts to identify typical risk characteristics that can be associated with each of these four dimensions of risk at different stages of maturity in the risk management process. Like some of the models discussed above, the proposed model was assigned four stages with provisional stage labels of Rudimentary, Intermediate, Standardised and Corporate. Maturity models typically have either four or five stages, but in the five stage models, the difference between stages one and two is generally minimal, with stage one often describing a non-existent or minimal initial capability. Four stage models have the additional benefit of avoiding an assessor's tendency to select middle values (Zou et al., 2010). These stages can be defined as follows:

Rudimentary: the organisation has no sense of need for risk management; teams do not follow any common approach in managing risks. Project risk activities are reactive and no lessons learned or improvement process is established. Typically, no project risk plan exists.

Intermediate: some project management practitioners undertake certain project risk management activities. Neither these activities, nor the systems and applications used to support risk management, are standardised. The organisation does not gain the full benefit of implementing these risk management activities.

Standardised: risk management is seen as part of core business processes, and risk responses and their effectiveness are reviewed in most projects. Systems and applications supporting risk management are accessible and lessons learned are established to improve the overall risk management process.

Corporate: the entire organisation recognises and values risk management, which is integrated into other processes. Executives actively audit and support risk owners. Multi-user risk databases are widely available and used as part of continuous improvement programs.

3. RESEARCH METHODOLOGY

The research method was qualitative and inductive, based on in-depth interviews in a single company case study. The case study entails a "detailed investigation of one or more organisations, or groups within organisations, with a view to providing an analysis of the context and processes involved in the phenomenon under study" (Hartley, 2004, p. 323). This is exploratory research that adopts a qualitative approach. Project management success is complex, messy, and involves a range of stakeholders with different concerns and perceptions (Skinner, Tagg, & Holloway, 2000). A qualitative approach is particularly appropriate for research that seeks to explore real organizational goals, linkages and processes in organizations; to understand the failure of policies and practices (Marshall & Rossman, 2014).

The research builds explanations of risk management in practice from the ground up, based on interview evidence, observations, and analysis of available documentation. The interview is an important source for collecting data, and may take several forms (Yin, 2012). To achieve quality in data collection, interviews must be carefully planned. Data collection was undertaken through 12 semi-structured interviews, three follow-up in-depth interviews, an on-line survey, informal discussions, secondary material, and participant observation.

This research took place within the automotive industry, one of the leading manufacturing industries worldwide, where scientific method has an undeniable influence in manufacturing industry development. Operational research and systems engineering are two of the main academic disciplines that provide the basis for process improvements in this industry. The underlying theoretical perspective of these disciplines is positivism (Taylor, 1911), and the concept of separating planning from doing is reflected in the emphasis on planning and control in modern project management. Furthermore, rationality, universality, objectivity, value-free decision making, and the possibility of generating law-like predictions in knowledge are basic assumptions of modern project management (Gauthier & Ika, 2012). The traditional project management paradigm has been described as "rational, normative, positivist and reductionist" (Harvett, 2013, p.51).

The study aligns with recent academic research from authors such as Harvett (2013), Niebecker (2009) and Olsson (2006) all of which explicitly characterize their work on project risk management in practice as post-positivist. This study adopts a qualitative research approach that identifies descriptive labels specific to different risk management contexts. Some may suggest this is an interpretivist approach, but interpretivism, as an alternative to the positivist orthodoxy, assumes there is no absolute truth, but multiple realities and is based on subjectivity

(Biedenbach & Müller, 2011). However, this research assumes there is an answer to the questions posed, even if the researchers must seek for the consensus views of the practitioners to validate what is known. For the interpretivist, all meaning is believed to be subjective, based on subjective perceptions and experiences with external environmental factors. This research adopts a post-positivist stance which looks for an objective, singular truth, thus differentiating it from the interpretivist paradigm (Phoenix et al., 2013).

The selected case study company was viewed as a reasonable example of a global automotive supplier organisation, because of its regional presence, customer mix, and product catalogue. The company has over 135,000 employees, around 200 production facilities in some 40 countries, sales of €35.2 billion in 2016, and a yearly investment on R&D of about €2 billion. It is highly dependent on the success of its new projects and the smooth launch of serial production for global customers. Project risk management is a fundamental aspect of its project management process, and is applied globally. Project risks are documented, evaluated and risk controls are applied, and the risk management process is reviewed regularly to adapt it to the market challenges. The unit of analysis is thus the entire organisation. Following Yin's (2012) distinctions of designs for case studies, the one chosen in this research is holistic as opposed to embedded, in which more than one unit of the organisation are the units of analysis (Saunders et al., 2009). In the application and testing of the model in 2022, two "live" business environments were used. The implementation of the cloud-based SAP Enterprise Resource Planning (ERP) product provided an ideal context for the application of the developed maturity model. The second project in which the maturity model was applied centred on the program management function responsible for product development (and launch). This represented a somewhat different application of the model – assessing a process or function rather than a defined project.

The initial research phase was conducted over an eighteen-month period and fourteen potential interviewees were initially invited, of which 12 accepted the invitation. These business leads were chosen because collectively they represented project managers of major projects with high impact to the organization. An initial semi-structured interview took place with these 12 personnel (Table 2), in which their previous experience with regards to project risk management and their understanding of the risk management dimensions were explored. The Participant Consent form and the project information sheet were sent in advance to the participants, together with an interview agenda and questionnaire.

1. ***Program Manager:*** *8 years' experience as Project Manager – published chapters on project risk management, PMP*
2. ***European ERP Manager:*** *12 years' experience in IT and project management as project manager and Steering Committee member, PhD in IT, PMP*
3. ***VP Program Management Global:*** *25 years' experience in Project Management, responsible for the Project and Project Risk Management methodology, training, templates and business process methods defined/deployed through the global organization, PMP*
4. ***Global ERP Manager:*** *20 years' experience, responsible for ERP competency center, responsible of several ERP rollouts worldwide, PMP*
5. ***Director, Global Program Management of business unit:*** *20 years' experience, responsible of the global business unit programs, manager of 15 program managers, experience with Project Risk management quantitative methods such as Monte Carlo, PMP*
6. ***Chief Engineer, PMO lead:*** *15 years' experience, responsible of the PMO, engineering programs methodologies and systems, PMP*
7. ***PMO / Program Systems Coordinator:*** *10 years' experience, responsible for standard program management training and Program management systems development, PMP*
8. ***Senior Program Manager:*** *15 years' experience – responsible for major programs, PMP*
9. ***Senior Program Manager:*** *15 years' experience – responsible for major programs, PMP*
10. ***Director, Global Program Management business unit:*** *10 years' experience, responsible of the global Engineered Fasteners & Components programs, manager of 10 program managers, PMP*
11. ***Applications Engineer and Project Manager:*** *5 years' experience, Project Risk management expert, co-author of the internal project risk management procedures.*
12. ***Senior Vice President, business unit:*** *15 years' experience - ultimate responsibility for 12 sites in 9 countries, acting as Sponsor and/or senior Steering Committee member on major customer programs.*

Table 2. Roles and experience of the 12 interviewees

The questions were grouped according to the four sequential project risk management dimensions. To support and balance these main questions, follow-up questions were developed to ensure breadth of discussion of each of the risk dimensions. The interview was introduced by a brief presentation using PowerPoint slides, to set the scene. Just four slides were discussed initially, and the remaining three slides were discussed in combination with questions. The interviews finished with a debriefing, requesting whether anything else could be relevant to the questions discussed, any other aspect that should be mentioned, or any question needing further elaboration. All 12 stakeholder interviews were transcribed verbatim, resulting in 135 pages of transcripts. These were then analysed and the initial version of the maturity model was constructed.

Having built the initial model from data collected through the 12 semi-structured interviews, this was then tested for validity and relevance (Maier et al., 2012). First, an online survey was undertaken involving six practitioners who were contacted by phone where the maturity model and the aim of the online survey was discussed. The responders were then requested to assign each of the 151 statements emanating from the interviews to one of the four maturity stages via an online form distributed via Google forms; a simple tool used to create and distribute questionnaires. The respondents answered the survey on their own with no influence from the

researcher, and the responses were collected and stored in a repository. Secondly, three semi structured interviews were conducted.

Although the above procedures constituted a form of model validation, the model was subsequently used to assess risk maturity in the two live environments, as noted above, in 2022. The first of the interviewees was the program manager responsible for defining the standard process template configuration of the SAP implementation, and for the subsequent rollout of the system through several production facilities in different continents. The template is designed to meet funcional, legal and customer requirements, which will eventually be standardised with few exceptions, based on a defined governance model. The second interviewee was the head of the program management function. For both interviewees, the maturity model was explained in outline, and interviewees were provided with a brief description of the labels and the maturity stages applied to the four dimensions were briefly discussed, with one or two more detailed explanations. Intervieweees were then asked to relect upon the model and identify, in a series of logical steps, the labels that best represented their project or process environment. The interviewer provided guidance and support to help the interviewees in this procedure (Figure 1).

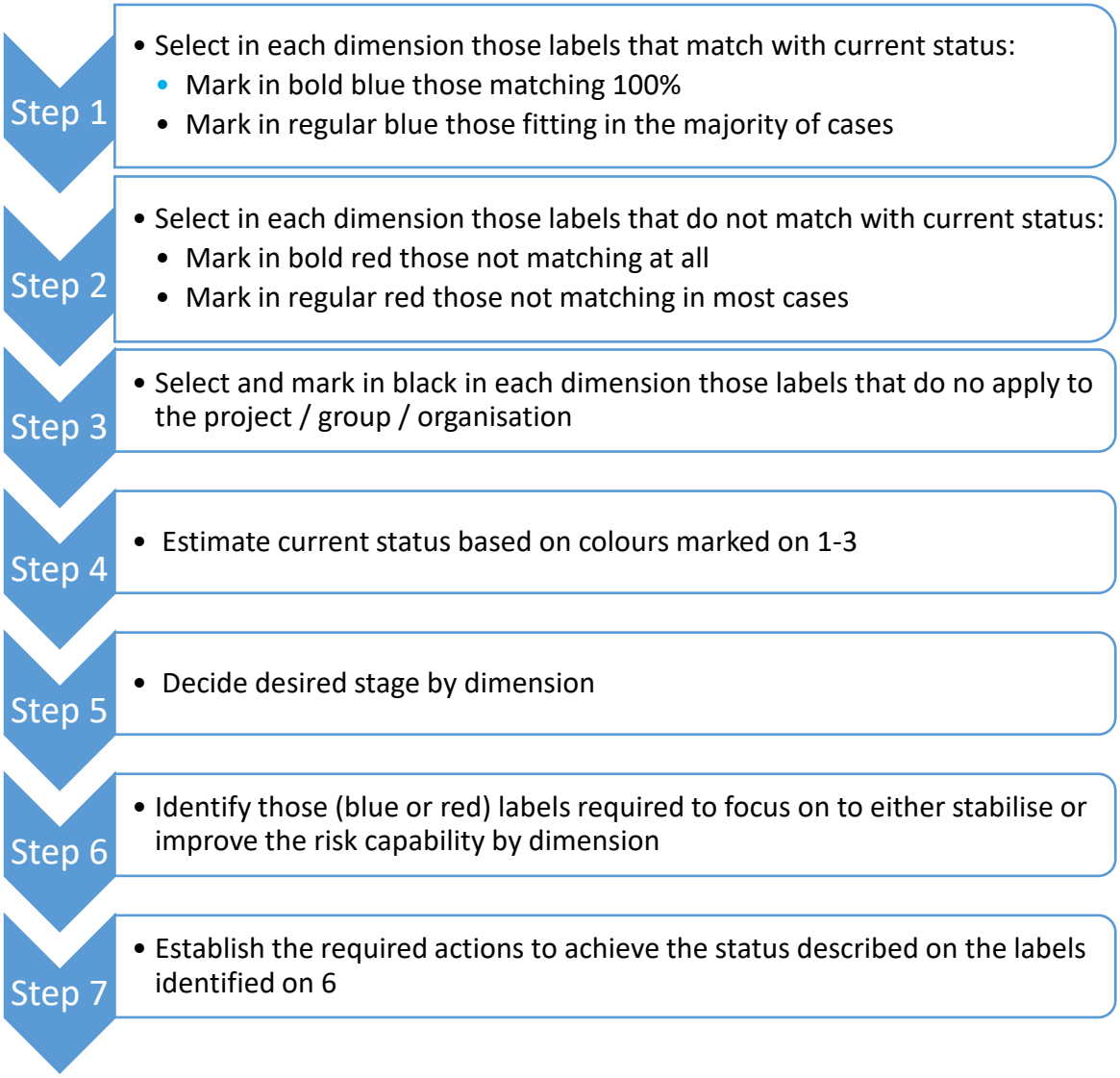


Figure 1. Guide for maturity model application

4. MATURITY MODEL PRESENTATION AND APPLICATION

The model, with its four stages of maturity, can be used to assess and understand the organisation's current project risk management capability and subsequently develop strategies to improve their risk management practice. The maturity model assesses four fundamental dimensions of project risk management, namely risk identification, assessment, allocation and appetite. There are 156 labels allocated to one of the four risk dimensions and one of the four stages in the model. The labels are grouped within the stages and dimensions into two types: 'people and organisation' and 'process and systems'. Following the verification process, the positioning of 51 of the labels was changed, 49 being changed by one stage in the model and two of the labels were relocated by two stages. The model is depicted in Figures 2-5 below,

and summary descriptions of each stage of each of the four dimensions are included in appendices 1-4.

Risk Identification

IDENTIFICATION	RUDIMENTARY	Negative perception of risk	End users no involvement with risk identification process	Fear of raising risk concerns	Compliancy risks not identified even though may exist	Risk identification is ad-hoc, basic, hit and miss
	INTERMEDIATE	People make full use of their freedom to act	Lack of integration of all stakeholder views	Disagreement among stakeholders if an event is a risk, subjectivity	Some compliancy aspects addressed but may have omitted significant ones	Potentially significant risk items may be omitted in reporting
		Lack of knowledge regarding what risk or uncertainty mean	Risk identification process characterised by subjectivity	No visibility of risk identification tasks / activities in project plan	Isolated non coordinated risk identification	Risk description is ambiguous, misleading
			New risks identified as they occur	Some remaining subjectivity (cultural differences)	Only focused on individual risks, managed at lower levels within team	Lessons learned not standardised. Unstructured documentation
	STANDARDISED	End users have an active role in the identification process	Timely integration of previous phases	Clear risk classification (standard risks)	Set minimum frequency risk identification rules with senior members	Shared understanding of group approach to risk identification
		Recognises risk management but not ready to invest resources	Instructions with project categorization / risk sources identification	Routine planning reviews to aid risk identification	Bridge from the lessons learned into the risk identification process	Mechanism identifies gaps between planned tasks and resources available
		Use quantitative risk methods (Montecarlo) to avoid subjectivity	Established procedure for contradictory views (objectivise)	A risk identification process guide may be Visibility on new sourcing, 'make-or-buy' decisions	Visibility of implications of risks associated with all relevant suppliers	Structured accessible lessons learned & risk registers database (DB)
	CORPORATE	Earned Value (EV) monitoring highlights project performance shortfalls	Integrated process with involvement of all stakeholders	Formal communication regarding risk interrelations between projects	Top down approach related to project purpose and strategy	Real time reporting based on realistic data from all stakeholders

Figure 2. Maturity model: risk identification

Risk Assessment

ASSESSMENT	RUDIMENTARY	No relationship between risk information and cost forecast	Responses based on weak understanding or delayed thus ineffective	Isolated non coordinated risk assessment No evidence of opportunities being pursued	No fall back plans for risk mitigation or management	Only considered if project in difficulty or imposed by management
	INTERMEDIATE	Higher focus on project issues than on risks is embedded in the culture Management does not prioritise project issues over project risks	Description includes an indication about the source of risk Quantitative schedule analysis is not used	Lacks standard impact & probability estimate methodologies. This increases 'subjectivity' Struggle with Probability Impact (P*I) threshold concept	Probability estimation accuracy is weak Formal risk register maintenance Prescribed risk categorisatio	Risk description is impact oriented, lacks context and of uncertain origin Use existing expertise and qualitative assessments
	STANDARDISED	FMEA, 6s, poka yoke used for quality management (in product design)	Clear procedure, minimum frequency to assess risk event - Evidence based	Realistic estimates, use existing expertise and qualitative assessments	Sound understanding of risk combined with use of Monte Carlo, decision tree	Description is useful for qualitative risk analysis
		Planned costs consider risk management - Threshold based on $ or days	Visibility of high-impact risks, risks which became issues, risks clustering ability	Valid methods for risk prioritisation and risk quantification	Team members have good understanding of project's context and overall goal	Impact estimation includes secondary effects Certain use of Quantitative Methods
		Considers secondary effects which extend beyond immediate impact	Measure project team members' performance regarding risk issues (commitment)	Steering Committee may challenge the risk process – escalate when required	Systems analyse and summarise risk categories by project, customer or industry	Project categorization is standard Attempts to prevent event from happening in first
	CORPORATE	Systemic risk assessment and continuous improvement	Ability to measure team members' performance	$ estimation of mitigated risk (Benefit of risk responses)	Risk management system integrated with other corporate systems	

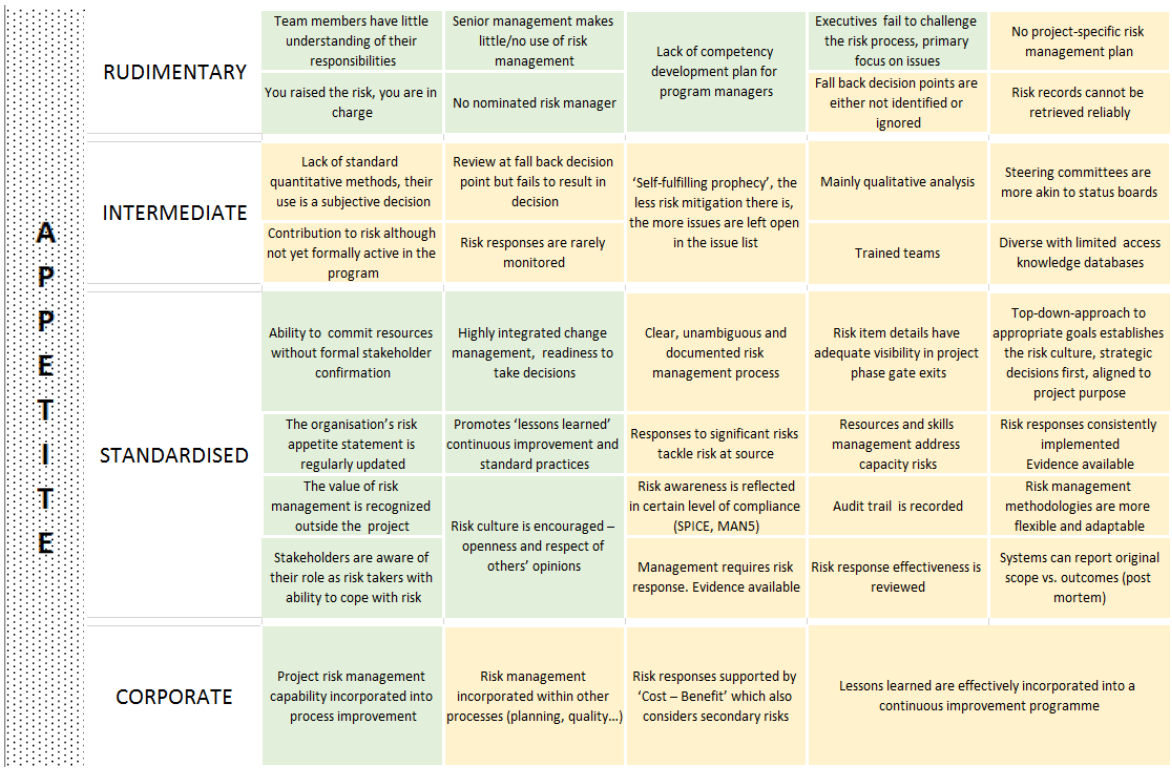
Figure 3. Maturity model: risk assessment

Risk Allocation

ALLOCATION	RUDIMENTARY	Some stakeholders reluctant to divulge new information on risk	Unwillingness to assign risk ownership - perceived as telling to the other person 'you are doing it wrong'	Reluctance to own risk	Isolated non coordinated risk allocation	Some departments do not feel responsible 'project manager will be hold responsible'
		No active recognition or support for good risk management practice		Risk perceived as intrusive, lot of work and not keen to talk about its ownership	Lack of risk disclosure with contracting parties	
	INTERMEDIATE	Dependent on project managers' personality some of which are no open to others' input	Some program managers doing everything, but recognised as inefficient	Steering Committee meetings are pure status meetings	Only program management (and engineering) drive the risk allocation	In most cases assigned to project manager
			Only dotted line reporting to project manager 'my boss has not told me ...'	Suppliers provide risk information however not complete	Identify groups with potential but currently not involved	Constant communication with customer / vendors
	STANDARDISED	There is expertise to assign risks across several groups	Team members' actions are aligned with achieving overall project objectives	Expertise within teams is recognised and harnessed	Formal agreements with risk sharing arrangements	Clear business guidelines regarding who is the risk-taker
		All people working in the project actually use the risk management plan	Autonomous functional risk allocation	All risks have a risk owner with authority and who accepts responsibility	Clear procedure with minimum frequency rules to update risk ownership	Suppliers undertake complementary risk management
			System accessible, customised and team trained			
		Steering Committee audits, processes and supports the risk owners	Contracts with formal risk agreement bearing clear financial liabilities	Every team member provides input on items with commercial impact	Prescriptive risk classification and job descriptions enable allocation automation	All stakeholders are open in their disclosure of all risk information
	CORPORATE	Good risk management practice, management audits the process and supports the risk owners		Escalation powers and procedures are in place	Consistently maintained multi-user concurrent access risk database is in place	

Figure 4. Maturity model: risk allocation

Risk Appetite



APPETITE	RUDIMENTARY	Team members have little understanding of their responsibilities	Senior management makes little/no use of risk management	Lack of competency development plan for program managers	Executives fail to challenge the risk process, primary focus on issues	No project-specific risk management plan
		You raised the risk, you are in charge	No nominated risk manager		Fall back decision points are either not identified or ignored	Risk records cannot be retrieved reliably
	INTERMEDIATE	Lack of standard quantitative methods, their use is a subjective decision	Review at fall back decision point but fails to result in decision	'Self-fulfilling prophecy', the less risk mitigation there is, the more issues are left open in the issue list	Mainly qualitative analysis	Steering committees are more akin to status boards
		Contribution to risk although not yet formally active in the program	Risk responses are rarely monitored		Trained teams	Diverse with limited access knowledge databases
	STANDARDISED	Ability to commit resources without formal stakeholder confirmation	Highly integrated change management, readiness to take decisions	Clear, unambiguous and documented risk management process	Risk item details have adequate visibility in project phase gate exits	Top-down-approach to appropriate goals establishes the risk culture, strategic decisions first, aligned to project purpose
		The organisation's risk appetite statement is regularly updated	Promotes 'lessons learned' continuous improvement and standard practices	Responses to significant risks tackle risk at source	Resources and skills management address capacity risks	Risk responses consistently implemented Evidence available
		The value of risk management is recognized outside the project	Risk culture is encouraged – openness and respect of others' opinions	Risk awareness is reflected in certain level of compliance (SPICE, MAN5)	Audit trail is recorded	Risk management methodologies are more flexible and adaptable
		Stakeholders are aware of their role as risk takers with ability to cope with risk		Management requires risk response. Evidence available	Risk response effectiveness is reviewed	Systems can report original scope vs. outcomes (post mortem)
	CORPORATE	Project risk management capability incorporated into process improvement	Risk management incorporated within other processes (planning, quality...)	Risk responses supported by 'Cost – Benefit' which also considers secondary risks	Lessons learned are effectively incorporated into a continuous improvement programme	

Figure 5. Maturity model: risk appetite

The application of the model in the two business environments noted in section 3 above is now discussed. In the *web-based SAP ERP project*, the maturity level for the Identification, Assessment and Allocation risk dimensions was assessed as Rudimentary, whilst Risk Appetite was seen as being at the Intermediate stage. For the *program management function*, risk Identification was judged as being at the Intermediate stage, whereas Risk Assessment and Allocation were slightly more mature, being between the Intermediate and Standardised stages. Risk Appetite was assessed as being between Rudimentary and Intermediate stages.

Risk identification in the *web-based SAP ERP* project does not involve end-users, and the project manager registers potential risks in an ad-hoc manner, which are then formalised in status reports. Project sponsors and Steering Committee members do not encourage anticipation of risks, but rather significant risks (such as lack of resource availability) are identified as these occur. Project team members do not make full use of their freedom to act in this regard. These features and the selected labels suggest risk Identification, Assessment, and Allocation are clearly at the rudimentary stage. The project manager assessed the risk appetite as being at the Intermediate stage, having selected a combination of labels at Rudimentary and Intermediate stages as matching with current status of the project.

For Risk Identification in the *program management function,* a number of labels from the standardized stage relevant to industrialization projects were selected, such as "visibility on new sourcing, make of buy decisions" and "visibility of implications of risk associated with all relevant suppliers". However, there was no overall matching of labels at the Standardized stage for this dimension, which was assessed as Intermediate. Regarding Risk Assessment, several features suggested a Standardized stage rating, but certain crucial capabilities indicative of the Standardised stage were not available – for example, "Impact estimation includes secondary effects", "Certain use of Quantitative Methods" and "Considers secondary effects which extend beyond immediate impact". In terms of Risk Allocation, certain aspects remained weak – for example, not all people working on a project could actually use the risk management plan, making it difficult to provide input on items with commercial impact. The level of collaboration among stakeholders was sub-optimal as there are no "Contracts with formal risk agreement bearing clear financial liabilities", nor are "All stakeholders are open in their disclosure of all risk information." Both Risk Assessment and Allocation were judged to be between the Intermediate and Standardised stages. The assessment of the Appetite dimension was more varied, spanning the Rudimentary and Intermediate stages. There were some labels linked to

the Rudimentary stage – for example "No nominated risk manager" - and not all project team members were trained in risk management, which is a requirement of the Intermediate stage. There was a clear failure to meet several of the specifications at Standardised stage, for example, there was no "Risk response effectiveness review", there was no recognition of the value of risk management, and there was a lack of systems functionality to provide variance reports regarding project original scope and project outcomes. Overall, Risk Appetite was deemed to be between Rudimentary and Intermediate stages.

Overall, the program management function attained a somewhat higher maturity rating than the web-based SAP ERP project. This possibly reflects the fact that for several years the program management function has adhered to the company's formal Global Development and Product Evolution Process (GDPEP), which includes elements of risk management. Although IT projects follow a similar process, working practices are not as well-developed as in the product development area, and this is clearly reflected in the maturity assessments.

A major benefit of using the model to assess risk maturity, is that it can provide the basis for an action plan to advance the organisation's capabilities in risk management. A review of the labels assigned to the current and following stages in the model can act as a trigger for new initiatives and follow-on actions (Tables 3 and 4). The SAP ERP project manager is now developing a formal method to train the program management staff on what risk is and how to manage it. He also proposes defining benchmarks for tracking and reporting risk in a standardized way. Although the risk register is currently kept up to date for the issuing of status reports, it has become a box ticking activity, and the project manager now plans to emphasise the significance of the register by making the communication and mitigation of risks a standard item on every Steering Committee meeting agenda. As regards risk appetite improvement, he is now stressing to colleagues the importance of evidence to support actions taken in response to risk alerts ("Management requires risk responses implemented with evidence available").

In the program management function, the functional head is now keen to underline the importance of formalising risk identification tasks and activities, in any project plan and associated work packages. He proposes the introduction of quantitative risk methods and advanced risk analysis training for all project managers in the function. He stresses the importance of usage of the project risk management plan by all project team members.

Action plan by project / dimension	ERP system Implementation	
	Current / next stage	Suggested next steps
IDENTIFICATION	Rudimentary / Intermediate	• Integrate risk identification into the planning process. • Involve end users in the risk identification process • Improve and standardize lessons learned structure
ASSESSMENT	Rudimentary / Intermediate	• Integrate risk assessent into the project cost planning • Expand opportunity management to risk management • Train project team members on advanced risk analysis
ALLOCATION	Rudimentary / Intermediate	• Reinforce usage of project risk management • Train executives and senior management on project risk management for Steering Committee Members • Train project team members on advanced risk analysis
APPETITE	Intermediate / Intermediate	• Train executives and senior management on project risk management for Steering Committee Members • Train project team members on advanced risk analysis • Develop risk management reporting (to ensure risk responses monitoring)

Table 3. Action plan to advance risk maturity in the SAP ERP project

Action plan by project / dimension	New product developement project	
	Current / next stage	Suggested next steps
IDENTIFICATION	Intermediate / Standardised	• Increase knowledge and usage of quantitative risk methods • Improve usage and availability of lessons learned • Provide visibility of planned tasks against committed resources
ASSESSMENT	Intermediate / Standardised	• Expand the use of risk quantification and quantitative analysis • Train project team members on advanced risk analysis (e. g. consider secondary risk effects) • Develop risk management reporting
ALLOCATION	Intermediate / Standardised	• Train executives and senior management about the responsibilities of Steering Committee Members • Enforce usage of project risk management plan by all project team members
APPETITE	Intermediate / Standardised	• Ensure project risk management training for all project stakeholders including Steering Committee members

Table 4. Action plan to advance risk maturity in the program management function

5. CONCLUSION

This chapter sets out a new maturity model for assessing risk management capability in the automotive industry in Germany. The model is based on 12 responsive interviews that provided the base material for model construction. The model was then validated and refined through an on-line survey and follow-up interviews with three of the original interviewees. It was then subsequently applied in two in-house environments, one concerning the implementation of the SAP ERP product, the other the program management function. The model can be used to gauge the capability level of an organization as a whole, or can be used to assess a particular

project. Once an initial assessment of maturity stages has been made, the model can be used as a guide or for the development of action plans and initiatives to improve different aspects of risk management.

The model can be used in practice in a variety of ways and contexts and for different purposes. Company project practitioners may select the appropriate labels from each dimension to assess their risk management capability. Senior management and project practitioners can identify a desired maturity stage; identify gaps in their capabilities with the help of the label descriptors; and develop a list of actions required to reach the chosen stage. In a training or workshop session, the model can also be "deconstructed", removing the allocation of labels to specific maturity stages, with project participants selecting labels that appear most appropriate to the environment in which they work. Ensuing debate can then suggest the current maturity level for that particular project risk management environment.

Joustra (2010, p.3) refers to project risk management as a set of activities often perceived as a "bolt-on-extra" rather than being integrated with the project management process and organization. This maturity model can be seen as an integrating matrix that encompasses a range of elements relating to process and systems and to organizations and people. The matrix can also be viewed as a means of achieving improved communication within and across a project team, termed the "instrumental effect of risk management" by de Bakker et al. (2011, p.76). A communicative effect occurs when stakeholders deliberately use risk management to convey messages to others, with the aim of influencing their behaviour, synchronizing their perception, and making them aware of the context and their responsibilities. As PwC (2021) note, risk management systems and infrastructure "provide an integrated platform to communicate identified risks and escalate decisions to senior management, as well as sharing good practice across the organisation" (p. 2). The matrix stimulates action and increases the effectiveness of the action, synchronizing stakeholders' actions and perceptions, making a situation more predictable which can lead to less uncertainty (de Bakker, Boonstra, & Wortmann, 2014).

Overall, the model has limitations. It has been developed from a small sample of practitioners in the German automotive industry. However, the participants have over 200 years of relevant project management experience between them, providing a unique knowledge base that was explored in depth in the interviews. Previous knowledge and experience also informed

judgements on the significance of specific factors, processes, or capabilities. The model is also aligned to the automotive industry and the particular type of projects that operate in this environment. The qualitative model provides a set of characteristics (labels) typifying different stages of risk management maturity, relating to both processes and systems, and to organisational and people aspects.

Future research directions will focus on using the model in different business environments, and developing its pedagogic and operational potential. The application of the model to date has provided valuable insights into the subjective phenomena of success and failure, and the link to the maturity concept has added to this area of knowledge. The model will be applied by the authors in other contexts in the host company, but would also benefit from application in other automotive organizations in other countries, and then in different industries. It has the potential to be developed into a more generic model with wider applicability, with more industry specific variations at a secondary level.

This chapter provides new knowledge on how to integrate multiple rationalities of risk management coexisting in a project with the objective of supporting rational and consistent decisions in projects. As a contribution to theory, the maturity model complements existing models, and is specifically oriented to the automotive industry, one of the major sectors in the global economy which is currently experiencing dramatic disruptions. Supplier dependencies and legal and normative changes are some of the issues constituting serious risk to this industry. As the OECD (2021) recently concluded "the maturity model will help an administration assess…. where they see themselves as to their current level of maturity and the kind of processes and broad outcomes they may wish to consider in order to improve their maturity." (p.7). The aim of this research was to support companies in the German automotive industry in achieving this endeavour.

References

Aloini, D., Dulmin, R., & Mininno, V. (2012). Risk assessment in ERP projects. *Information Systems, 37*(3), 183-199. doi: 10.1016/j.is.2011.10.001

Bannerman, P. L. (2008). Risk and Risk management in software projects: A reassessment. *The journal of systems and software, 81,* 2118–2133.

Bazaeea, G., Hassanib, M. & Shahmansouri, A. (2020). Identifying Blockchain Technology

Maturity's Levels in the Oil and Gas Industry. *Petroleum Business Review, 4*(3), September, pp. 43-61

Berntzen, L. (2013). Citizen-centric eGovernment Services. in *CENTRIC 2013, The Sixth International Conference on Advances in Human oriented and Personalized*

Mechanisms, Technologies, and Services, ThinkMind, 132-138. ISBN: 978-1-61208-306-3

Biedenbach, T., & Müller, R. (2011). Paradigms in project management research: examples from 15 years of IRNOP conferences. *International journal of managing projects in business, 4*(1), 82-104. doi: 10.1108/17538371111096908

Blakemore, M. (2006). Think Paper 2: Customer-centric, citizen centric. Should Government learn directly from business? Working paper, prepared for the e-Government unit, DG Information Society and Media, European Commision, available at http://europa*. eu. int/e-Government _research*.

Bollinger, R. (2010). *Lean Risk Management.* Project Management Institute.

Bryman, A., & Bell, E. (2011). *Business research methods.* Cambridge: Oxford University Press.

Chapman, C., & Ward, S. (2007). *Project risk management: processes, techniques and insights.* John Wiley & Sons.

Chapman, R. J. (2001). The controlling influences on effective risk identification and assessment for construction design management. *International Journal of Project Management, 19*(3)*,* 147-160. doi: http://dx.doi.org/10.1016/S0263-7863(99)00070-8

Chobanova, E. (2014). Why You Should Share Your Risk With Business Partners. Available at: http://www.executiveboard.com/it-blog/why-you-should-share-your-risk-with-business-partners/?utm_source=Tech&utm_medium=CIO-Banner&v2=banner

Ciorciari, M. & Blattner, P. (2008). Enterprise risk management maturity-level assessment tool. Paper presented at the 2008 Enterprise risk management symposium, Chicago, IL.

Crawford, J. K. (2006). The Project Management Maturity Model. *Information Systems Management, 23*(2), 50-58.

Creswell, J. W. (2007). *Qualitative enquiry and research design: Choosing among five approaches.* US: Sage publications Ltd.

Dawotola, A. W., Gelder, P. H., & Vrijling, J. K. (2012). Design for acceptable risk in transportation pipelines. *International Journal of Risk Assessment & Management, 16*(1-3), 112-127.

de Bakker, K., Boonstra, A., & Wortmann, H. (2011). Risk management affecting IS/IT project success through communicative action. *Project Management Journal, 42*(3), 75-90. doi: 10.1002/pmj.20242

de Bakker, K., Boonstra, A., & Wortmann, H. (2012). Risk managements' communicative effects influencing IT project success. *International Journal of Project Management, 30*(4), 444-457. doi: 10.1016/j.ijproman.2011.09.003

de Bakker, K., Boonstra, A., & Wortmann, H. (2014).The communicative effect of risk identification on project success. *International Journal of Project Organisation and Management, 6* (1-2), 138 - 156.

Emblemsvåg, J., & Kjølstad, L. E. (2006). Qualitative risk analysis: some problems and remedies. *Management Decision, 44*(3) 395-408.

Gauthier, J.-B., & Ika, L. A. (2012). Foundations of Project Management Research: An Explicit and Six-Facet Ontological Framework. *Project Management Journal, 43*(5), 5-23. doi: 10.1002/pmj.21288

Hartley, J. (2004). *Case study research*: SAGE Publications.

Harvett, C. M. (2013). A Study of Uncertainty and Risk Management Practice Related to Perceived Project Complexity. PhD thesis, Bond University, ePublications@bond.

Harwood, I. A., Ward, S. C., & Chapman, C. B. (2009). A grounded exploration of organisational risk propensity. *Journal of Risk Research, 12*(5), 563-579. doi: 10.1080/13669870802497751

Hillson, D. A. (1997). Towards a risk maturity model. *The International Journal of Project and Business Risk Management, 1* (1), 35-45.

Holzmann, V. (2012). Analyzing Lessons Learned to Identify Potential Risks in new Product Development Projects. Paper presented at the 6th European Conference on Information Management and Evaluation, Cork, Ireland: Academic Conferences Limited., 127 – 134.

Hopkinson, M. (2012). *The project risk maturity model: measuring and improving risk management capability.* Gower Publishing, Ltd.

Jen, R. (2009). *Visual Ishikawa Risk Techique (VIRT) - An Approach to Risk Management.* PMI Virtual Library.

Joustra, S. B. (2010). Towards the effective management of project risk in complex projects: A case study review. Retrieved from www.sk.tbm.tudelft.nl.

Khan, O., & Burnes, B. (2007). Risk and supply chain management: creating a research agenda. *International Journal of Logistics Management, 18*(2), 197-216. doi: http://dx.doi.org/10.1108/09574090710816931

Krane, H. P., Olsson, N. O. E., & Rolstadås, A. (2012). How Project Manager-Project Owner Interaction Can Work Within and Influence Project Risk Management. *Project Management Journal, 43*(2), 54-67. doi: 10.1002/pmj.20284

Lamberti, L. (2013). Customer centricity: The construct and the operational antecedents. *Journal of Strategic Marketing, 21*(7), 588-612.

Maier, A. M., Moultrie, J., & Clarkson, P. J. (2012). Assessing organizational capabilities: reviewing and guiding the development of maturity grids. *Engineering Management, IEEE Transactions on, 59*(1), 138-159.

Man, T.-J. (2007). A framework for the comparison of Maturity Models for Project-based Management. unpublished MBA thesis, *Utrecht University*.

Marshall, C., & Rossman, G. B. (2014). *Designing qualitative research.* Sage publications.

Martínez Lamas, M., Quintas Ferrín, A., & Pardo Froján, J. (2012). *Project Risk Management in Automotive Industry. A Case Study.* Paper presented at the 6th International Conference on Industrial Engineering and Industrial Management.

McClure, D. (2007). From the CIO trenches: Why some projects fail and others succeed. Gartner Industry Research.

McDonald, N. (2006). Think Paper 5: Is Citizen-centric the same as Customer-centric: October) Ccegov Project,[cited November 22 2006]. http://www. ccegov. eu/thinkpapers. asp.

Namey, E., Guest, G., Thairu, L., & Johnson, L. (2008). Data reduction techniques for large qualitative data sets. *Handbook for team-based qualitative research, 2*, 137-161.

Niebecker, K. (2009). *Collaborative and cross-company project management within the automotive industry using the Balanced Scorecard.* PhD thesis, University of Technology, Sydney.

OECD (2021). *Enterprise Risk Management Maturity Model Maturity Model*, OECD Tax Administration Maturity Model Series, OECD, Paris. Retrieved March 6, 2022, from www.oecd.org/tax/forum-on-tax-administration/publications-and-products/enterprise-risk-managementmaturity-model.htm

Olakunle, O., & Win, T. (2022). Cybersecurity and Data Privacy in the Digital Age: Two Case Studies. In M. Wynn (ed). *Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive*

Technologies.(pp. 117-131). Advances in E-Business Research Book Series . IGI-Global, USA. ISBN 9781799877127

Olsen, M. D., & Roper, A. (1998). Research in strategic management in the hospitality industry. *International Journal of Hospitality Management, 17*(2), 111-124.

Olsson, R. (2006). *Managing project uncertainty by using an enhanced risk management process.* Unpublished PhD thesis, University of Västerås, Mälardalen.

Patterson, F. D. (2002). *Project risk management and its application into the automotive manufacturing industry.* PhD Thesis, University of Warwick. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=edsble&AN=ethos.007151837&site=eds-live&scope=site&custid=s1123095 Available from EBSCOhost edsble database.

Patterson, F. D., & Neailey, K. (2002). A Risk Register Database System to aid the management of project risk. *International Journal of Project Management, 20*(5), 365.

Phoenix, C., Osborne, N. J., Redshaw, C., Moran, R., Stahl-timmins, W., Depledge, M. H., . . . Wheeler, B. W. (2013). *Paradigmatic approaches to studying environment and human health: (Forgotten) implications for interdisciplinary research*. Retrieved from OAIster database.

Project Management.com (2019). *Ineffective Risk Management – That's Risky!* White paper. PMI/Deltek. Retrieved January 19, 2022, from https://img.en25.com/Web/DeltekInc/%7Bb6abeb66-b499-4ee4-ae8d-022336a3b88e%7D_Ineffective_Risk_Management_%E2%80%93_That's_Risky_.pdf?elqTrackId=91ad96e2cb854183987f4c254d285ab0&elqaid=11820&elqat=2

PwC (2021). Enterprise Risk Management. Pricewaterhouse Coopers LLP. Retrieved March 6, 2022, from https://www.pwc.co.uk/audit-assurance/assets/pdf/enterprise-risk-management.pdf

Rübesam, T. (2015). Drug funding decision-making in hospital formulary committees in Germany. Unpublished DBA thesis, University of Gloucestershire.

Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data.* Sage.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students.* Harlow, England: FT/Prentice Hall.

Skinner, D., Tagg, C., & Holloway, J. (2000). Managers and Research: The Pros and Cons of Qualitative Approaches. *Management Learning, 31*(2), 163-179.

Taylor, F. W. (1911). *The Principles of Scientific Management.* Harper and Brothers.

Thomas, P. (2013). *The Risk of Using Risk Matrices.* (Masters Master's thesis), University of Stavanger. Retrieved from http://brage.bibsys.no/uis/bitstream/URN:NBN:no-bibsys_brage_45899/1/Thomas_Philip.pdf

TowerGroup, C. (2014). Reducing Risk Management's Organizational Drag *Executive Guidance* (Vol. Executive Guidance Q3 2014). Arlington VA: CIO Executive Board.

Vaish, R., Agrawal, A., & Kapoor, S. (2021). *AI maturity framework for enterprise applications*. IBM Corporation, Armonk, New York, USA.

Wall, K. D. (2011). The Trouble With Risk Matrices. *DRMI Working Papers Ongoing Research*.

Wang, H., Chen, K., & Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation, 2*(12), pp. 1-5. Springer Open. DOI 10.1186/s40854-016-0031-z

Wynn, M., Bakeer, A., & Forti, Y. (2021) E-government and digital transformation in Libyan local authorities. *International Journal of Teaching and Case Studies, 12* (2), pp. 119-139. doi:10.1504/IJTCS.2021.116139

Wynn, M., Turner, P., & Lau, E. (2013). E-business and process change: two case studies (towards an assessment framework). *Journal of Small Business and Enterprise Development, 20* (4), pp. 913-933. doi:10.1108/JSBED-03-2012-0044. Retrieved from https://eprints.glos.ac.uk/1382/

Yeo, K., & Ren, Y. (2009). Risk management capability maturity model for complex product systems (CoPS) projects. *Systems Engineering, 12*(4), 275-294.

Yin, R. K. (2012). *Applications of case study research.* London: SAGE Publications Ltd.

Zayed, T., Amer, M., & Pan, J. (2008). Assessing risk and uncertainty inherent in Chinese highway projects using AHP. *International Journal of Project Management, 26*(4), 408-419. doi: 10.1016/j.ijproman.2007.05.012

Zou, P. X., Chen, Y., & Chan, T.-Y. (2010). Understanding and improving your risk management capability: Assessment model for construction organizations. *Journal of Construction Engineering and Management, 136*(8). Retrieved March 6, 2022, from https://ascelibrary.org/doi/abs/10.1061/%28ASCE%29CO.1943-7862.0000175.

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

KEY TERMS AND DEFINITIONS

Enterprise Resource Planning (ERP): An integrated software package that supports all main business functions. Examples include SAP, Oracle, Infor and Epicor.

Risk Allocation (or Risk Ownership): involves allocating responsibility for managing project uncertainty to appropriate project parties. These allocations are fundamental because they can strongly influence the motivation of parties and the extent to which project uncertainty is assessed and managed by each party.

Risk Appetite (or Risk Treatment or Risk Propensity): reflects an organisation's attitude and strategy towards risk. It encompasses how risk is managed and whether exposure to risk should be reduced, or the impact of risk should be mitigated, transferred, externalized or accepted.

Risk Assessment: is the stage in the risk management process at which each identified risk is assessed for its probability or likelihood of occurrence, and its potential impact on either the project phase or the entire project.

Risk Identification: involves the detection and classification of all known and - as far as is possible - unknown, risks, thus producing the foundation upon which the overall risk management process can be established.

APPENDIX 1: RISK IDENTIFICATION - MATURITY STAGE DESCRIPTIONS

RISK IDENTIFICATION
Rudimentary stage: Risks are identified in an *ad hoc* manner, and the process may be driven by one single group or individual, thus missing the opportunity to consider other groups' views and enhancements. Potentially high risks, such as those related to compliance, may remain unaddressed, as the process of identification is eventually subsumed within other project initiatives, and risk logs are not systematically updated during the project life cycle. The individuals involved in the project may well share a negative perception of risk and may be reluctant to bring these risks forward for discussion and review. End users who may have experience of the project environment have no involvement in the risk identification process.
Intermediate stage: The project plan does not show any specific work package or activities for project risk identification. Project records are maintained, but central documentation, such as lessons learned, is not standardised. The documentation is unstructured, and data searches on project history are cumbersome. Risk management tends to focus on individual risks managed at lower levels within the team. The activity may be a single action, without clarity on how to periodically review the validity of identified risks, conduct new identification sessions, monitor risk amelioration plans and communicate identified risks to all relevant stakeholders. Risks are often identified as they occur, leaving inadequate time to address them effectively. The documented risk item descriptions may be ambiguous, in many cases describing potential events instead of the root cause that originates the risk. Impact oriented risk descriptions with no insight into how to manage risks proactively are typical at this stage. Some compliance aspects are addressed, but the risk identification process may have failed to recognise some significant risks. Potentially significant risk items may be omitted in reporting. There is a lack of knowledge of the meaning and significance of risk and uncertainty which, together with the lack of involvement of specific stakeholders, increases the subjectivity of how potential events are documented as risks for the project. Several stakeholders and groups with significant involvement in the project do not contribute to risk identification.
Standardised stage: Some standard guide or developed documentation to support project risk identification may be used, but the process may not be known to all stakeholders nor implemented by the project management practitioners with due rigour. Practitioners follow specific project and risk management guidelines and instructions – these may provide a methodology to categorise the project's complexity based on several dimensions such as business impact, project team size or project schedule. Project planning and risk management are fully integrated. Routine planning reviews consistently use lessons learned logs, as well as risk register databases to aid risk identification. All stakeholders contribute to the process whereby their input and their views are considered. The risk register template provides clear risk classifications which can be mapped to established standard risks. Project categorisation establishes minimum frequency rules to perform risk identification. The project team adheres to these rules, and evidence regarding risk identification is documented, and senior members are involved in the process. A holistic view of the project is required in order to properly identify risks. Risk identification is performed at a group level, encouraging and integrating all stakeholders' views. Project team members are knowledgeable and use quantitative data and methods such as Monte Carlo simulation when required. Documentation, such as lessons learned logs and risk registers, is standardised to a certain level and regularly maintained. Records are accessible by all project team members. An active role for the end users is promoted. These are permanently informed about project progress, and they are actively involved in the testing and validation process.
Corporate stage: Use and monitoring of earned value (EV) management supports the identification of potential risk areas. A high maturity in risk identification allows a focus on the key risks. The risk identification process is driven by an initial iterative top-down approach based on the project's purpose and strategy. The risk prioritisation is based on the project's strategic goals. Risk analysis must focus on the right questions and the fundamental purpose of the project. The big picture needs to be understood from the beginning instead of adding risk effects from different areas. The project team ensures formal communication about the identified risk items within the organisation while keeping an overview of the interrelationship or impact of other projects' risks. There is good evidence that risk data emerging from all stakeholders is reported and documented in a timely manner. Systems supporting risk management are available to all stakeholders, and these enable real time reporting.

APPENDIX 2: RISK ASSESSMENT - MATURITY STAGE DESCRIPTIONS

RISK ASSESSMENT
Rudimentary stage: Risk assessment performed at the rudimentary stage is not regularly maintained. Changes in the project which could influence the impact or the likelihood of the event are not considered. As results are not reviewed regularly, risk information may become stale. The approach can be described as static as opposed to an active style. Risk assessment tends to be considered only when the project is in difficulty, or when it is imposed by senior management. Risk responses are often based on rapid decisions reflecting a poor understanding of the alternative courses of action. Sometimes there is a delay between risk identification and response implementation, which results in their ineffectiveness. The organisation focuses exclusively on threat management when addressing uncertainty and does not consider opportunity management. The assessment results are not reflected in the cost forecast. Typically, no fall-back plans are developed.
Intermediate stage: Risks are updated, and certain risk categorisation is assigned with the utilisation of risk register templates. Risk description tends to be impact-oriented and often lacks context and identification of relevant sources of uncertainty. Sometimes the risk descriptions provide some indication regarding the source of risks. However, probability estimation is weak. The project team deploys mainly qualitative assessments, e.g., a probability and impact matrix. Quantitative schedule analysis is not generally executed. In addition, existing expertise from previous projects is used as an input for these assessments. The lack of standards to estimate impacts and the difficulty in quantifying likelihood increases the subjectivity of the risk assessment results, and therefore any subsequent risk prioritisation. Individuals required to participate in risk assessment do not completely understand how to assign the likelihood and the impact of the potential risks. They struggle with how to rate the risk statements against prescribed risk tolerance thresholds. There is a lack of knowledge of the risk concept and its potential effect on the project outcomes. The organisation and management would rather deal with issues than with risks - it is embedded in the culture; resource constraints and a focus on problem-solving make it difficult to undertake an adequate risk assessment.
Standardised stage: Project categorisation is performed, based on several dimensions reflecting project complexity. The greater the complexity, the higher is the level of management attention and risk assessment detail. The project teams are capable and sufficiently knowledgeable to undertake risk assessment deploying quantitative quality methods. The team also uses certain risk analysis quantitative methods, such as Monte Carlo, decision trees or Bayesian belief networks, underpinned by a sound understanding of risk with significant thought put into identifying relevant sources of uncertainty. There are clear minimum frequency rules on when to perform risk assessments. Action response plans to the identified risks are regularly reviewed. The description of the risks documented in the risk register is useful for qualitative risk analysis. Some risk effects may extend beyond the immediate risk impact. These effects could also exacerbate other existing risks. Such secondary risks are considered in the assessment. There is a clear method to estimate the Overall Risk Priority Rating, which determines the threshold for taking a certain risk into the risk response plan or not. The threshold for taking events into the risk register's response plan is based on estimated costs or project delays in case of the event happening. Risk assessment is reviewed against the likelihood of any risk happening – a risk assessment at standardised level is one that aims at preventing the events from happening in the first place. Project reporting supports management with visibility of the high impact risks, with clustering and prioritisation functionalities. Systems provide risk aggregation by customers, groups of programs or project portfolios. Steering Committees challenge the assessment process and initiate appropriate escalation when required. A method is designed for the project manager to measure team members' commitment by means of their performance.
Corporate stage: The organisation assesses systemic risks based on past projects; this assessment can be part of a continuous improvement initiative. This initiative evaluates those risks in more detail and determines how to mitigate or change procedures or ways of working to minimise, if not eliminate, the potential impact on the project. Risk assessment includes the quantification of mitigated risks, benefit of risk responses and secondary effects. The project budget contains appropriate funding for overall risk costing. The project

managers measure and monitor the project team members' performance against project deliverables. The risk register lists are the result of all stakeholders' and functions' inputs into an integrated system.

APPENDIX 3: RISK ALLOCATION - MATURITY STAGE DESCRIPTIONS

RISK ALLOCATION
Rudimentary stage: Risk ownership is not reviewed and remains assigned to the same individual during the different project phases. Risk allocation is hampered by the lack of risk disclosure with the contracting parties, e.g., suppliers or external customers. Individuals from different functions involved in the project do not feel responsible for the program - it is the project manager that will be associated with the result - and therefore those functions do not feel responsible for the risk which remains with the project manager. Team members are mostly reluctant to own the risks. There is the general impression that assigning somebody a risk item equates to telling them they are doing something wrong. The reluctance of certain stakeholders, in particular suppliers, to divulge new information on risk prevents them being effectively allocated to individuals or groups. Individuals involved in the project perceive risks as intrusive. Being owners of a risk item represents for them an additional burden. In most cases, they do not feel motivated to talk about risk and the associated problems of risk ownership. The organisation does not actively recognise the support of good risk management practice.
Intermediate stage: Central risk allocation is carried out only by the project manager with most risks remaining with the project manager. These are characteristics of risk ownership centricity. Project managers maintain constant communication with third parties and customers to agree on risk accountability. However, there are groups with a critical role in the project who have little or no involvement in the risk allocation process. Suppliers provide risk information; nevertheless, this is sometimes not complete. Some project managers recognise the inefficiency of this centric approach, but sometimes they are reluctant to receive input from other team members or functions. This seems to be dependent on the personal attitude of the project manager. Some of them do everything, from assigning the risk, maintaining the risk registers, and even owning most of the actions documented in the risk response plan. Steering committees are more status boards; in their meetings, risk allocation is not reviewed. Individuals working on the project usually only report in a dotted line to the project manager, but direct line to their functions. This negatively influences risk ownership and therefore allocation. There is a lack of willingness to own risk by the project team members.
Standardised stage: There is a clear procedure to assign risks in the risk register. Clear instructions determine at what point in time these assignments are to be documented or reviewed, typically at the end of any given project phase. Organisations review and assess team members' expertise to assign risk items to the appropriate person. Functional groups involved in the project are able to assign the identified risks internally without much involvement from the project manager. By doing so, the project manager is released from risk allocation activity, allowing him/her to concentrate on other critical activities. The organisation has established guidelines to clearly identify and specify the risk taker, be it the project sponsor, the project manager, or the stream lead. The introduction of prescribed risk classification and job descriptions in the project provides the opportunity to introduce some automation in the risk allocation process. All identified risks have a risk owner with authority and skills to undertake the required actions from the response plan and who accept responsibility. The organisation has established guidelines to clearly identify and specify the risk taker. In some cases, risk ownership is documented in the contracts awarded to suppliers. The contracts contain formal risk agreements with clear financial liabilities for bearing risk. Collaboration and risk sharing are required between partners of different size. Risk sharing promotes risk disclosure; it is also a means of engaging the customer in the process. All stakeholders are open in their disclosure of all risk information. Suppliers operate risk management processes which are complementary to the ones used in the project. In terms of systems, risk registers are accessible and used by all members and functions. All team members are trained in the use of these systems. Steering committees audit the risk allocation process, and steering committee members actively support the risk owners and their mitigation actions. There is evidence that all people working on the project use the risk

management plan. Risk project team members know enough about the ultimate project goal and align their actions accordingly.
Corporate stage: There is transparency of the escalation procedure of risk allocation for project team members. These procedures address the following: Who is the next person the risk is allocated to when I am not able to cope with the risk? Who needs to take a decision when the actions described in the risk response plan are well above my responsibility? In term of systems, the risk database is consistently maintained and enables multi-user concurrent access. Management actively rewards good risk management practice and supports the risk owners as contributors to project success. Good risk management practice continuously monitors and tries to improve the risk management processes, sets comprehensive and stretching targets, and promotes high-performing employees in regards to risk management.

APPENDIX 4: RISK APPETITE - MATURITY STAGE DESCRIPTIONS

RISK APPETITE
Rudimentary stage: There is no project-specific risk management plan. Fall back decision points (such as a date, or the point in the project's schedule at which a decision on implementing the fall back should be taken) are either not identified or ignored. Risk records cannot be retrieved reliably. Senior management makes little or no use of risk management. Executives fail to challenge the documented project risks, as they feel uncertain as to how to deal with risks, and their comfort area remains on how to address issues. Team members have little understanding of their responsibilities. In some cases, there is no nominated risk manager. People avoid raising risk items. Team members are afraid that if they bring up their concerns, they may end up being made responsible for the potential risk. There is a general failure to offer competency development plans for program managers, resulting in a misalignment of employee competencies with the organisational strategy. This lack of potential development negatively affects the project management performance from the risk management perspective.
Intermediate stage: Risk is not at the top of the executive agenda. Risk responses are rarely monitored. Steering committees are typically status boards; risk is discussed only during phase exits or program reviews. However, management only adopts mainly qualitative risk analysis. There are no formalised standard quantitative methods - the use of these may vary from project to project, and the decision to use quantitative methods is left to the project manager or subject matter expert. Sometimes a fall-back decision point fails to result in a decision. Teams are typically trained in project risk management. Project team members start doing some risk identification and assessments. As the project moves forward, the project manager and team members typically come under time pressure and risk management falls increasingly behind. As the team is not able to cope with the execution of the planned risk mitigation actions, more issues are raised in the open issue list. As resources are assigned to address the issues, less time and resources are available for risk management. Functions still not active in the project at a certain point in time are requested to contribute with their risk assessment to consider potential future implications of current project developments or status. There are systems designed to document risks, but these are not common to all functions and may not be accessible to all project stakeholders.
Standardised stage: Project management is supported with guidelines and methods containing clear, unambiguous process descriptions. Companies train staff in project management specific to their industry, let their risk management process be assessed by auditors, and follow risk management process reference models. Risk items have adequate visibility at project phase exits and review. Executives request evidence for risk mitigation actions and dictate compliance with certain risk management activities. Responses to significant risks tackle risk at source. Importantly, risk response effectiveness is reviewed. Risk responses are consistently implemented. Executives and steering committees provide leadership in risk management. Executives request evidence of risk activities and challenge the risk management process. They support an iterative top-down approach to risk management which supports key strategy decisions first. The risk management methodology is used flexibly, and is adapted to project particularities. Project management practitioners within the organisation stress the importance of project governance, clarity of roles and responsibilities, authority, and

competency. Management has the ability to quantify risks associated with capacity shortcomings. Project governance and project human resource management are integrated into the overall project plan. The risk management applications enable 'post-mortem' analysis which compares historical original project scope and outcomes. Project risk management applications enable audit trail functions.
Corporate stage: Risk management is integrated into project planning. The project plan considers routine activities that aid risk identification and assessment. Cost of risk responses is considered. Risk responses which are consistently implemented are supported by cost benefit analysis which also considers secondary risks. Lessons learned are effectively incorporated into a continuous improvement programme. Organisations have at their disposal all elements needed to perform continuous improvement initiatives in risk management. These include project history with risk registers; risk items detailing whether events occurred or not; results of mitigation actions; systems that support queries/aggregation. Project risk management capability is assessed and process improvements in risk management are implemented.