sustainability

Article

Improving Operational Risk Management Using Business Performance Management Technologies

Bram Pieket Weeserik and Marco Spruit *

Department of Information and Computing Sciences, Utrecht University, Princetonplein 5, 3584 CC Utrecht, The Netherlands; bram.pieket.weeserik@celcus.nl

* Correspondence: m.r.spruit@uu.nl; Tel.: +31-(30)-253-3708

Received: 21 January 2018; Accepted: 22 February 2018; Published: 28 February 2018

Abstract: Operational Risk Management (ORM) comprises the continuous management of risks resulting from: human actions, internal processes, systems, and external events. With increasing requirements, complexity and a growing volume of risks, information systems provide benefits for integrating risk management activities and optimizing performance. Business Performance Management (BPM) technologies are believed to provide a solution for effective Operational Risk Management by offering several combined technologies including: work flow, data warehousing, (advanced) analytics, reporting and dashboards. BPM technologies can be integrated with an organization's Planning & Control cycle and related to strategic objectives. This manuscript aims to show how ORM can benefit from BPM technologies via the development and practical validation of a new maturity model. The B4ORM maturity model was developed following the Design Science Research approach. The maturity model relates specific maturity levels of ORM processes with BPM technologies applicable for a specific maturity stage. There appears to be a strong relationship (0.78) with ORM process maturity and supporting BPM technologies. The B4ORM maturity model as described in this manuscript provides an ideal path of BPM technologies related to six distinctive stages of ORM, leading towards technologies suitable for continuous improvement of ORM processes and organization-wide integration.

Keywords: risk management; Enterprise Risk Management; Business Intelligence; Corporate Performance Management; maturity model

1. Introduction

Operational risks are the root cause for many of the (large scale) financial failures in the past decades [1–4]. The aforementioned studies note that operational risks are not new: human mistakes, fraud, theft, process failures, system errors and external hazards, such as fires and floods, have been around for decades. However, the impact of operational risks was most often relatively insignificant. In contrast, recent trends such as globalization, global internet connectivity, and (value) chain dependencies, have made operational risks more significant than ever before. With increasing requirements, complexity and volume of risks, information systems are believed to provide benefits for risk management activities [5–8].

An increasing number of organizations, mainly in the financial sector, are required by regulatory authorities or by law to manage their operational risks. Fontnouvelle, et al. [9] found that in the early 2000s most international banks were already allocating more financial reserves to account for operational risks than for market risks. Operational risks tend to become more relevant in different types of organizations [10,11]. For example, operational risks have been studied for years in the healthcare sector [12,13]. Marques [14] and Cruz [15] describe how effective risk management influences the results in infrastructure contracts. Additionally, operational risks are becoming increasingly important in the energy sector [16]. Mitra, et al. [17] describe that the importance of operational risks varies depending on industry and the markets that an organization operates in. They found that financial organizations have the lowest expected returns on operational risk, and basic material producers have the highest return. Operational risk is different from other risks, such as credit risk or market risk, because operational risk is usually not taken to retrieve an expected return. Operational risk exists in every organizational activity. Inappropriate management of operational risks can result in significant losses.

With increasing requirements, complexity and volume of risks, information systems provide benefits for integrating risk management activities and optimizing risk management performance. Information systems and technologies can support the improvement of operational risk management processes [6–8]. Lam [18] and Arnold, et al. [19] describe performance management systems as a set of technologies from the information systems domain suitable for application to support the operational risk management process. In recent years, this recognition is supported from practice by consulting firms, PwC [20] and Deloitte [21] who state Business Performance Management and its supporting technologies could provide effective support for risk management processes.

Nyenrode Business University [22] performed a large scale study about the state of risk management practices in the Netherlands. Nyenrode writes risk management should be part of the Planning and Control cycle, aligned with strategic goals of the organization. Integrated risk management and better collaboration lead to a more mature risk management. These benefits could only effectively be achieved by using appropriate software. However, Nyenrode concludes that many organizations do not appear to know what software features to use for effectively improving risk management.

Several sources [19,23,24] describe Business Performance Management (BPM) related technologies such as workflow, centralized storage, and dashboarding, which could provide a solution for Operational Risk Management (ORM) issues. However, it remains unclear whether the full spectrum of Business Performance Management technologies is suitable for improving operational risk management processes and whether the same set of BPM technologies are applicable for all types of organizations. Additionally, there appears to be no existing or specific guidance for organizations seeking to improve operational risk management processes using Business Performance Management Technologies (BPMT).

The following section describes important background information about the context and the domains of Operational Risk Management and Business Performance Management Technologies. This research follows the Design Science approach using the methodology as described by Hevner, et al. [25]. The Design Science approach describes an artifact to be studied and validated. The section Materials and Methods describes and motivates the development of the maturity model artifact. Maturity models are used to guide improvements of certain processes using capabilities or technologies, corresponding to levels of maturity. Sections four and five show the results of validating the maturity model in practice from two different perspectives: ORM as process and the use of BPM technologies. The results are concluded with some recommendations for further research and potential applications in practice. The scientific contribution, some remarks and implications regarding quality are the points of discussion in the final section of this manuscript.

2. Theoretical Framework

Several studies [1,26–30] describe that risk management approaches throughout the 1980s and 1990s had grown into different silos of risk management practices; each type of risk was managed independently. Different silos of risk management practices lacked organization wide overview and insights. This led to concepts of integrating organization wide risk management practices with the objective of eliminating redundancies in double activities and other inefficiencies.

Culp [31] describes that the classical view on risk management was mostly financial and insurance focused on reducing financial drawbacks, rather than actually managing risks. In the

1990s, a transformation started towards more integrated risk management practices, combining all risk management activities in Enterprise Risk Management and appointing a Chief Risk Officer (CRO) on board level of organizations. According to Olson and Wu [32], the concept of Enterprise Risk Management (ERM) developed from the 1990s into a discipline around the 2000s. In this period the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed an internal control framework that was aimed to counter fraud. The first internal control framework was published in 1992, but gained wide acceptance following financial failures of the early 2000s, such as the Enron and WorldCom scandals.

Nowadays COSO ERM is a de facto standard risk and control framework used within many larger organizations. COSO is aimed at corporate wide governance including enterprise wide risk management. Gordon, et al. [33] state Enterprise Risk Management is a subset of an organization's management internal control system. Enterprise Risk Management is the domain that provides a holistic approach on risk management practices throughout an entire organization and is related to the organization's objectives. ERM combines different risk management practices into a holistic discipline.

Another perspective on enterprise wide integration of risk management practices, comes from a technology perspective [34]. The Open Compliance and Ethics Group (OCEG) is a nonprofit organization with roots in the IT services industry. The OCEG developed standards and guidance on integrating Corporate Governance, Risk Management and Compliance (GRC) practices. Integrated Governance, Risk Management and Compliance consists of four holistic and organization wide components: strategy, people, processes and technology. Correctly managing and supporting operations with integrated GRC results in ethically correct behavior, improvements of efficiency and effectiveness [35]. Racz, et al. [36] researched the relationships between ERM and GRC, as shown in Table 1. The authors describe two different perspectives:

1. ERM is a full subset of GRC, where GRC is the umbrella concept, overreaching ERM;
2. ERM and GRC overlap. Both share common objectives, processes and technologies, however both domains have their own specific processes as well.

Table 1. Comparison of different perspectives on ERM and GRC.

Factors	Enterprise Risk Management (*ERM*)	Governance, Risk and Compliance (*GRC*)
Root domain	Accounting	Information Technologies
Goal	Reasonable assurance regarding the achievement of entity objectives [37].	Ethically correct improving efficiency and effectiveness trough GRC [35].
Type	ERM is a continuous **process** across the enterprise [37].	GRC is an integrated, holistic **approach** [35].
Approach on integration	Integrating silos of different types of risk management [30,38].	Silos of duplicating efforts in the different areas of governance, risk and compliance [39].
Role of Information Technology	Information Technology as enabler of firm agility and flexibility [19].	Information technologies as an enabler for GRC to increase compliance procedures and concurrently reducing costs [40].

2.1. Operational Risk Defined

Power [3] writes that the term "*operations risk*" first appeared in the early 1990s. When the Committee of Sponsoring Organizations of the Treadway Commission (COSO) officially introduced its first version of the integrated internal control framework in 1991. According to Power, the term "operations risk" did not gain full attention until 1999 when the Basel Committee introduced Basel II.

Around the 2000s the Basel committee identified a need for a new type of risk appearing from fraud and human misbehaviors such as theft, mistakes or fraudulent actions, which were not covered by any other type of risk management. Therefore the Basel committee defined operational risk as: "*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.*

This definition includes legal risk, but excludes strategic and reputation risk" [41]. The committee states organizations can adapt or modify the definition to their own specific context.

The Basel committee [42] detailed operational risks further into specific event type categories:

1. **Internal fraud**, losses related to intentional or inappropriate acts. Circumventing laws, regulations or organization policy, involving at least one internal stakeholder;
2. **External fraud**, losses related to intentional or inappropriate acts regarding misappropriate property, information breaches (cyber-crime) or acts that circumvent the law by a third party;
3. **Employment practices and workplace safety**, losses related to acts inconsistent with health, safety or employment laws or agreements;
4. **Clients, products and business practices**, losses arising from a failure to meet professional obligations to clients or from the nature or design of a product;
5. **Damage to physical assets**, losses or damage related to natural disasters or other events;
6. **Business disruptions and system failures**, loss from business disruptions and system failures;
7. **Execution, Delivery & Process Management**, losses resulting from process management, transaction processing or external relations, such as trade counter parties and vendors.

Operational risk, as defined by the Basel Committee, is a financial term, meaning the term operational risk is well known and understood by banking and insurance organizations. Within the financial services industry, operational risks are often part of COSO ERM activities and related to corporate governance activities.

2.2. Operational Risk Management

Properly managing operational risks is described as a 'three lines of defense' model [11,43,44]. Operational risk events and their consequences should be handled at the organization function in which they occur, however, severe consequences should be directly reported to the board and other stakeholders. Proper execution of the operational risk actions on the first lines should be managed and monitored by an (independent) function within the organization, called a second line of defense. A third line of defense is formed by an (independent) audit committee assessing the complete operational risk management structure, process and implementation on a regular basis. An audit team can be internal, external or both.

Effective risk management practices require a structured process. In 1974 Gustav Hamilton developed the "risk management circle" that shows risk management as a continuous process. Hamilton's publication is described as the first to depict risk management types and activities as applied in an organizational risk management context [45]. Over the following years from several different domains in engineering, accounting and more disciplines developed their own risk management best practices. For example, Carr, Konda, Monarch, Ulrich and Walker [46] from Carnegie-Mellon university created a risk management process for use in software engineering.

In 1995, Standards Australia (AS) and Standards New Zealand (NZS) published the first official Risk Management Standard. Purdy [47] writes that the AS/NZS 4360:1995 standard was created by a team from multiple disciplines working together to create a common frame of reference for risk management.

In 2004, COSO ERM was published, providing an internal control framework including risk management from an accounting perspective. COSO ERM aimed to provide a framework including risk management activities as an essential part in steering organizational objectives.

In 2005, The International Organization for Standardization (ISO) identified a need for resolving inconsistencies and ambiguous practices from different disciplines. The ISO created a working group including hundreds of experts from 28 different countries to write a global standard providing a definition, generic application practices, and one language of risk management. Four years later the ISO Committee for risk management published ISO 31000. Purdy describes that the plan, do, check, act cycle by Deming and structure from the Australian and New Zealand standards were used as an important source by the ISO committee to develop ISO 31000 for risk management. However, most of their content was completely rewritten.

Although COSO ERM and ISO 31000 use a different language, both risk management processes appear to have a similar structure. As presented in Table 2, both frameworks are structured in a similar way, however their approach, some activities and terminology are different.

Table 2. Comparing process activities between COSO ERM and ISO 31000.

COSO ERM [37]	**ISO 31000** [48]
Internal Environment	Internal and external environment
Objective setting	Identifying and describing objectives
Risk Assessment: 1. Event identification 2. Risk assessment 3. Risk response	Risk Assessment: 1. Risk identification 2. Risk analysis 3. Risk evaluation
Control activities	Risk Treatment
Information and communication	Communication and consultation
Monitoring activities	Monitoring and review

2.3. *Performance Management*

Performance management is an abstract term that can be confusing because of its broad nature and the meaning of the words 'performance' and 'management'. It all depends on what kind of performance is intended to be managed.

Hoffmann [1] defined performance as "valued contribution to reach the goals of an organization". In general, Performance Management can be seen as a way for organizations to become more successful and make sure they are delivering against their strategic priorities. The process of performance management starts at the highest level of the organization by translating a mission and vision statement into a strategy, composed of objectives and priorities. These objectives and priorities should then be translated to high level measures and then by middle management into measures on operational levels. These high-level measures and operational measures express organizational performance. The performance should then be communicated by reporting the measured performance and managed to align people and culture with strategic goals.

2.4. *Performance Measurement*

Performance can only be managed when the actual performance is known. Performance Measurement is the method of developing performance indicators and relating them to contextual factors to enable measurement of performance. Performance could then be actively improved by management. According to Lebas [49], Performance Measurement is a critical and inseparable component of Performance Management.

Simons [50] describes performance measurement systems: "Assist managers in tracking the implementations of business strategy by comparing actual results against strategic goals and objectives. A performance measurement system typically comprises systematic methods of setting business goals together with periodic feedback reports that indicate progress against goals".

2.5. *Business Performance Management*

Business Performance Management evolved from Decision Support Systems (DSS) in the 1960s and developed throughout the following years into Executive Information Systems (EIS). The development of aggregated data storage, known as Data Warehousing (DW), led to the inception of

Business Intelligence (BI) in the late 1980s [51]. Business Performance Management (BPM) builds on the foundations of BI, extending BI with planning, consolidation and process automation [52].

Business Performance Management (BPM) is defined by Sharda et al. [53] as "the business processes, methodologies, metrics and technologies used by enterprises to measure, monitor and manage business performance." Synonyms for BPM are Corporate Performance Management (CPM) by Gartner research, Enterprise Performance Management (EPM) by Oracle and Strategic Enterprise Management (SEM) by SAP. In this research the term Business Performance Management (BPM) is used, because this term is not related to a specific organization or technology vendor.

BPM is supported by a set of technologies for integrating and analyzing performance-relevant data, supporting decision making and facilitating the communication of decisions. Frolick and Ariyachandra [51] describe BPM developed from DSS to EIS, then combined with Data Warehousing into Business Intelligence. Melchert et al. [54] describe Business Performance Management as a combination of technologies from the domains: Business Intelligence, Business Process Modelling and Enterprise Application Integration. Combined with elements from Process Performance Management, Business Process Automation and Real-time Analytics. Figure 1 combines all BPM related technologies.

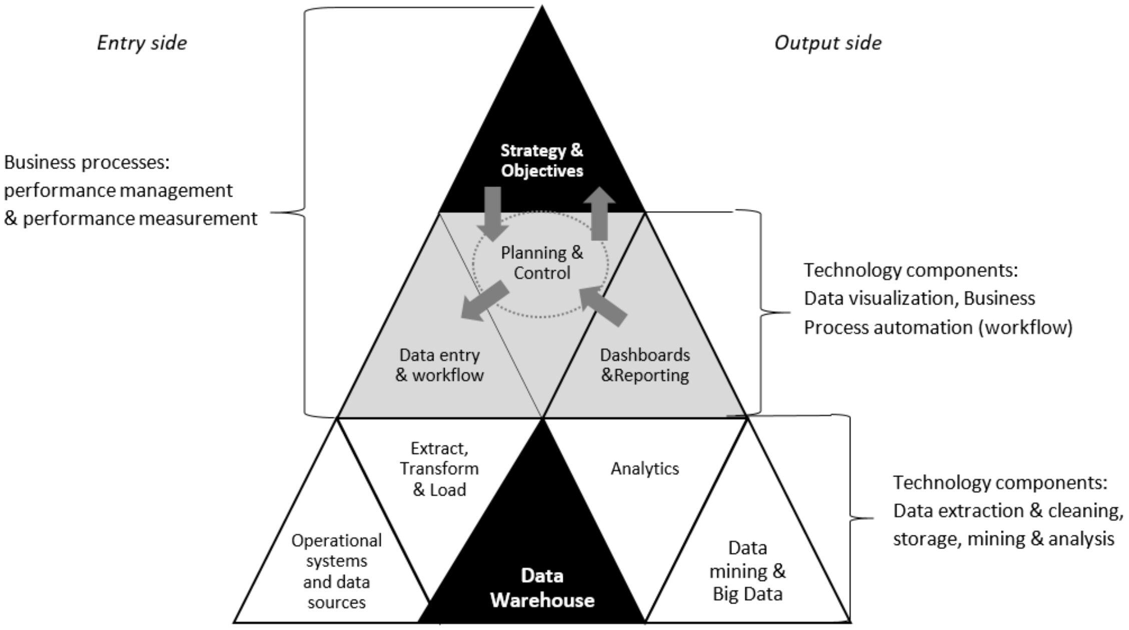
Entry side
Output side
Business processes: performance management & performance measurement
Strategy & Objectives
Planning & Control
Data entry & workflow
Dashboards &Reporting
Technology components: Data visualization, Business Process automation (workflow)
Extract, Transform & Load
Analytics
Operational systems and data sources
Data Warehouse
Data mining & Big Data
Technology components: Data extraction & cleaning, storage, mining & analysis

Figure 1. The Business Performance Management (BPM) pyramid; BPM related processes and supporting technologies, based on: Melchert, et al. [54], Frolick and Ariyachandra [51], Samsonowa [55].

The BPM pyramid is intended to summarize the domain of Business Performance Management. It is composed of three different layers: Strategy and objective setting at the top, because that is the ultimate goal related to (*strategic*) management, similar to the [56] BI pyramid. The middle layer is an important interface layer between organizational planning & control and supporting technologies. Data entry and workflow enable planning on the entry side. Dashboards and reporting interface the results and enable controlling on the output side. Proper implementation of this interface layer may also be facilitated by descriptive meta-algorithmic models as best practices process guides [57]. The bottom layer is only technology related, facilitating input of clean source data on the entry side. Building on a Data Warehouse as central data storage, data mining and big data enhancing the data on the output side with analytics, as source for dashboards and reporting [58].

Business Performance Management technologies as described can support any process with a continuous improvement cycle—using goal setting, performance measurement and reporting.

Integration of operational risk management practices appears to benefit from several Business Performance Management technologies, such as workflow and data entry to support collaboration between the three lines of defense and other stakeholders, such as the board of directors and shareholders. Analysis, dashboarding and reporting could support communication and process monitoring activities.

3. Materials and Methods

According to McCormack et al. [59] process maturity is increasingly important. Since the 1980s, maturity models were developed to guide an organization through the process of improving maturity that leads to competitive advantage. A maturity model artefact, developed through the Design Science approach was considered the most suitable for this research. Following from the research objective, the main research question is formulated as follows:

> *"How can organizations incrementally improve their Operational Risk Management processes using Business Performance Management technologies?"*

This research project follows the design science approach and the related design science guidelines as shown in Figure 2 and described by Hevner et al. [25]. Additionally, this research follows the design science processes as described by Hevner [60]. Hevner clarified the design science process as an iterative process of continuously building knowledge base used for developing an artifact to be evaluated and tested for relevance in practice. The process cycles as followed are shown below.

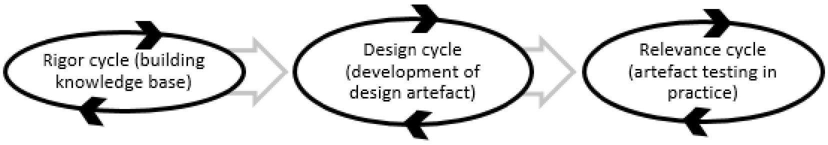
Rigor cycle (building knowledge base)
Design cycle (development of design artefact)
Relevance cycle (artefact testing in practice)

Figure 2. The Design Science cycles, adapted from Hevner [60].

3.1. The Need for a New Maturity Model

Maturity models appear to be strongly influenced by developments in the domains of Information Technology and Quality management. In 1973 Richard Nolan [61] developed the stages of growth model for mature use of computer resources within businesses. This model included six different stages, describing key elements and controls for successfully integrating information technologies within a business organization. In 1979 Crosby [62] developed a quality management maturity grid (QMMG) from a quality management perspective, intended to improve business processes. This grid was focused on improving quality management processes based on five levels of maturity: uncertainty, awakening, enlightenment, wisdom and certainty. Crosby's work was adapted by Watt Humphrey [63] to create the first process maturity framework, aimed at improving software development practices. Watts Humphrey's work laid the foundations for the Capability Maturity Model (CMM). The Capability Maturity Model (CMM) was developed by Paulk et al. [64] from the Carnegie Mellon University Software Engineering Institute (SEI).

Since the introduction of the Capability Maturity Model (CMM) and CMM Integration (CMMI), many different maturity models have been developed. The concepts of maturity models expanded to different industries and specific applications. Notable applications of advanced maturity models have been developed for information security management [65], master data management [66], and datawarehousing [52], among many others. Furthermore, several maturity models for risk management have been proposed. From a technology perspective there are also maturity models on the domains of Business Intelligence and Business Performance Management.

Seven different maturity models related to risk management were examined in more detail:

- Hillson's Risk Maturity Model [67];
- Risk Management Society (*RIMS*) Risk Maturity Model [68];
- BDO's Operational Risk Management Maturity Model [69];
- Assessment Framework for Information Security from the Dutch National Bank [70];
- U.S. Department of Energy's Cybersecurity Capability Maturity Model (*C*2*M*2) [71];
- Deloitte Enterprise Risk Management Maturity [21];
- RSA's Maturity Model for operational risk management [72].

From a technology perspective there are also maturity models on the domains of Business Intelligence and Business Performance Management, the following were studied:

- Wettstein & Kueng's maturity model for performance measurement systems [73];
- AMR Research's Business Intelligence/Performance Management Maturity Model, Version 2 [74];
- Gartner's Business Intelligence & Performance Management Maturity Model [75];
- Aho's (*Logica*) Capability Maturity Model for Corporate Performance Management [76];
- IBM's Big Data & Analytics Maturity Model [77];
- UU's Business Intelligence Development Model [78].

From the maturity models studied, the following became clear:

- Most risk management related maturity models do not include a relationship with software technologies; when they do acknowledge this relation, these models are not detailed and are incomplete about specific requirements suitable;
- Technology related maturity models often appeared to be focused on one silo of ORM, for example only the Information Technology or Information systems part of ORM. Additionally these models do not include a risk management cycle, these models do not support risk management processes sufficiently;
- Only RSA's ORM maturity model appears to focus on both software technologies and risk management, however it is developed commercially and therefore it is vague about specific features. Additionally, the RSA model appears to be very focused on their own product ('*RSAArcher*') rather than supporting generic risk management practices with other solutions.

Next to the theoretical gap in knowledge, this appears to be a problem with practical relevance as well. In practice there appear to be several issues with ORM software. Nyenrode Business University [22] and Sadgrove [44] describe unsatisfied users of current ORM software. Specific issues relate to reporting and insights and (*complicated*) integration with the Plan and Control cycle. Business Performance Management includes tools for measurement, reporting and work flow. BPM is specifically developed towards the improvement of organizational performance to meet its strategic objectives. BPM technologies appears to be a reasonably complete set of software technologies to be suitable specifically for improving operational risk management. No such maturity model exists, while there appears to be a need for a detailed description of suitable technologies related to ORM.

3.2. Maturity Model Development

Since no maturity model appears to exist for improving ORM using BPM technologies, a new maturity model was developed for this purpose: B4ORM. From the exploration of existing maturity models, as described in the previous section, it became clear that a maturity model is composed of a (business) process that needs to be improved and the means (technologies) that need to advance to a more mature process. The following procedure was followed for maturity model development:

1. Process part: ORM detailed from literature and standards
    - Process maturity levels adapted from literature, CMM(I) based;
    - Process structure from literature, COSO ERM and ISO 31000;
2. Technology part: mostly unclear, explored in this research as following:

  - Identification of BPM technologies or features suitable for ORM trough literature study;
  - Market analysis of existing ORM software products for identification of suitable technologies;
  - Expert panel for validation and ranking suitable technologies;

3. Mapping features to ORM processes, based on expert panel ranking;
4. Initial maturity model.

The maturity model as developed in this research is structured with enterprise wide risk management integration in mind. An important part of operational risk management are the processes to manage risk. From literature it appears that operational risk management is often part of enterprise risk management (ERM) and its related risk management processes. Therefore, the process structures for ERM are used for ORM.

Based on the existing maturity models for risk management and their different approaches with a proliferation of terminology, this maturity model uses standard terminology as found in the COSO ERM and ISO 31000 frameworks.

As a starting point for maturity model development, it is presumed important to know what software products already exist and what features are provided for use with operational risk management. Therefore, 65 existing software products were selected on occurrence and relevance. The software products were selected based on their self-promoted or marketed terminology.

On average, a software product for operational risk management is marketed at around five different sectors or industries. Most software for operational risk related practices is marketed for financial services, even though this research also included products for different terminology, such as Health, Safety, Environment and Quality (HSEQ) and specific areas of operational risk management, as used and known in other industries. Enterprise wide risk management practices such as ERM and GRC appear to be well known. ORM is known as a term in financial services and energy and appears also in the most marketed sectors. Interestingly, HSEQ is mentioned by just 18%, while the sectors using the term HSEQ are addressed and marketed by about 30% of ORM software vendors.

The possible options to measure operational risk management regarding process implementation and process maturity were rated by the five experts for suitability. The software features were grouped according to their relating process steps and the experts were asked to determine a ranking of software features according to importance regarding operational risk. For validation of the practical completeness regarding features found during market analysis, each expert was asked to indicate missing software features. All five experts indicated that all of the identified software features were sufficient to support operational risk management processes.

3.3. Expert Panel Driven Development

Table 3 introduces our expert panel of five operational risk management experts whom we consulted using the score voting method. The votes were given anonymously using a voting system that worked with Kahoot, via the participants' mobile/smart phones. On points where no dominant vote was given by the experts, a discussion was held. All experts received all questions and possible answers two weeks before the actual panel session. The scores as given by the experts were mapped to ORM maturity levels and the results of this mapping resulted in a maturity model as shown in the diagram (Figure 3).

Table 3. Expert panel members and their experience with ORM.

Type of Organization	Org. Size in FTE	Experience with ORM
Business Consulting	18	13 years
Business Consulting	18	14 years
Business University	290	10 years
Financial services	3600	3 years
Financial services	390	15 years

3.4. BPM for ORM (B4ORM) Maturity Model

The diagram in Figure 3 visualizes the B4ORM maturity model structure in a matrix. The horizontal axle shows the different maturity levels of the B4ORM maturity model. The vertical axle describes each of the different risk management process stages according to ISO 31000. Each cell of the matrix is filled with a technology requirement, that can be created using BPM technologies.

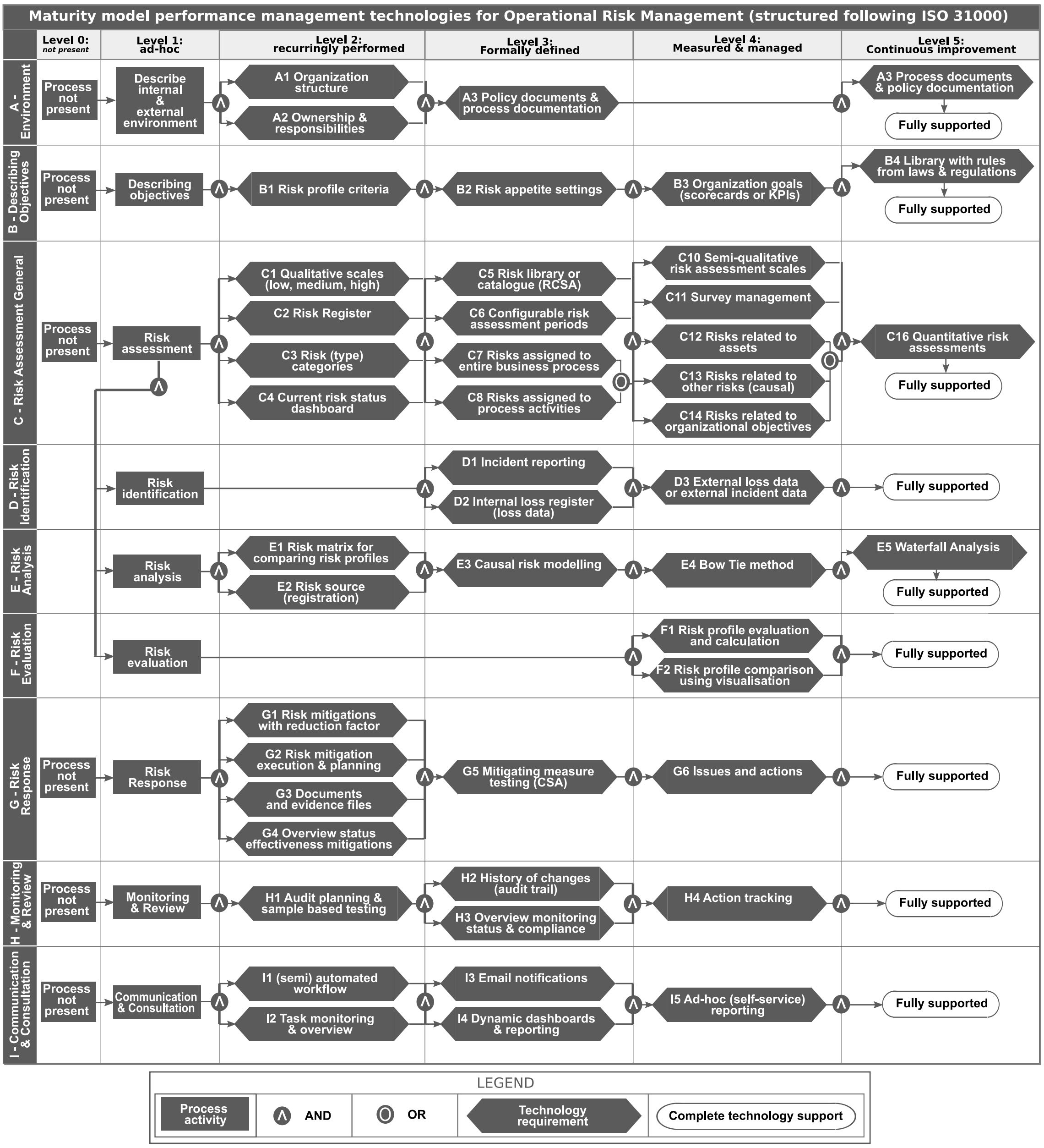
Maturity model performance management technologies for Operational Risk Management (structured following ISO 31000)
Level 0: not present
Level 1: ad-hoc
Level 2: recurringly performed
Level 3: Formally defined
Level 4: Measured & managed
Level 5: Continuous improvement
A - Environment
Process not present
Describe internal & external environment
A1 Organization structure
A2 Ownership & responsibilities
A3 Policy documents & process documentation
A3 Process documents & policy documentation
Fully supported
B - Describing Objectives
Process not present
Describing objectives
B1 Risk profile criteria
B2 Risk appetite settings
B3 Organization goals (scorecards or KPIs)
B4 Library with rules from laws & regulations
Fully supported
C - Risk Assessment General
Process not present
Risk assessment
C1 Qualitative scales (low, medium, high)
C2 Risk Register
C3 Risk (type) categories
C4 Current risk status dashboard
C5 Risk library or catalogue (RCSA)
C6 Configurable risk assessment periods
C7 Risks assigned to entire business process
C8 Risks assigned to process activities
C10 Semi-qualitative risk assessment scales
C11 Survey management
C12 Risks related to assets
C13 Risks related to other risks (causal)
C14 Risks related to organizational objectives
C16 Quantitative risk assessments
Fully supported
D - Risk Identification
Risk identification
D1 Incident reporting
D2 Internal loss register (loss data)
D3 External loss data or external incident data
Fully supported
E - Risk Analysis
Risk analysis
E1 Risk matrix for comparing risk profiles
E2 Risk source (registration)
E3 Causal risk modelling
E4 Bow Tie method
E5 Waterfall Analysis
Fully supported
F - Risk Evaluation
Risk evaluation
F1 Risk profile evaluation and calculation
F2 Risk profile comparison using visualisation
Fully supported
G - Risk Response
Process not present
Risk Response
G1 Risk mitigations with reduction factor
G2 Risk mitigation execution & planning
G3 Documents and evidence files
G4 Overview status effectiveness mitigations
G5 Mitigating measure testing (CSA)
G6 Issues and actions
Fully supported
H - Monitoring & Review
Process not present
Monitoring & Review
H1 Audit planning & sample based testing
H2 History of changes (audit trail)
H3 Overview monitoring status & compliance
H4 Action tracking
Fully supported
I - Communication & Consultation
Process not present
Communication & Consultation
I1 (semi) automated workflow
I2 Task monitoring & overview
I3 Email notifications
I4 Dynamic dashboards & reporting
I5 Ad-hoc (self-service) reporting
Fully supported
LEGEND
Process activity
Λ AND
O OR
Technology requirement
Complete technology support

Figure 3. B4ORM maturity model components and logic visualized.

The input from the expert panel was used to map each technology requirement to a suitable maturity stage. Level 0 (not present) and level 1 (ad-hoc) contain only process activities, since BPM technologies do not benefit these stages. Up from level 2, BPM technologies support improvements in process maturity on a recurring basis and it is formalized towards organization-wide integration.

The B4ORM maturity assessment artifact created in this research [79] was evaluated using a field study to examine the use of practical application regarding the maturity model artifact. The field study was composed of open interview questions for determining contextual information and perceptions that might influence the maturity model application and use. The interviews were transcribed and analyzed through coding and ranking. Additionally, structured assessments were performed using a programmed assessment instrument to instantiate the designed maturity model artifact for evaluation in practice.

4. Results: The Importance of ORM

Table 4 lists the sixteen organizations which provided usable information to answer the research questions. Per participating organization, at least one person was willing to participate in this research. Some organizations provided answers from multiple participants.

Table 4. Organizations participating in maturity model evaluation.

Organization & Industry	Primary Focus
Energy 1	Energy provider
Energy 2	Energy provider
Financial services 1	Insurance services
Financial services 2	Pension services
Financial services 3	Banking services
Financial services 4	Banking services
Financial services 5	Banking services
Financial services 6	Insurance services
Healthcare 1	Patient treatment
Healthcare 2	Patient treatment
Production & trade 1	Organic materials
Retail & consumer goods 1	Groceries
Retail & consumer goods 2	Health & beauty
Transport & Infrastructure 1	Airline services
Transport & Infrastructure 2	Airline services
Transport & Infrastructure 3	Infrastructure provider

The Importance of ORM was measured with the actual implementation of ERM related practices and perceived implementation or maturity level of ORM. The implementation of an enterprise wide approach towards risk management was measured trough the coordination central or de-centralized. A central approach towards risk is recognized by most of the participating organizations. About 88% indicated to have a central department coordinating risk management.

The presence of a Chief Risk Officer (CRO) role at the board level is another indicator of organization wide approach to risk management. Interestingly, 44% of the organizations delegate risk management to their Chief Financial Officer (CFO) compared to 44% appointing a dedicated CRO. In a few cases, even the Chief Executive Officer (CEO) or Chief Operations Officer (COO) was responsible for all risks. The CEO in most organizations (76%) just received reports or received reports and was brought up to speed regarding severe operational risk related incidents. ORM was given an overall importance of 7.6 (SD = 1.8) of 10. This indicates that most organizations find ORM quite important, but not the most important. Most implemented (100%) and most important process of ORM is risk assessment (8.8 of 10), including risk identification, analysis and evaluation.

Most organizations have a relatively small ORM department: 82% of the participating organizations dedicate between 1 and 15 Full Time Equivalent (FTE) to ORM, with some exceptions indicating higher numbers, mainly large international banks. On average, an ORM department is made up of 13 FTE, however a standard deviation of 14 indicates high fluctuations from this average in both ways (positive and negative). Not only the ORM department is involved with operational risks. On average about 5.7 (SD = 2.9) different roles are mentioned to be involved with ORM on a regular basis.

An enterprise wide risk management framework is often also described to structure the organization and its processes regarding risk management. COSO ERM appears to be the most popular by 56% of the participating organizations. While 25% of the participating organizations have no framework at all. The maturity of ORM processes overall was measured using perception of the participants and via calculation of the maturity scores. Most participants scored their current maturity level 3.7 of 5 (SD = 1.1) very similar to their calculated score of 3.4 (SD = 0.99). The initial results of the maturity model were considered to yield an accuracy of 75%, accurately reflecting their current status.

5. Results: Tooling Use for ORM

For most organizations tooling for risk management is just known as software. Although BPM technologies are not equal to all software features, the actual use and availability of all software features are first described to provide context of tooling use. Then the software features are reduced towards the scope of this research and related to BPM technologies.

Most organizations, 14 of 16 (87.5%) indicated they use dedicated software for ORM, while 2 of 16 (12.5%) organizations indicated they rely primarily on self-made excel solutions for risk assessment or reporting. All participating organizations were asked why software is needed for operational risk management. From interview analysis it appears that most, or 11 of 16 (69%) organizations, primarily need the software for efficiency; without the software more people are needed to perform the same tasks.

On average, 37 (55%) distinctive software features are used for operational risk management, from the 68 identified software features in the market analysis. Software features for describing the organizational environment, such as organogram and processes, are most used by all organizations. Qualitative scales for operational risk assessments are used by almost all organizations (88%) in this research. Risk assessment features (incl. the processes of identification, analysis and evaluation) appear to be used by most organizations, however around 12 percent indicate that these features are not actually available in the purchased software and therefore these organizations rely on spreadsheet solutions.

Interview transcript analysis showed that half of the participating organizations, 8 of 16 (50%), indicated the software for ORM leads to a better overview & insights regarding operational risks. Additionally, about one third, or 5 of 16 (31%), of the participating organizations indicated that the integration of all operational risk related data into one integrated tool enables efficient and effective communication and collaboration. Dashboards & Reporting are the most used software features as indicated by 9 of 16 (56%) of the participating organizations. Half of the participating organizations, 8 of 16 (50%), talk about risk assessment. Central storage or a central database, or data warehouse is described by 6 of 16 (38%). Process modelling is described to be used by one third or 5 of 16 (31%). Incident registration is reported to be used by 4 of 16 (25%). Workflow as a component of collaboration is used by 3 of 16 (18%). The use of a file manager for documents and reports is used by 3 of 16 (19%). The least used software features are Action Tracking—2 of 16 (13%)—and Filter & sort features for reports and data sets—2 of 16 (13%). Features that were only mentioned once include a rules engine for fraud detection, control monitoring (measuring mitigation effectiveness) and operational risk workshop support.

5.1. Satisfaction of ORM Software

Only 25% of the organizations indicated that they were fully satisfied with their software for ORM. While 44% indicated that they had small points for improvements. About one third (31%) are not satisfied on their most important points. When considering motivations for satisfaction, it appears most complaints (26%) relate to central integration into a central data repository for operational risks and resulting quality of reporting (18%). Usability in the sense of a user friendly interface is a fairly large (18%) reason for being dissatisfied.

5.2. Use & Availability of BPM Technologies

The previous sections described the use of software as a whole. This section describes the relation with Business Performance Management related technologies. From the 68 identified software features, 63 = 94% are related to Business Performance Management Technologies. Excluded BPM technologies are process modelling functionalities, process documentation and policy documents (used by 69%) via a file system, risk voting (used by 12.5%), process or scenario simulation (used by 12.5%) and rich text editor functionality (used by 6%).

On average. 2% of all used software features cannot be realized using business performance management technologies. Most notable features are process documentation & policy documents (used by 69%) via a file storage manager and process flow modelling (used by 75%). Currently the most used business performance management technologies from interviews are: dashboards & Reporting: 9 of 16 (56%), risk assessment 8 of 16 (50%), central storage or database 6 of 16 (37%), data entry for incident registration 4 of 16 (25%), workflow 5 of 16 (31%). Most of the participating organizations (62%) indicated falling back to using spreadsheet solutions for ORM, organizations utilizing more than 60% Business Performance Management Technologies available do not appear to have this fallback.

During interviews, the participants were asked about their future (5 year) perspective regarding the software for Operational Risk Management. 10 of 16 (63%) expect data integration to become more important. 8 of 16 (50%) describe improvements of dashboards & reporting functionalities. Insights related to risks and mitigating measures by 5 of 6 (31%). 6 of 16 (38%) indicated context aware solutions, adapting to a specific role in the organization (e.g., only information that is relevant for that specific person at a specific time) is an important improvement in the future. Additionally, usability, specifically user friendliness and easy-to-use interfaces, is required by 4 of 16 (25%). Collaboration, process automation & process monitoring functionalities are described by 3 of 16 (19%) of the participants.

5.3. BPM Technologies Related to ORM

The goal of this section is to describe how the maturity levels relate with actually used technologies in order to describe their qualities and suitability for measurement.

The overall average of calculated ORM maturity scores per organization were compared with overall average of BPM technologies regarding use and availability. On average, calculated ORM process maturity has a strong (0.78) Pearson correlation with overall BPM technology use. Note this correlation was performed on a relatively small sample (n = 16). However, such a strong correlation indicates that the level of ORM maturity is related to actual BPM technologies used.

When diving into more detail, the environment, risk identification, risk analysis, risk evaluation and mitigation steps are quite decently correlated with maturity and used technologies. Objective setting and monitoring functionalities appear to be available to organizations with higher maturity scores, but they are far from the most used. Risk assessment in general might be too general, because it does not appear to have any relationship with maturity and technologies. No relationship was found for maturity and technologies to aid communication, but this might be explained by the fact that communication is a human process and does not necessarily rely on technology to be successful.

5.4. Other Factors of Maturity

Since the maturity model context was also recorded for interpretation, these organization characteristics were also compared to maturity as measured with the developed maturity model. Pearson correlations were performed on a small sample (n = 16). Weaker correlations than 0.20 with alpha 0.05 are left out, because such correlations are so weak that considering the sample size they do not indicate anything at all.

Organization size, especially the amount of FTE appears to correlate moderately (0.50 alpha 0.05) with ORM process maturity. Additionally, technology maturity and BPMT use show a weak relationship. A similar relationship is not found when considering the yearly income where only a weak relationship exists with maturity. Being an international organization or not does not appear to indicate a difference for ORM.

The number of laws and regulations for an organization do not appear to influence the actual maturity, however they have a weak relationship (0.27 alpha 0.05) with the technology maturity. A perception of a higher competitive pressure interestingly seems to relate moderate (−0.41 alpha 0.05) negative to the actual use of technology.

When considering the structure of ORM, the presence of a framework for ORM does not appear to be meaningful. The same appears to be the case for a centralized or de-centralized approach towards ERM; these correlations are so weak that they do not really indicate anything. The number of FTE dedicated to ORM appears to have a weak relationship (0.27 alpha 0.05) with ORM maturity.

The appointment of a Chief Risk Officer appears to have a moderate relationship (0.49 alpha 0.05) with technology maturity and BPMT use (0.39 alpha 0.05). Cost of the tooling does not need to increase with more technologies, but the data shows that process maturity increases with higher software costs (0.42 alpha 0.05). There is a reasonably moderate to strong relationship with satisfaction and ORM maturity (0.45 alpha 0.05) and a very strong relation with higher tooling satisfaction when using more BPM technologies (0.88 alpha 0.05). Organizations scoring higher on maturity appear to have less expectations (−0.45 alpha 0.05) about changes in importance of ORM software. Additionally, these organizations use less spreadsheets for ORM (−0.60 alpha 0.05).

5.5. ORM Tooling in Different Sectors

The importance of software for operational risk management varies per industry. Table 5 illustrates that most industries find the use of dedicated software for ORM important or very important; in most cases the analysis from interviews corresponds with the given scores on a scale from 1 (not important) to 10 (very important).

Table 5. Importance of ORM tooling.

Sector	AVG BPM Technology Score	AVG ORM Maturity Score	Perceived Overall Importance
Energy	3.1	4.1	7.5
Financial services	3.7	3.6	7.2
Healthcare	3.2	3.4	8
Retail & consumer goods	2.8	3.6	8.5
Transport & Infrastructures	3.5	4.1	9

Table 6 shows that healthcare appears to be the industry with the highest BPM technology use and availability. ORM was found most important with an average of 9 out of 10 in the transport industry. Airline companies especially consider ORM to be of vital importance for the safety of their passengers. This sector is the only sector using exactly as many technologies as they have available. However, their ORM software appears incomplete, because 66% need solutions in Excel and the satisfaction with ORM software is only 50%. However, this sector achieved the highest ORM maturity scores. On average financial services organizations pay the highest yearly software fees. This is caused by a number of large banks with expensive and very complete ORM software. The BPM technologies used and available are much less by smaller financial services organizations. The retail and consumer industry appears to use more than actually available. This means these organizations rely heavily on non-integrated spreadsheet based solutions for ORM. The average 80k yearly fees in this case are skewed because one retail organization used expensive anti-fraud software. The energy industry appears to be average on almost all aspects. The entire sector indicated needing spreadsheet solutions while none were fully satisfied with their software solution for ORM. Interestingly, they achieved the highest ORM maturity level, but compared to their use of technology they lag the most of all industries.

Table 6. Business Performance Management technologies as used in different sectors.

Sector	BPMT Use	BPMT Availability	Delta	Manual Work in Excel	AVG Yearly Software Fees	AVG Satisfaction
Energy	49%	52%	+3	100%	75k	25%
Financial services	62%	69%	+7	50%	500k	58%
Healthcare	68%	77%	+9	0%	60k	75%
Retail & consumer goods	44%	32%	−12	100%	80k	25%
Transport & infrastructure	65%	65%	0	66%	50k	50%

6. Conclusions and Recommendations

Operational risks are seen as the root cause for many of the (large scale) financial failures in the past decades. Operational Risk is defined by the Basel Committee from the Bank of International Settlements as risks resulting from: Internal Processes, Humans, Systems and External events. In most organizations Operational Risk Management is part of Enterprise Risk Management (ERM). Business Performance Management (BPM) technologies are believed to provide a solution for effective Operational Risk Management by offering several combined technologies including: work flow, data warehousing, (advanced) analytics, reporting and dashboards. The combination of different BPM technologies appeared to match for 94% with requirements for ORM tooling.

Central in this research was the development and practical validation of a new maturity model: B4ORM. The model was developed using the Design Science method as described by Hevner [60]. The maturity model was constructed of a process part, related to operational risk management implementation and the technologies part, relating to BPM technologies used. The initial results of the maturity model were considered to yield an accuracy of 75% by the participating organizations. On average, calculated ORM process maturity has a strong (0.78) Pearson correlation with overall BPM technology use.

Operational Risk Management was first placed into context by measuring the importance of the organizational process, before measuring the actual implementation level of ORM and the use of BPM technologies. The importance of ORM—as scored by the participants—resulted in an overall score of 7.6 on a scale from 1 (not important) to 10 (very important). In conclusion, most organizations consider operational risks fairly important. ORM is most often (50%) used to prevent damage and other adverse effects, more than for learning, improvement or awareness (13%). Business Performance Management Technologies can be seen as a subset of software related technologies. Therefore, the measured software technologies were first analyzed and then scoped back to BPM technologies. Most organizations 87.5%) indicated using dedicated tooling for ORM, while 12.5% organizations indicated relying primarily on self-made Excel solutions for risk assessment or reporting. The importance of tooling for operational risk management varies by industry. Healthcare, Transport & Infrastructure and the Financial Services industries utilize most BPM technologies. Of these, the industries using more than 60% BPM technologies appear to be most satisfied with their software solutions for ORM. These same industries also have less need to fall back on using spreadsheet software.

From this research we can conclude that there are some clear relations with specific sets of BPM technologies found to influence the maturity of Operational Risk Management. Therefore, the maturity model as developed in this research could provide some useful guidelines on the applicability of certain technologies. The maturity model as developed in this research provides a suitable path with six stages for organizations seeking to improve their ORM processes. The six stages provide an instrument to match appropriate technologies to the current stage of maturity and enables organizations to grow in maturity towards enterprise integration and continuous improvement.

As this research provides some answers to unanswered questions, all research leads to new research possibilities. Therefore, this section provides some future research directions. As this research explored a novel domain in a qualitative manner, larger samples are needed for further validation of the maturity model. Additionally, there appears to be a difference between industries but the samples for each industry are too shallow for real conclusions.

ORM tooling in general is required for efficiency and structure. Only when using ORM tooling it will be possible to reach organization-wide integration. Especially BPM technologies support organization wide integration and collaboration via workflow. Some participants suggested that maintainability of tooling for ORM is an issue. This suggestion could be related to dissatisfaction, complaints about user-friendliness and mismatch between tooling and ORM as described in this research.

7. Discussion

There are some relations found with specific sets of BPM technologies to influence the maturity of Operational Risk Management. Therefore, the maturity model as developed in this research could provide some useful guidelines on the applicability of certain technologies, especially for non-mature industries. The maturity model as developed in this research provides a suitable path with six stages for organizations seeking to improve their ORM processes. The six stages provide an instrument to match appropriate technologies to the current stage of maturity and enables organizations to grow in maturity towards enterprise integration and continuous improvement.

This research provides substantial new insights into the actual use and availability of BPM technologies in different industries. These insights can be used for further empirical research projects and the results provide a kind of ranking about the feasibility or existence of the phenomena reported in this paper.

Considering the general research design it is important to note that the selection criteria were in part not based on indisputable and objective information, but also on qualitative interpretation. Although this is rather common and not necessarily problematic for this type of explorative and qualitative research, the results might be different when applying these criteria.

Only Dutch organizations participated in this research. Our findings might, therefore, differ somewhat in other countries. The financial services industry is mostly harmonized in Europe by the EU regulations, but especially other sectors might uncover severe differences among countries due to different laws, regulations and culture.

During the B4ORM maturity model development, the market analysis was limited to 65 products. However, we did not validate our sample for completeness and representativeness with respect to the entire ORM software market. As a matter of fact, the ORM software market size is currently unknown. Nevertheless, the results in this research are validated using an expert panel. The expert panel served the purpose of validation and ranking of identified software features.

The size of the expert panel was limited. Experts were mainly involved in financial services. Furthermore, five experts were considered sufficient, however eight or more experts would have been better [80]. During the expert panel, the range voting method was used. Although this method allowed for sufficient answers, this is not a Delphi method with full anonymity (e.g., [81]). There is no guarantee that the expert panel was unbiased regarding their answers. However, a Delphi expert panel would have consumed too much time [82,83]. Some bias was prevented via an anonymous voting system and a discussion afterwards.

An evident limitation of this research is its sample size. This situation puts limits on considering any generalizations. Therefore, at this moment no real generalizations can be made yet. As such, there is still room for further refining the reliability and validity of the scales of the maturity model. According to Hoyle [84], with respect to a relatively modest data sample as gathered and reported on in this research, a Pearson correlation coefficient does not have to pose problems for qualitative research (because you do not test a hypothesis), when being aware of the fact that small samples are less reliable and never reach a significance level lower than .05. In conclusion, the results in this research should not be seen as clear-cut evidence, but as providing clear directions for further empirical research.

Acknowledgments: The authors want to thank Celcus B. V. in Soesterberg, the Netherlands, for facilitating this research by providing access to the broad customer network, and are grateful to the editors and anonymous reviewers for providing valuable comments.

Author Contributions: B.P.W. made substantial contributions to the study design, acquisition of data, analysis and interpretation of data, and has been leading in drafting the manuscript. M.S. supervised the research, and made substantial contributions to the study design, interpretation of data, maturity model design, and has reviewed the manuscript critically for important intellectual content and co-authored the paper. All authors read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

ORM	Operational Risk Management
DSS	Decision Support System
EIS	Executive Information System
DW	Data Warehouse
BI	Business Intelligence
BPM	Business Performance Management
CPM	Corporate Performance Management
EPM	Enterprise Performance Management
BPMT	Business Performance Management Technologies
ERM	Enterprise Risk Management
SEM	Strategic Enterprise Management
QMMG	Quality Management Maturity Grid
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
GRC	Governance, Risk and Compliance
HSEQ	Health, Safety, Environment and Quality
CRO	Chief Risk Officer
CFO	Chief Financial Officer
CEO	Chief Executive Officer
COO	Chief Operating Officer
FTE	Full Time Equivalent
COSO	Committee of Sponsoring Organizations of the Treadway Commission
OCEG	Open Compliance and Ethics Group
ISO	International Organization for Standardization
AS/NZS	Standards Australia and Standards New Zealand

References

1. Hoffman, D.G. *Managing Operational Risk: 20 Firmwide Best Practice Strategies*; John Wiley & Sons: Hoboken, NJ, USA, 2002.
2. Alexander, C. *Operational Risk: Regulation, Analysis and Management*; Pearson Education: London, UK, 2003.
3. Power, M. The invention of operational risk. *Rev. Int. Political Econ.* **2005**, *12*, 577–599.
4. Moosa, I.A. Operational risk: A survey. *Financ. Mark. Inst. Instrum.* **2007**, *16*, 167–200.
5. Chernobai, A.S.; Rachev, S.T.; Fabozzi, F.J. *Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis*; John Wiley & Sons: Hoboken, NJ, USA, 2008.
6. Breden, D. Managing Operational Risk in a Continuously Changing Environment (Bank of Finland). Available online: http://www.webcitation.org/6tjvVI1pV (accessed on 25 September 2017).
7. Tarantino, A. *Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices*; John Wiley & Sons: Hoboken, NJ, USA, 2008.

8. Malik, S.A.; Holt, B. Factors that affect the adoption of Enterprise Risk Management (ERM). *OR Insight* **2013**, *26*, 253–269.
9. Fontnouvelle, P.; DeJesus-Rueff, V.; Jordan, J.; Rosengren, E. *Using Loss Data to Quantify Operational Risk*; Federal Reserve Bank of Boston: Boston, MA, USA.
10. Panjer, H.H. *Operational Risk: Modeling Analytics*; John Wiley & Sons: Hoboken, NJ, USA, 2006.
11. Kenett, R.S.; Raanan, Y. *Operational Risk Management: A Practical Approach to Intelligent Data Analysis*; John Wiley & Sons: Hoboken, NJ, USA, 2011.
12. Kavakr, F.; Spiegel, A.D. Risk management in health care institutions A strategic approach. *J. Healthc. Qual.* **2004**, *26*, 56–58.
13. Moseley, G.B., III. *Managing Legal Compliance in the Health Care Industry*; Jones and Bartlett Publishers: Burlington, MA, USA, 2013.
14. Marques, R.C.; Berg, S. Risks, contracts, and private-sector participation in infrastructure. *J. Constr. Eng. Manag.* **2011**, *137*, 925–932.
15. Cruz, C.O.; Marques, R.C. Risk-sharing in seaport terminal concessions. *Transp. Rev.* **2012**, *32*, 455–471.
16. Coca, D.; de Blas, R.; Gallejones, C.; Moral, R.; Calvo, J.; Álvarez, J.; del Canto, Á. Operational Risk Management in the Energy Industry, 2014. Available online: http://www.webcitation.org/6xA33zgEB (accessed on 11 February 2018).
17. Mitra, S.; Karathanasopoulos, A.; Sermpinis, G.; Dunis, C.; Hood, J. Operational risk: Emerging markets, sectors and measurement. *Eur. J. Oper. Res.* **2015**, *24*, 122–132.
18. Lam, J. *Enterprise Risk Management: From Incentives to Controls*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
19. Arnold, V.; Benford, T.; Canada, J.; Sutton, S.G. Leveraging integrated information systems to enhance strategic flexibility and performance: The enabling role of enterprise risk management. *Int. J. Account. Inf. Syst.* **2015**, *19*, 1–16.
20. Operational Issues of Risk Management (PwC). Available online: http://www.webcitation.org/6xA3V6UXv (accessed on 11 February 2018).
21. Enterprise Risk Management A 'Risk-Intelligent' Approach (Deloitte). Available online: http://www.webcitation.org/6tqFniCol (accessed on 29 September 2017).
22. Tweede Nationaal Onderzoek Risicomanagement in Nederland (Nyenrode Business University). Available online: http://www.webcitation.org/6u4NMANUK (accessed on 8 October 2017).
23. Beasley, M.; Chen, A.; Nunez, K.; Wright, L. Working hand in hand: Balanced scorecards and enterprise risk management. *Strateg. Financ.* **2006**, *87*, 49–55.
24. Azvine, B.; Cui, Z.; Majeed, B.; Spott, M. Operational risk management with real-time business intelligence. *BT Technol. J.* **2007**, *25*, 154–167.
25. Hevner, A.; March, S.T.; Park, J.; Ram, S. Design science in information systems research. *MIS Q.* **2004**, *28*, 75–105.
26. Fraser, J.; Simkins, B.; Narvaez, K. *Implementing Enterprise Risk Management: Case Studies and Best Practices*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
27. Miller, K.D. A framework for integrated risk management in international business. *J. Int. Bus. Stud.* **1992**, *23*, 311–331.
28. Meulbroek, L.K. A senior manager's guide to integrated risk management. *J. Appl. Corp. Financ.* **2002**, *14*, 56–70.
29. Rosenberg, J.V.; Schuermann, T. A general approach to integrated risk management with skewed, fat-tailed risks. *J. Financ. Econ.* **2006**, *79*, 569–614.
30. Simkins, B.; Ramirez, S.A. Enterprise-wide risk management and corporate governance. *Loyola Univ. Chic. Law J.* **2007**, *39*, 571.
31. Culp, C.L. The revolution in corporate risk management: A decade of innovations in process and products. *J. Appl. Corp. Financ.* **2002**, *14*, 8–26.
32. Olson, D.L.; Wu, D.D. *Enterprise Risk Management*; World Scientific Publishing Co., Inc.: Singapore, 2015.
33. Gordon, L.A.; Loeb, M.P.; Tseng, C.Y. Enterprise risk management and firm performance: A contingency perspective. *J. Account. Public Policy* **2009**, *28*, 301–327.
34. GRC Defined (OCEG). Available online: http://www.webcitation.org/6u4EFWKFn (accessed on 29 September 2017).

35. Racz, N.; Weippl, E.; Seufert, A. A frame of reference for research of integrated GRC. In *Communications and Multimedia Security*; Springer: Berlin, Germany, 2010; pp. 106–117.
36. Racz, N.; Weippl, E.; Seufert, A. Governance, risk & compliance (GRC) software-an exploratory study of software vendor and market research perspectives. In Proceedings of the 44th Hawaii International Conference of System Sciences (HICSS), Honolulu, HI, USA, 4–7 January 2011; pp. 1–10.
37. Enterprise Risk Management—Integrated Framework (COSO). Available online: http://www.webcitation.org/6tq28Hzzq (accessed on 29 September 2017).
38. Power, M. The risk management of nothing. *Account. Organ. Soc.* **2009**, *34*, 849–855.
39. The 2015 GRC Maturity Survey Report (OCEG). Available online: http://www.webcitation.org/6tq1Wnl8r (accessed on 29 September 2017).
40. Nissen, V.; Marekfia, W. Towards a research agenda for strategic governance, risk and compliance (GRC) management. In Proceedings of the Conference Business Informatics (CBI), Vienna, Austria, 15–18 July 2013; pp. 1–6.
41. Operational Risk (Bank of International Settlements). Available online: http://www.webcitation.org/6tjuXt27o (accessed on 25 September 2017).
42. Sound Practices for the Management and Supervision of Operational Risk (Bank of International Settlements). Available online: http://www.webcitation.org/6tjugPqoB (accessed on 25 September 2017).
43. Tattam, D. *A Short Guide to Operational Risk*; Gower Publishing: Farnham, UK, 2011.
44. Sadgrove, K. *The Complete Guide to Business Risk Management*; Routledge: Abingdon-on-Thames, UK, 2016.
45. Fraser, J.; Simkins, B.J. *Enterprise Risk Management*; John Wiley & Sons: Hoboken, NJ, USA, 2008; pp. 19–29.
46. Taxonomy-Based Risk Identification (Carnegie-Mellon University). Available online: http://www.webcitation.org/6tjvlXoXf (accessed on 25 September 2017).
47. Purdy, G. ISO 31000: 2009—Setting a new standard for risk management. *Risk Anal.* **2010**, *30*, 881–886.
48. ISO 31000 Risk management—Principles and Guidelines. Available online: http://www.webcitation.org/6u4GJyZ7w (accessed on 8 October 2017).
49. Lebas, M. Performance measurement and performance management. *Int. J. Prod. Econ.* **1995**, *41*, doi:10.1016/0925-5273(95)00081-X.
50. Simons, R. *Performance Measurement and Control Systems for Implementing Strategy*; Prentice Hall: Upper Saddle River, NJ, USA, 2002.
51. Frolick, M.N.; Ariyachandra, T.R. Business performance management: One truth. *IS Manag.* **2006**, *23*, 41–44.
52. Spruit, M.; Sacu, C. DWCMM: The Data Warehouse Capability Maturity Model. *J. Univ. Comput. Sci.* **2015**, *21*, 1508–1534.
53. Sharda, R.; Delen, D.; Turban, E. *Business Intelligence A Managerial Perspective on Analytics*; Pearson Education Limited: London, UK, 2014.
54. Melchert, F.; Winter, R.; Klesse, M. Aligning process automation and business intelligence to support corporate performance management. In Proceedings of the Tenth Americas Conference on Information Systems, New York, NY, USA, 6–8 August 2004; pp. 4053–4063.
55. Samsonowa, T. *Industrial Research Performance Management: Key Performance Indicators in the ICT Industry*; Springer: Berlin, Germany, 2011.
56. Wasmann, M.; Spruit, M. Performance Management within Social Network Sites: The Social Network Intelligence Process Method. *Int. J. Bus. Intell. Res.* **2012**, *3*, 49–63.
57. Spruit, M.; Jagesar, R. Power to the People! Meta-algorithmic modelling in applied data science. In Proceedings of the 8th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, Porto, Portugal, 11–13 November 2016; pp. 400–406.
58. Lytras, M.; Raghavan, V.; Damiani, E. Big data and data analytics research: From metaphors to value space for collective wisdom in human decision making and smart machines. *Int. J. Sem. Web Inf. Sys.* **2017**, *13*, 1–10.
59. McCormack, K.; Willems, J.; Van den Bergh, J.; Deschoolmeester, D.; Willaert, P.; Štemberger, M.; Vlahovic, N. A global investigation of key turning points in business process maturity. *Bus. Process Manag. J.* **2009**, *15*, 792–815.
60. Hevner, A.R. A three cycle view of design science research. *Scand. J. Inf. Syst.* **2007**, *11*, 87–92.
61. Nolan, R.L. Managing the computer resource: A stage hypothesis. *Commun. ACM* **1973**, *16*, 399–405.

62. Fraser, P.; Moultrie, J.; Gregory, M. The use of maturity models/grids as a tool in assessing product development capability. In Proceedings of the Engineering Management Conference, Cambridge, UK, 18–20 August 2002; pp. 244–249.
63. Humphrey, W.S. Characterizing the software process: A maturity framework. *IEEE Softw.* **1988**, *5*, 73–79.
64. Paulk, M.C.; Curtis, B.; Chrissis, M.B.; Weber, C.V. Capability maturity model, version 1.1. *IEEE Softw.* **1993**, *10*, 18–27.
65. Spruit, M.; Roeling, M. ISFAM: The Information Security Focus Area Maturity model. In Proceedings of the 22nd European Conference on Information Systems, Tel Aviv, Israel, 9–14 June 2014.
66. Spruit, M.; Pietzka, K. MD3M: The Master Data Management Maturity Model. *Comput. Hum. Behav.* **2015**, *51*, 1068–1076.
67. Hillson, D.A. Towards a risk maturity model. *Int. J. Proj. Bus. Risk Manag.* **1997**, *1*, 35–45.
68. RIMS Risk Maturity Model (RMM) for Enterprise Risk Management. Available online: http://www.webcitation.org/6u4JnW9Vu (accessed on 8 October 2017).
69. BDO Operational Risk Management Maturity Model. Available online: http://www.webcitation.org/6tjv044RV (accessed on 25 September 2017).
70. Assessment Framework for Information Security. Available online: http://www.webcitation.org/6tqGVV1fF (accessed on 29 September 2017).
71. Cybersecurity Capability Maturity Model (C2M2). Available online: http://www.webcitation.org/6u4KJW1Pf (accessed on 8 October 2017).
72. Maturity Model for Operational Risk Management. Available online: http://www.webcitation.org/6u4KS5LSa (accessed on 8 October 2017).
73. Wettstein, T.; Kueng, P. A maturity model for performance measurement systems. *WIT Trans. Inf. Commun. Technol.* **2002**, *26*, 113–122.
74. AMR's Business Intelligence/Performance Management Maturity Model. Available online: http://www.webcitation.org/6tjsca0P4 (accessed on 25 September 2017).
75. Maturity Model for Business Intelligence and Performance Management. Available online: http://www.webcitation.org/6u4L6tRsm (accessed on 8 October 2017).
76. Aho's Capability Maturity Model for Corporate Performance Management. Available online: http://www.webcitation.org/6tjsFaUHz (accessed on 25 September 2017).
77. Big Data & Analytics Maturity Model. Available online: http://www.webcitation.org/6u4LXWzsH (accessed on 8 October 2017).
78. Sacu, C.; Spruit, M. BIDM: The Business Intelligence development model. In Proceedings of the 12th International Conference on Enterprise Information Systems, Funchal, Madeira, Portugal, 8–12 June 2010; pp. 288–293.
79. Pieket Weeserik, B.; Spruit, M. B4ORM assessment instrument. Available online: http://bit.ly/b4orm-assessment (accessed on 27 February 2018).
80. Ashton, R.H. Combining the judgment of experts: How many and which ones? *Organ. Behav. Hum. Decis. Process.* **1986**, *38*, 405–414.
81. Baars, T.; Spruit, M. Designing a Secure Cloud Architecture: The SeCA Model. *Int. J. Inf. Secur. Priv.* **2012**, *6*, 14–32.
82. Linstone, H.A.; Turoff, M. *The Delphi Method. Techniques and Applications*; Addison-Wesley: Reading, MA, USA, 2002.
83. Hsu, C.C.; Sandford, B.A. The Delphi technique: Making sense of consensus. *Pract. Assess. Res. Eval.* **2007**, *12*, 1–8.
84. Hoyle, R.H. *Statistical Strategies for Small Sample Research*; Sage: Newcastle upon Tyne, UK, 1999.