Abstract
The management of risk in business processes has been the subject of active research in the past few years. Many benefits can potentially be obtained by integrating the two traditionally separated fields of risk management and business process management, including the ability to minimize risks in business processes by design, and to mitigate such risks at run time. While there has been an increasing amount of research aimed at delivering such an integrated system, these research efforts vary in terms of their scope, goals, and functionality. Through the systematic collection and evaluation of relevant literature, this paper compares and classifies current approaches in the area of risk-aware business process management in order to expose and explain current research gaps. The process through which relevant literature was collected, filtered, and evaluated is also detailed. Finally, a research agenda is proposed.

Keywords: risk-aware; business process management; risk management; survey
I. INTRODUCTION

Recent surveys have shown that many organizations have deployed business process management (BPM) systems to manage their businesses [Dixon, 2011] [Dixon and Jones, 2011] [Vollmer, Leganza, Pilecki and Smillie, 2008] [Gengler, 2008]. This is not surprising given the demonstrable benefits offered by BPM, such as cost reduction and in overall process quality improvement [Searle, 2011]. These benefits are achieved by taking the concept of process as the starting point for understanding and streamlining business activities [van der Aalst, Adams, ter Hofstede and Russell, 2010].

Unfortunately, traditional BPM systems do not address the problem of uncertainties that organizations face in their day-to-day operations, such as IT infrastructure malfunctions or share market movements, which may have a profound impact on organizational objectives. These uncertainties and their impact on organizations are commonly known as risks, and they need to be managed through the application of relevant principles, frameworks and processes. The application of this set of principles, frameworks and processes is commonly known as risk management [Standards Australia and Standards New Zealand, 2009].

A number of recent financial scandals such as the $2.3B UBS rogue trading scandal in 2011 [Howley and Thomasson, 2011] and the €4.9B fraud at Société Générale in 2008 [Clark and Jolly, 2008], highlight the disconnected nature between risk management practices and their corresponding business processes [Horwood and Lee, 2011]. In particular, the UBS example shows how the exploitation of the inherently risky exchange-traded fund (ETF) confirmation process by the rogue trader [Lee, 2011] [Silver, 2011], could go on for years without being appropriately addressed [Trenor, Bowers and Jones, 2011]. Such incidents highlight the need to bring risk management practices closer to the business process management domain.

Not surprisingly, the management of risk in business processes has been a subject of active research in the past few years, e.g. [Rosemann and zur Muehlen, 2005] [Ho and zur Muehlen, 2009] [Tjoa, Jakoubi, Goluch, Kitzler, Goluch et al., 2011]. The importance of this research has also been confirmed in a number of studies [Rikhardsson, Best, Green and Rosemann, 2006] [Becker, Breuker, Weiß and Winkelmann, 2010].

We call a system which allows the reasoning about and management of risks in business processes a risk-aware business process management (R-BPM) system. Many benefits can potentially be obtained by integrating the two traditionally separated fields of risk management and BPM, including the ability to analyse risks and incorporate risk mitigation strategies into a business process model during design time [Goluch, Ekelhart, Fenz, Jakoubi, Tjoa et al., 2008], to monitor the emergence of risks and apply risk mitigation actions during run time [Conforti, Fortino, La Rosa and ter Hofstede, 2011], as well as to identify risks from logs and other post-execution artifacts [Jans, van der Werf, Lybaert and Vanhoof, 2011]. Furthermore, an integrated R-BPM system may also aid businesses to comply with various legislations and regulations, such as the Sarbanes-Oxley Act [107th Congress - USA, 2002] and Basel II [Basel, 2006].

In the past few years, an increasing amount of research aimed at achieving R-BPM has been proposed. However, the contributions from this research vary in terms of scope, goals and functionality. This is expected given the wide-range of forms in which risk can manifest itself in business processes (e.g. regulatory non-compliance, financial fraud, natural disasters, data leakage), the proliferation of underlying business process modeling approaches and automation tools with differing degrees of formalization [van der Aalst, Adams, ter Hofstede and Russell, 2010], and the various levels at which risk management can be incorporated into the realm of business process management. To date, there has not been a systematic study investigating the state-of-the-art in this area.

The main contribution of this paper is an identification of research gaps in the area of R-BPM and the proposal of a research agenda. According to Cooper’s taxonomy, our literature review focuses on the research outcomes of relevant academic literature, with the goal of identifying the central issues of the research in this field that “should dominate future endeavors” [Cooper, 1988, p. 109]. In other words, we summarize those research topics which have been well-studied (if any), and those which have not received much attention but still need to be properly studied.

Through a systematic collection of literature, we identified 96 papers deemed relevant, out of a pool of over 20,000 papers. Research gaps in the area of R-BPM were then identified through a methodical comparison of the functionality and the maturity of the contributions, based on a set of common evaluation criteria which we developed and illustrate in this paper.

This paper is organized as follows. Section II provides a brief explanation of the concept of BPM and how it relates to R-BPM. Section III describes the related literature published in the area of R-BPM. Section IV describes the scope of our literature review. Section V describes our collection methods in selecting relevant literature to be evaluated in this paper. Section VI illustrates our literature analysis approach, including the theoretical foundation upon which our
evaluation framework is constructed. Section VII presents and evaluates the relevant literature using the evaluation framework detailed in Section VI. In Section VIII, a gap analysis of the current state of research in the area of R-BPM is performed, which forms the basis for a proposed research agenda. Finally, conclusions are provided in Section IX.

II. BACKGROUND

BPM supports businesses by providing a set of tools, methods and techniques to identify and discover business processes, to analyze these processes in order to find opportunities for improvement, to enact the improved processes and monitor and control their execution [Dumas, Rosa, Mendling and Reijers, 2013]. A business process typically involves different organizational aspects, ranging from human resources, to business documents and technology. The use of BPM has been widely adopted in today’s organizations [Dixon, 2011] [Dixon and Jones, 2011] [Vollmer, Leganza, Pilecki and Smillie, 2008] [Gengler, 2008].

An organization using BPM strategies typically goes through a number of stages, known as the BPM lifecycle. While there are several models of BPM lifecycles [van der Aalst, Adams, ter Hofstede and Russell, 2010] [Dumas, van der Aalst and ter Hofstede, 2005] [Dumas, Rosa, Mendling and Reijers, 2013], they generally consist of the following stages: design, design-time analysis, execution, run-time analysis, and post-execution analysis. During the design stage, business requirements are identified and business processes which fulfill these requirements are identified, delimited, and related to each other. These business processes are typically organized hierarchically in a process architecture. Next, the identified business processes are documented by means of business process models, according to the requirements identified in the previous stage. These “as-is” process models contain activities and events describing the sequence in which these activities and events are to be executed, along with the human participants, documents, technology and other organizational resources involved. The as-is process models capture a snapshot of the current way in which business processes are conducted in an organization. Thus, these processes may not necessarily be optimized. In the subsequent stage, that is, the design-time analysis stage, the as-is business processes are analyzed to identify opportunities for improvement, such as costs and time reduction, and elimination of waste. The analysis results can then be incorporated into the as-is models to fix the identified issues, resulting in a set of “to-be” process models. Next, in execution stage, the to-be process models are enacted accordingly. The execution of activities captured in the models can be performed manually and/or automatically, via the use of BPM systems. A BPM system can be used to automate (to varying degrees) the management and execution of business processes as defined in the models. Typical functions of such systems are resource allocation, task scheduling, and business data and rules management. The execution of business processes is then monitored and analyzed, in real-time, during the run-time analysis stage to ensure that problems that have not been considered during design-time can be handled accordingly. Furthermore, logs and other data generated from the execution of the business processes can also be analyzed off-line during the post-execution analysis stage to gain insights into how the processes have actually been carried out. Insights gained from the post-execution analysis stage can of course be used as a feedback to the design stage again to enable further process improvement. Note that the run-time analysis and post-execution analysis stages are also commonly known as the monitoring and controlling stage.

Unfortunately, traditional BPM systems operate separately from the domain of risk management [Conforti, Fortino, La Rosa and ter Hofstede, 2011], resulting in the occurrence of undesirable events, as explained in Section I. It is logical, and desirable, for business processes to be aware of the risks they face and to directly manage these risks as an integral part of their process execution, rather than as separate activities or as an after-thought. For example, as shown in Figure 1, an ideal R-BPM should be able to identify and analyze process-related risks explicitly during design time, as well as to design the necessary risk mitigation strategies. During run time, the emergence of risks should be constantly monitored and, once occurred, should be mitigated immediately to ensure a proper termination of the process. The logs produced from the execution of business processes should also be analyzed to identify the occurrences of risks in the executed processes, as well as to understand the reasons behind their occurrences.

Nevertheless, the capabilities just described are still being developed by the research community and they still require further study. This article compares current research approaches in this area and identifies the corresponding research gaps. We define an approach as a specific contribution to research in the area of R-BPM (e.g., a methodology to identify and communicate risks in process models). When two or more approaches are deemed to be similar (i.e., when it is clear that latter approaches are indeed an evolution of one or more earlier approaches typically proposed by similar authors), they are grouped together. A collection of similar approaches is also called an approach. In the reminder of this paper, the term approach should thus be interpreted as a collection of similar approaches based on the criteria explained above.
III. RELATED WORK

To our knowledge, there has only been a limited literature review of research in the area of R-BPM. For example, in Jakoubi et al.’s work, nine scientific approaches, all of which attempt to integrate risk and/or security aspects into business process management, were evaluated [Jakoubi, Tjoa, Goluch and Quirchmayr, 2009]. Rikhardsson et al. conducted a literature review and interviews with industry-based risk managers to establish the research gaps in the area of risk management, compliance, and internal control [Rikhardsson, Best, Green and Rosemann, 2006].

While the literature reviews just mentioned are closely related to ours, the scope differs. Jakoubi et al. considered research papers which focus on both the issue of ‘security in BPM’ and the issue of ‘risk in BPM’ [Jakoubi, Tjoa, Goluch and Quirchmayr, 2009]. Similarly, the scope of Rikhardsson et al.’s literature review is also broader as it includes research papers in the area of compliance and internal control, as well as risk management [Rikhardsson, Best, Green and Rosemann, 2006]. In our case, however, we focus only on papers which explicitly try to reason about ‘risk in BPM’. Carnaghan looked into the extent to which existing business process model constructs support audit risk assessment [Carnaghan, 2006]. Our literature review, on the other hand, is concerned with novel approaches to integrate the concept of risk into BPM. Consequently, Carnaghan’s evaluation framework is also different from the one we developed.

Although there is only a limited number of literature reviews in the area of R-BPM, research in this area encompasses a broad-range of (sometimes overlapping) research topics. The precise scope of our literature review is detailed in the following section.

IV. SCOPE OF LITERATURE REVIEW

To ensure that our literature review remains within a manageable scope, we have established a set of criteria to guide the selection of papers to be evaluated. As a consequence, a number of related papers have been excluded. A brief explanation of the selection criteria and the resulting list of papers excluded from our literature review are
detailed in the remainder of this section. For those papers that did meet our selection criteria, they were then grouped into a set of ‘approaches’ and evaluated using the standard evaluation framework detailed in Section VI.

As a general rule, we only consider those papers which specifically attempt to integrate and/or reason about risks in business process management systems. Therefore, those papers which focus only on risk management aspects and do not demonstrate any strong links with business process management/workflow systems are excluded. Examples of risk-management-focused work which we excluded are the CORAS method [M.S. Lund and Stolen, 2011], the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management framework [COSO, 2004], and Cheng and Iida et al.’s work [Cheng, Sadiq and Indulska, 2011] [Iida, Denker and Talcott, 2009].

Similarly, those papers which interpret business processes in a very generic sense without any notion of activities or relationships between activities are excluded. Examples of papers in this category include Mansour and Murthy’s and Salmela’s [Mansour and Murthy, 2007] [Salmela, 2007].

We also excluded those papers whose main focus is on the topic of business process-based risk management [Sackmann, 2008] [Cha, Liu and Yu, 2009] [Taubenberger and Jürjens, 2008] [Yu, 2011]. While these papers may seem relevant, they are more concerned with the issue of risk management than with business process management — business processes are merely used as tools to facilitate the process of risk management. In other words, these papers have a different set of goals to those which our literature review considers.

Papers that are relevant but are written in languages other than English are also excluded in our literature review as they are unlikely to be accessible to all international community due to language barriers [Brabänder and Ochs, 2002] [Hengsmith, 2005] [Rieke and Winkelmann, 2008] [Rieke, 2009].

The need for organizations to comply with legislative regulations has highlighted the need to address risks of regulatory non-compliance. Consequently, research in business process compliance has been increasingly linked to risk management. However, business process compliance is distinct from risk-aware business process management: the former seeks to provide solutions to ensure the compliance of business processes to regulations, while the latter seeks to reason about the likelihood of business processes violating some regulations and the consequences of those violations. Our literature is concerned with the latter, and we have thus excluded many papers in the area of business process compliance which do not demonstrate any strong links to the concept of risk [Namiri and Stojanovic, 2007] [Orriëns, van den Heuvel and Papazoglou, 2009] [Sadiq, Governatori and Namiri, 2007] [Goedertier and Vanthienen, 2006] [Lu, Sadiq and Governatori, 2007] [Ly, Rinderle-Ma and Dadam, 2010] [Awad, Decker and Weske, 2008] [Lohmann, 2011] [Gerke, Cardoso and Claus, 2009] [Ghanavati, Amyot and Peyton, 2007] [Governatori, Hoffmann, Sadiq and Weber, 2009].

Similarly, information security is another risk factor in a BPM system. In this respect, our literature review focuses on those papers which attempt to facilitate the reasoning about security risks in business process management systems, rather than those which attempt to provide solutions to security management problems. Thus a large number of papers concerning security management were excluded [Rodriguez, Fernandez-Medina and Piattini, 2007] [Rodriguez, Fernandez-Medina and Piattini, 2006b] [Rodriguez, Fernandez-Medina and Piattini, 2006a] [Wolter and Schaad, 2007] [Wainer, Kumar and Barthelmess, 2007] [Neubauer and Heurix, 2008] [Neubauer, Klemen and Biffl, 2005] [Neubauer, Klemen and Biffl, 2006] [Neubauer and Pehn, 2010] [Wang and Li, 2007] [Xiangpeng, Cerone and Krishnan, 2006] [Rodriguez, Garcia-Rodriguez de Guzmán, Fernandez-Medina and Piattini, 2010] [Montagut and Molva, 2007] [Ayed, Cuppens-Boulahia and Cuppens, 2009] [Aziz, Arenas, Martinelli, Matteucci and Mori, 2008].

We have also excluded zur Muehlen and Ho’s paper [zur Muehlen and Ho, 2005]: while this paper may, at first, seem relevant, it actually discusses issues related to risk management in a BPM project (that is, the various risks that can happen at each stage of a BPM project lifecycle). It is a project risk management paper and is thus excluded.

Finally, we do not consider papers of a preliminary nature [Fugini, Damiani and Reed, 2007] [Kriksciuniene and Strigunaite, 2010] [Weist and Deokar, 2008] [Xie, Liu and Chen, 2007] [Ruffolo, Curia and Gallucci, 2005] [Loehndorf, Petzel and Portmannss, 2007] [Rausch, 2006] [Wahler, 2005] [Cernauskas and Tarantino, 2009]. While such papers may be relevant, the work reported therein is not sufficiently detailed and/or advanced to allow for a proper evaluation.
V. LITERATURE COLLECTION METHODS

Informed by the importance of documenting our literature collection process [vom Brocke, Simons, Niehaves, Niehaves, Reimer et al., 2009], this section details our literature collection methods. Due to resource constraints, a truly exhaustive literature collection process across a plethora of academic forums was not possible. Thus, we classify the coverage of our literature review to be ‘representative’ (according to Cooper’s taxonomy [Cooper, 1988]): we do not claim that our literature review covers all work that has been published in this area; rather, our literature review covers a representative sample of the work in this area.

Relevant literature was collected in two stages between March 2011 and September 2011. In the first stage, two literature collection methods were undertaken to select potentially relevant papers. This was achieved by investigating relevant academic forums and by using well-known scholarly-article search engines (e.g. Google Scholar, Scopus, and Web of Science). To maximize the inclusiveness of our search, at this stage, any papers which were somewhat related to the issue of risks in BPM (such as process-related risk management in BPM, security issues in BPM, and regulatory compliance management) were selected. In the second stage, we narrowed down the papers to be evaluated by eliminating those papers which fell outside the scope of our literature review (detailed in Section IV). To broaden our search, during our review process, we also undertook a ‘backward reference search’ process whereby we took note of any relevant papers referenced by the papers being reviewed and added these referenced papers to our collection of papers to evaluate. The details of our literature collection methods are provided in the remainder of this section.

First Stage

Academic Forums

A set of well-known academic forums (conferences and journals) were systematically searched to select papers related to the topic of risk in business process management from year 2005 until September 2011. Given the cross-disciplinary nature of R-BPM, research papers were collected from a wide-range of disciplines, including information systems, business process management, risk management, and information security.

Forums were chosen based on their field of research (FoR) classification [Australian Bureau of Statistics, 2008] and their indicative quality as determined by the Australian Research Council (ARC). The main FoR codes considered include 0806 (information systems), 0803 (computer software), and 0804 (data format). However, selecting forums solely based on FoR codes resulted in an unmanageable number of journals and conferences to investigate. Therefore, we filtered forums by selecting only those of reasonable quality as demonstrated by their classification as A*, A, or B forums according to the ARC’s journal classification2, that is the forums recognized as publishing quality research by relevant research communities. The list of forums from which relevant papers were collected is available in Appendix A.

From each identified forum, relevant papers were selected by checking their titles to see if they were somewhat related to the topic of ‘risk in business process management’. For each paper whose title seemed relevant, the abstract was then read and a quick scan of the paper was performed to confirm the paper’s relevance. If these checks passed, we then included the paper into our literature list. Those papers whose title clearly indicated their irrelevance were eliminated. This process allowed us to select 151 potentially-relevant papers out of a pool of more than 20,700 papers.

Scholarly-article Databases

We complemented our forum-based literature collection method with a keyword-based search using popular scholarly-article databases, including Google Scholar, Scopus, and Web of Science. These databases were selected because they are well-known sources of citations.3 For each database, we conducted two search iterations (except for Google Scholar where three iterations were performed) using the following search criteria:

- keywords: “process” “risk” (all of the words) in the article title (first iteration),
- keywords: “workflow” “risk” (all of the words) in the article title (second iteration),
- keywords: “operational risk” “process model” (Google Scholar only).

---

2 www.arc.gov.au/xls/era2010_jurnal_title_list.xls
3 Of course, we could have used other scholarly databases, such as Proquest or EBSCO to produce a (possibly) more complete literature review. However, to keep our literature review manageable, we had to limit our search to only the three databases mentioned above (Google Scholar, Scopus, and Web of Science).
Further engine-specific filtering rules were applied:

- **Google Scholar:**
  - searches were performed within 1-year intervals (2005 to 2006, then 2006 to 2007, and so on until the last interval of 2010 to 2011) to ensure that all results were included (at the time the searches were conducted, Google Scholar only displayed the first 1000 results), and
  - we restricted our search to the following subject fields: “Engineering, Computer Science, Mathematics” and “Business, Administration, Finance, Economics”.

- **Scopus:**
  - searches were conducted for papers published between the year of 2005 to 2011, and

- **Web of Science:**
  - searches were conducted for papers published between the year of 2005 to 2011, and

Using these search engines, we obtained a total of 1,960 hits, of which 135 were selected based on the relevance of their titles and abstracts. Of those, 17 were papers that had already been selected during the forum-based search.

**Second Stage**

Through the first stage of literature collection, we collected 269 papers. This was still too large a number of papers to review. Therefore, we further reduced the scope of our literature review to only consider those papers which explicitly try to reason about risks within the context of BPM. The criteria used to exclude papers from our literature review are explained in Section IV. Finally, during our review process, we also took note of any relevant papers referenced by the papers being reviewed, and added these referenced papers to our collection of papers to review (about 11 papers).

At the end, we had 96 papers that we considered to be worthy of thorough evaluation. We then applied the evaluation framework described in the following section to those papers. After the framework had been applied, a further 33 papers were deemed to be outside the scope for final evaluation, leaving a final 60 papers for thorough review and evaluation (see Section VII).

**VI. LITERATURE EVALUATION FRAMEWORK**

In this paper, we assume a **neutral representation** perspective in the process of literature evaluation [Cooper, 1988]. We do so by assessing each paper based on the common evaluation framework detailed in this section. Where appropriate, the theoretical basis that underpins this framework is also explained.

Our evaluation framework is mainly influenced by the design-science research paradigm [Hevner, March, Park and Ram, 2004] because the type of research conducted in the area of R-BPM can be seen as a form of design-science research. Design science “...creates and evaluates IT artifacts intended to solve identified organizational problems” [Hevner, March, Park and Ram, 2004, p. 77]. In our case, the ‘organizational problem’ of the integration of risk management with business processes is addressed by the research community through the proposal of various IT artifacts, such as constructs, models, methods, and instantiations [March and Smith, 1995].

The focus of this literature review is on the outcomes or artifacts of research in the area of R-BPM. We assess these research outcomes or artifacts from two perspectives: the BPM lifecycle perspective and the maturity perspective. Furthermore, given that R-BPM attempts to integrate risk management principles into BPM, it is only natural that we also assess to what extent the risk management domain informs the approaches of R-BPM.
**Process Lifecycle Evaluation**

Given that the central theme of this paper is how risk can be reasoned about within a BPM system, it is natural that we are interested in assessing the BPM lifecycle stages to which a particular research artifact can be applied. To this end, five distinct BPM lifecycle stages (as described in Section II) are used in our evaluation framework. These five stages are the design stage, the design-time analysis stage, the execution stage, the runtime analysis stage, and the post-execution analysis stage. These five stages are inspired by van der Aalst et al.'s BPM lifecycle [van der Aalst, Adams, ter Hofstede and Russell, 2010]: the first two stages of our BPM lifecycle correspond to the process (re-)design phase of their model, the third and fourth stages correspond to the process enactment and monitoring phase, and finally, the fifth stage of our BPM lifecycle corresponds to the diagnosis stage. Based on these five stages, we define the following evaluation criteria. For evaluation purpose, each criterion can be assigned an evaluation ‘score’ of full support (+), partial support (±), or no support (−). For the detailed explanation as to what these ratings mean with respect to each evaluation criterion, please refer to Appendix B.

**Design**

Does the approach propose modelling constructs (such as graphical notations) that can be used to communicate risk information in business process models, and/or principles/guidelines that can be used to minimize business process' risks by design?

**Design-time Analysis**

Does the approach provide technique(s) to analyze/evaluate business process’ risks during design time?

**Execution**

Can the risk-related extensions of a process model be executed and somehow exploited to monitor risk or to influence execution behavior of processes at runtime?

**Runtime Analysis**

Does the approach propose one or more technique(s) to analyze/evaluate business process risks during runtime?

**Post-execution Analysis**

Does the approach propose techniques to analyze/evaluate risks of a business process (after its execution) based on the logs and other process-related information collected during the execution of the process?

**Maturity Evaluation**

The development of the evaluation criteria to assess the maturity of an artifact is underpinned by Hevner et al.'s design science research guidance [Hevner, March, Park and Ram, 2004]. These criteria (and how design science guidelines underpin these criteria) are detailed below. Similar to the process lifecycle evaluation, each criterion can be assigned an evaluation ‘score’ of full support (+), partial support (±), or no support (−). Furthermore, where appropriate, the evaluation score of ‘N/A’ can also be assigned if a particular criterion is not applicable to the approach being evaluated (see Appendix B for the detailed explanation).

**Integrated Risk Formalization**

Does the approach propose novel constructs to capture risk-related information such that we can reason about risk together (in an integrated manner) during design-time, runtime, and/or post-execution? If so, were the proposed risk constructs developed through a rigorous process? This evaluation criterion is informed by two research design guidelines: design as an artifact and research rigor [Hevner, March, Park and Ram, 2004]. The former states that design science research produces artefacts in various forms, including constructs. Using this guideline, we therefore assess if an approach proposes risk-related constructs that can be used to enhance existing process models such that integrated reasoning of risks within a process model can be achieved. The second guideline states that design science requires the “…application of rigorous methods in both the construction and evaluation of the designed artifact.” [Hevner, March, Park and Ram, 2004, p. 87]. As detailed below, we assess the rigorousness of an approach by the extent to which the risk constructs proposed are formalized in terms of their abstract syntax, concrete syntax, and semantics.

- **Abstract Syntax:** does the approach specify the key ‘components’ or the ‘deep structure’ of the proposed risk constructs using appropriate formal description technique(s)? The abstract syntax of a construct can be expressed in the form of a conceptual model (such as UML [OMG, 2011a] [OMG, 2011b]) or a grammar

---

4 This term is borrowed from Meyer [Meyer, 1990].
(such as the Metanot grammar [Meyer, 1990]). For example, the abstract syntax of a construct representing a risk event can be expressed as a UML class diagram capturing the attributes that the proposed construct should possess (such as the name of the event and the severity of the event).

- Concrete Syntax: does the approach specify the forms in which the proposed risk constructs can be represented? While abstract syntax is concerned with the ‘deep structure’ of a construct, concrete syntax is concerned with the external representation of the construct. For example, the concrete syntax of a construct representing a risk event can be expressed as an exclamation mark inside a rectangle with the name of the event written below the exclamation mark and the severity of the event captured by the fill-color of the rectangle.

- Semantics: does the approach specify the operations (and the effects of those operations) that can be applied to the proposed constructs using appropriate formal techniques? In other words, does the approach go as far as defining the operations that can be executed on the proposed constructs and the effects of those operations on a process model? For example, given the existence of a risk event notation associated with a particular activity (which is also followed by an OR-split control) in a process model, the semantics of the risk event construct can be defined in terms of how it determines the choice of the subsequent path(s) to execute based on the value of the severity attribute of the construct. Typically, the semantics of a construct can be expressed by using well-known formal techniques, such as Coloured Petri Nets [Jensen and Kristensen, 2009] or Pi-calculus [Milner, 1999]. It has been argued that the use of natural language may be sufficient to provide a clear and unambiguous definition of the semantics of some constructs. While it may be true, to ensure a consistent and objective evaluation, this paper classifies the use of natural language for semantics/syntax definition as informal.

It should be noted that the BPM lifecycle criteria are used to indicate the BPM lifecycle stage(s) addressed by a particular approach. The ‘integrated risk formalization’ criterion is, on the other hand, used to indicate not only the maturity of the proposed constructs (in terms of the clarity and unambiguity of the specifications of the constructs), but also the process lifecycle stages to which the constructs can be applied:

- if an approach receives a non-applicable (N/A) evaluation for the ‘integrated risk formalization’ criterion, then it means that the approach does not propose any new risk constructs to support the BPM lifecycle stage(s) addressed by the approach (instead, other techniques, such as Bayesian network analysis, are used to analyze and reason about risks in business processes);

- however, if an approach receives an evaluation result of no support (−), partial support (+), or full support (++) for any one of the ‘integrated risk formalization’ sub-criteria (abstract syntax, concrete syntax, and/or semantics), then it means that the BPM lifecycle stage(s) addressed by the approach are somewhat supported by the use of new risk constructs.

To clarify, if an approach receives an N/A evaluation, it means that the approach does not even attempt to propose any new integrated risk constructs; however, if an approach receives a no support (−) evaluation, it means that the approach proposes some integrated risk constructs, but they are not formalized.

Implementation
Has the proposed approach been implemented? This evaluation criterion is informed by the design as an artifact guideline [Hevner, March, Park and Ram, 2004]. In particular, we are interested if there is an instantiation artifact of the approach.

Application Method
Does the approach provide any method through which it can be applied in practice? This evaluation criterion is informed by the design as an artifact guideline [Hevner, March, Park and Ram, 2004] and the artifact we are interested in this evaluation criterion is of type method.

Application in Practice
Has the proposed approach been applied and validated in practice? This evaluation criterion is informed by the design evaluation guideline [Hevner, March, Park and Ram, 2004, p. 85]. This guideline states that the “...utility, quality, and efficacy of a design artifact must be rigorously demonstrated...”. An obvious way to demonstrate the utility, quality, and efficacy of an approach is by applying it in practice. By doing so, we can evaluate the extent to which a proposed approach can be used to solve real-world problems.
Influence of Risk Management Domain

The final evaluation criteria attempt to evaluate the extent to which techniques and standards from the traditional risk-management domain have influenced the R-BPM approach being evaluated. Given the comparatively mature risk analysis techniques from the risk management domain (such as the Bayesian network analysis [Heckerman, 1995] and Monte Carlo simulation [Metropolis, 1987]), it may be beneficial to apply them to reason about or analyze risks in an R-BPM system. Similarly, an R-BPM system may also benefit from the application of best-practices and guidelines from existing risk management standards, both domain-independent (such as the AS/NZS ISO 31000:2009 standard [Standards Australia and Standards New Zealand, 2009]) and domain-specific ones (such as the Sarbanes-Oxley standard [107th Congress - USA, 2002]).

Therefore, in order to evaluate the extent to which the risk management domain has influenced R-BPM approaches, we developed four evaluation criteria. The last two evaluation criteria can be assigned an evaluation ‘score’ of full support (+), partial support (±), or no support (−) (see Appendix B for the detailed explanation).

**Risk Type**
Which type(s) of risk (based on Rosemann and zur Muehlen’s risk taxonomy [Rosemann and zur Muehlen, 2005]) does the approach address?

**Domain**
To which risk domain(s) is the approach applicable (for example, the finance domain or the procurement domain)?

**Risk Analysis Technique**
Which risk analysis technique(s), if any, have been applied by the approaches evaluated in this paper?

**Risk Standards**
By which risk standards (such as the Sarbanes-Oxley and Basel II standards), if any, have R-BPM approaches been influenced? Given that one of the drivers for research in the area of R-BPM is the need to comply with various risk-related regulations/standards, it is interesting to evaluate the extent to which R-BPM approaches have actually incorporated those standards.

**VII. LITERATURE EVALUATION**

As described in Section V, at the end of our literature collection process, there were 96 papers which were deemed to be suited for evaluation. However, through a detailed evaluation process, 33 out of those 96 papers were deemed to be borderline papers which were outside the scope of our literature review (as detailed in Section IV). Therefore, we have excluded them. Furthermore, 3 out of those 96 papers were actually ‘related work’ papers already discussed in Section III. The remaining 60 papers were then further grouped into 27 distinct approaches. These 27 distinct approaches were thoroughly reviewed using the evaluation framework discussed in Section VI.

The evaluation of these approaches was conducted iteratively. Preliminary evaluation results were obtained towards the end of November 2011 (after about two months of evaluation process). Throughout the writing up process, new issues related to the preliminary evaluation results (such as evaluation inconsistencies) were also identified and resolved. Towards the end of March 2012, the first complete draft of this paper was produced. This draft was then circulated to the main authors of all of the 27 approaches considered in this paper to give them the opportunity to challenge our evaluation results. The authors of three approaches were unreachable. By mid-April 2012, the authors of seven approaches responded and their feedback has been incorporated into this paper to the extent possible.

In particular, five authors representing five approaches agreed with our evaluation of their work, while authors of two approaches disputed the evaluation. The author of one of the disputed approaches challenged our definition of semantics in the evaluation framework, arguing that ‘formal’ semantics cannot capture the complexity of the concept of ‘risks’. This dispute has resulted in a more elaborate explanation of the semantics evaluation criterion in Section VI. The authors of the other disputed approach disagreed with the no-support (−) evaluation we gave in relation to the semantics evaluation criterion. They stated that the relatively simple risk constructs proposed in their approach make the use of natural language sufficient for the purpose of semantics definition. We have addressed this challenge by adding a clarifying remark, where appropriate, in the description of each approach (in Appendices C, D, E, and F).
<table>
<thead>
<tr>
<th>Authors</th>
<th>Approach Code</th>
<th>Reference(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jans et al.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kang et al.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Singh et al.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conforti et al.</td>
<td>RT01</td>
<td>[Conforti, Fortino, La Rosa and ter Hofstede, 2011]</td>
</tr>
<tr>
<td>Kang et al.</td>
<td>RT02</td>
<td>[Kang, Cho and Kang, 2009]</td>
</tr>
<tr>
<td>Jans et al.</td>
<td>PE01</td>
<td>[Jans, van der Werf, Lybaert and Vanhoof, 2011], [Jans, Lybaert, Vanhoof and van der Werf, 2008], [Jans, Depaire and Vanhoof, 2011]</td>
</tr>
<tr>
<td>Wickboldt et al.</td>
<td>PE02</td>
<td>[Wickboldt, Bianchin, Lunardi, Granville, Gaspar et al., 2011]</td>
</tr>
<tr>
<td>Cope et al.</td>
<td>DI03</td>
<td>[Cope, Kuster, Etzweiler, Deleris and Ray, 2010], [Cope, Küster and Etzweiler, 2009], [Cope, Deleris, Etzweiler, Koehler, Kuester et al., 2010]</td>
</tr>
<tr>
<td>Weiβ and Winkelmann</td>
<td>DI04</td>
<td>[Weiβ and Winkelmann, 2011]</td>
</tr>
<tr>
<td>Asnar and Giorgini</td>
<td>DI05</td>
<td>[Asnar and Giorgini, 2008]</td>
</tr>
<tr>
<td>Mock and Corvo</td>
<td>DI06</td>
<td>[Mock and Corvo, 2005]</td>
</tr>
<tr>
<td>Rosemann and zur Muehlen</td>
<td>DI07</td>
<td>[Rosemann and zur Muehlen, 2005]</td>
</tr>
<tr>
<td>Rotaru et al.</td>
<td>DI08</td>
<td>[Rotaru, Wilkin, Churilov and Neiger, 2008], [Neiger, Churilov, zur Muehlen and Rosemann, 2006], [Rotaru, Wilkin, Churilov, Neiger and Ceglowski, 2009]</td>
</tr>
<tr>
<td>Betz et al.</td>
<td>DI09</td>
<td>[Betz, Hickl and Oberweis, 2011]</td>
</tr>
<tr>
<td>Herrmann and Herrmann</td>
<td>DI10</td>
<td>[Herrmann and Herrmann, 2006]</td>
</tr>
<tr>
<td>Strecker et al.</td>
<td>DI11</td>
<td>[Strecker, Heise and Frank, 2011]</td>
</tr>
<tr>
<td>Karagiannis et al.</td>
<td>DI12</td>
<td>[Karagiannis, Mylopoulos and Schwab, 2007]</td>
</tr>
<tr>
<td>Taylor et al.</td>
<td>DI13</td>
<td>[Taylor, Godino and Majeed, 2008]</td>
</tr>
<tr>
<td>Panayiotou et al.</td>
<td>DI14</td>
<td>[Panayiotou, Oikonomitsios, Athanasiadou and Gayialis, 2010]</td>
</tr>
<tr>
<td>Lambert et al.</td>
<td>DI15</td>
<td>[Lambert, Jennings and Joshi, 2006]</td>
</tr>
<tr>
<td>Bhuiyan et al.</td>
<td>DN01</td>
<td>[Islam, Bhuiyan, Krishna and Ghose, 2009], [Bhuiyan, Islam, Koliadis, Krishna and Ghose, 2007]</td>
</tr>
<tr>
<td>Fenz et al.</td>
<td>DN02</td>
<td>[Fenz and Neubauer, 2009], [Fenz, Ekelhart and Neubauer, 2009], [Fenz and Ekelhart, 2009], [Fenz, 2010]</td>
</tr>
<tr>
<td>Muehlen et al.</td>
<td>DN03</td>
<td>[zur Muehlen, Baumgart and Junkers, 2006]</td>
</tr>
<tr>
<td>Kaegi et al.</td>
<td>DN04</td>
<td>[Kaegi, Mock, Ziegler and Nibali, 2006]</td>
</tr>
<tr>
<td>Bergholtz et al.</td>
<td>DN05</td>
<td>[Andersson, Bergholtz, Edirisuriya, Ilayperuma and Johansson, 2005], [Bergholtz, Grégoire, Johansson, Schmitt, Wohed et al., 2005], [Schmitt, Grégoire and Dubois, 2005]</td>
</tr>
<tr>
<td>Jallow et al.</td>
<td>DN06</td>
<td>[Jallow, Majeed, Vergidis, Tiwari and Roy, 2007]</td>
</tr>
<tr>
<td>Singh et al.</td>
<td>DN07</td>
<td>[Singh, Gelgi, Davulcu, Yau and Mukhopadhyay, 2008]</td>
</tr>
<tr>
<td>Conforti et al.</td>
<td>RT01</td>
<td>[Conforti, Fortino, La Rosa and ter Hofstede, 2011]</td>
</tr>
<tr>
<td>Jallow et al.</td>
<td>DN06</td>
<td>[Jallow, Majeed, Vergidis, Tiwari and Roy, 2007]</td>
</tr>
<tr>
<td>Singh et al.</td>
<td>DN07</td>
<td>[Singh, Gelgi, Davulcu, Yau and Mukhopadhyay, 2008]</td>
</tr>
<tr>
<td>Conforti et al.</td>
<td>RT01</td>
<td>[Conforti, Fortino, La Rosa and ter Hofstede, 2011]</td>
</tr>
<tr>
<td>Kang et al.</td>
<td>RT02</td>
<td>[Kang, Cho and Kang, 2009]</td>
</tr>
<tr>
<td>Jans et al.</td>
<td>PE01</td>
<td>[Jans, van der Werf, Lybaert and Vanhoof, 2011], [Jans, Lybaert, Vanhoof and van der Werf, 2008], [Jans, Depaire and Vanhoof, 2011]</td>
</tr>
<tr>
<td>Wickboldt et al.</td>
<td>PE02</td>
<td>[Wickboldt, Bianchin, Lunardi, Granville, Gaspar et al., 2011]</td>
</tr>
</tbody>
</table>
The list of these 27 approaches is shown in Table 1. Roughly speaking, we can categorize these approaches into three groups based on the main BPM lifecycle stage addressed: (1) design-time, including design-time analysis, (2) runtime, including runtime analysis, and (3) post-execution. The approach code column shown in Table 1 indicates the group to which each of the 27 approaches belongs: those approaches with an ‘approach code’ starting with the letter ‘D’ belong to the first group, those with ‘RT’ belong to the second group, and those with ‘PE’ belong to the third group. To aid our evaluation, Table 2 is also provided to summarize the types of risk-related activities that each of the 27 approaches supports at each stage of the BPM Lifecycle stages.

### Table 2: Risk Management Activities Supported by Each Evaluated Approach

<table>
<thead>
<tr>
<th>Risk Identification</th>
<th>Design-time Analysis</th>
<th>Execution</th>
<th>Runtime Analysis</th>
<th>Post-execution Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Identification</strong></td>
<td><strong>Risk Discovery Techniques</strong></td>
<td>DI02</td>
<td>DI03, DI06, DI09, DI10, DI11, DI12, DI14, DN03</td>
<td>PE01, PE02</td>
</tr>
<tr>
<td><strong>Annotation Techniques</strong></td>
<td>DI01, DI02, DI03, DI04, DI05, DI06, DI07, DI08, DI09, DI10, DI11, DI12, DI13, DI14, DI15, DI16, RT01</td>
<td>DI08, DN03</td>
<td>RT01</td>
<td>PE02</td>
</tr>
<tr>
<td><strong>Risk Analysis</strong></td>
<td><strong>Probability Analysis</strong></td>
<td>DI16, DN02</td>
<td>RT01, RT02</td>
<td>PE01, PE02</td>
</tr>
<tr>
<td><strong>Impact Analysis</strong></td>
<td>DN01</td>
<td>DI01, DI16, DN01, DN02, DN06</td>
<td>PE02</td>
<td></td>
</tr>
<tr>
<td><strong>Risk Propagation</strong></td>
<td>DI06, DI16, DN02</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk Evaluation</strong></td>
<td>DI02, DN07</td>
<td>DI05, DI10, DI11, DI12, DI13, DI14, DI16, DN02, DN04, DN07</td>
<td>PE02</td>
<td></td>
</tr>
<tr>
<td><strong>Risk Treatment</strong></td>
<td>DI02, DI10, DI12, DN05</td>
<td>DI01, DI05, DI08, DI09, DI10, DI16, DN07</td>
<td>DN07</td>
<td></td>
</tr>
</tbody>
</table>

The evaluation of these 27 approaches is summarized in the remainder of this section. Please refer to Appendices C, D, E, and F for a detailed description and evaluation of each approach.

**Design-time R-BPM**

There is a significant amount of research attempting to address the issue of risk in business processes at design-time. We divide papers in this category into two groups: those which attempt to reason about risks through the introduction of new integrated risk constructs to capture risk-related information within a business process model, and those which attempt to reason about risks through the use of existing risk analysis methods without the introduction of any new constructs.

**Design-time R-BPM with Integrated Risk Constructs**

Tables 3 and 4 summarize the evaluation results of those approaches which introduce risk constructs to communicate and reason about risks during design-time. In these tables, each approach is identified by its respective ‘approach code’ in accordance with Table 1. There are in total sixteen approaches in this category. All of the approaches in this category provide support during the design stage of a BPM lifecycle, and most of them also provide some form of design-time analysis capability.
Overall, the approaches in this category mainly focus on defining the \textit{concrete syntax} of the proposed risk constructs. For example, the Risk-Oriented Process Evaluation (ROPE) approach proposed by Jakoubi et al. (D101) introduces a set of graphical notations to represent risk elements (such as threats, resources, counter measures, and recovery actions) that can be attached to any business process activities. On the other hand, the approaches proposed by Sienou et al (D102), Mock and Corvo (D106), Rosemann and zur Muehlen (D107), and Rotaru et al. (D108) introduce new graphical notations to represent risk elements by extending the Event-driven Process Chain (EPC) language. In fact, all approaches in this category, with the exception of the approaches proposed by Bai et al. (D116), propose some \textit{concrete syntax} to capture risk-related constructs.

On the other hand, the number of approaches that attempt to formalize the deep-structure (or the \textit{abstract syntax}) of the risk-related constructs proposed is fewer. Among those approaches, Sienou et al. (D102), Cope et al. (D103), Betz et al. (D109), and Strecker et al. (D111) use UML to define the \textit{abstract syntax} of their constructs, while in the approaches proposed by Weiβ and Winkelmann (D104) and Rotaru et al. (D108), Entity Relationship (ER) diagrams are used.

The biggest gap, however, is in the formalization of the \textit{semantics} of the constructs: only one approach (i.e. Rotaru et al. – D108) attempts to formalize the semantics of the risk constructs proposed. However, even so, the formalization of the risk constructs only goes as far as defining the rules or constraints with respect to the notion of a risk-aware process mode (but not the \textit{execution} semantics of the constructs). Furthermore, only around a third of all approaches in this category have some form of implementation and application in practice. For example, Weiβ and Winkelmann (D104) and Mock and Corvo (D106) have applied their approaches to major banks in Germany, while the approach proposed by Karagiannis et al. (D112) has been adopted by an insurance company in the United States. Finally, only about a quarter of all approaches in this category that apply some existing risk analysis techniques. For example, Mock and Corvo (D106) apply the Failure Mode and Effects Analysis (FMEA) technique in their approach, while Bai et al. (D116) apply the Conditional Value-at-Risk technique. The majority of approaches are not guided by any existing risk standards, except for the work by Karagiannis et al. (D12) (which is informed by the SOX Act [107th Congress - USA, 2002]), the work by Weiβ and Winkelmann (D104) (which is informed by the Basel II standard [Basel, 2006]), as well as the work by Sienou et al. (D102) (which is informed by the Generalised Enterprise Reference Architecture and Methodology (GERAM) framework [IFIP-IFAC Task Force on Architectures for Enterprise Integration, 1999]). Most of the approaches in this category are generic enough to be applicable to any domain, although a few of them have been developed for specific domains. For a detailed review and evaluation of all approaches in this category, please refer to Appendix C.

<table>
<thead>
<tr>
<th>Approach</th>
<th>DI01</th>
<th>DI02</th>
<th>DI03</th>
<th>DI04</th>
<th>DI05</th>
<th>DI06</th>
<th>DI07</th>
<th>DI08</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Generic</td>
<td>Finance</td>
<td>Generic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Type</td>
<td>IT</td>
<td>Generic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing Risk Analysis</td>
<td>–</td>
<td>–</td>
<td>±</td>
<td>–</td>
<td>+</td>
<td>+</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Risk Standard</td>
<td>–</td>
<td>±</td>
<td>–</td>
<td>+</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Maturity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated Risk Formalization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abstract Syntax</td>
<td>–</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>+</td>
</tr>
<tr>
<td>Concrete Syntax</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Semantics</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>±</td>
</tr>
<tr>
<td>Implementation</td>
<td>±</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>±</td>
</tr>
<tr>
<td>Application Methodology</td>
<td>±</td>
<td>+</td>
<td>+</td>
<td>±</td>
<td>–</td>
<td>+</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Application in Practice</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>+</td>
<td>±</td>
<td>+</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>BPM Lifecycle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design-time Analysis</td>
<td>±</td>
<td>–</td>
<td>±</td>
<td>–</td>
<td>+</td>
<td>±</td>
<td>–</td>
<td>±</td>
</tr>
<tr>
<td>Execution</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Runtime Analysis</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Post-execution Analysis</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>
Table 4: Evaluation – Design Stage with Integrated Risk Constructs (2/2)

<table>
<thead>
<tr>
<th>Approach</th>
<th>DI09</th>
<th>DI10</th>
<th>DI11</th>
<th>DI12</th>
<th>DI13</th>
<th>DI14</th>
<th>DI15</th>
<th>DI16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Generic</td>
<td>FInance</td>
<td>Generic</td>
<td>Supply Chain</td>
<td>Generic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Type</td>
<td>Generic</td>
<td>Data</td>
<td>IT</td>
<td>Structural</td>
<td>Generic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing Risk Analysis</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Risk Standard</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Maturity</td>
<td>Integrated Risk</td>
<td>Abstract Syntax</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Formalization</td>
<td>Concrete Syntax</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>±</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Semantics</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>±</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Implementation</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>(+)(1)</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Application Methodology</td>
<td>+</td>
<td>-</td>
<td>±</td>
<td>±</td>
<td>+</td>
<td>±</td>
<td>-</td>
<td>±</td>
</tr>
<tr>
<td>Application in Practice</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>±</td>
<td>+</td>
</tr>
<tr>
<td>BPM Lifecycle</td>
<td>Design</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>±</td>
<td>±</td>
<td>±</td>
</tr>
<tr>
<td></td>
<td>Design-time Analysis</td>
<td>±</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>±</td>
<td>±</td>
<td>±</td>
</tr>
<tr>
<td></td>
<td>Execution</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Runtime Analysis</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Post-execution Analysis</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Note:
(1) Implemented in the sense that it exploits an existing ADONIS environment.

Design-time R-BPM Without Integrated Risk Constructs

Table 5 summarizes the evaluation results of those papers which address design-time R-BPM without introducing integrated risk constructs. There are a total of 7 approaches in this category.

The majority of the approaches in this category focus on providing support for *design-time analysis* (in terms of various risk analysis activities). The extent to which this has been accomplished by existing approaches leaves room for improvement, as most approaches only provide partial support for design-time risk analysis capability. For example, Bhuiyan et al. (DN01) and Jallow et al. (DN06) propose techniques to estimate the consequences of the occurrence of risk events to business processes; however, no techniques are proposed with regards to how to estimate the probability of the occurrence of the risk events. Therefore, the *design-time risk analysis* capability provided is partial as risk is a function of both the probability of the occurrence of risk events, and the impact of those events on processes.

An exception to this trend is the work by Fenz et al. (DN02) whereby a comprehensive set of risk analysis techniques (considering both probability and impact), informed by well-established technical foundations (such as Petri nets and Bayesian network analysis), is proposed.

The approaches in this category provide very minimal support for the *design-time* activities, partly due to the fact that they do not attempt to introduce new risk-related constructs to aid users in designing a risk-aware business process model. Even so, most approaches do not provide principles or guidance to support risk-*informed* business process models. An exception to this is the work by Bergholtz et al. (DN05) whereby an approach that considers risk events (and their treatments) in the design of a process model is proposed. The work by Bhuiyan et al. (DN01) suggests that the resource criticality analysis that they proposed could be used to enable a risk-*informed* business process design; however, there is a lack of details in terms of how the results of resource criticality analysis should precisely be used to guide the design of a process model.

Only a handful of approaches in this category have been implemented or applied in practice. For example, the work by zur Muehlen et al. has been applied to a payroll process in a university, while the work by Bhuiyan et al. and Fenz et al. have been empirically validated in a workshop setting. With a few exceptions, most approaches are not
influenced by any existing risk analysis techniques or standards. Examples of the mentioned exceptions include the work by Fenz et al. (DN02) (which is influenced by the NIST 800-30 recommendations regarding risk management for IT systems) and the work by zur Muehlen et al. (DN03) (which is influenced by the risk analysis technique called Failure Modes, Effects, and Criticality Analysis [US Department of Defense, 1949]). Most of these approaches have been developed to be generic enough to be applied in any domain. Please refer to Appendix D for a detailed analysis of the approaches in this category.

<table>
<thead>
<tr>
<th>Approach</th>
<th>DN01</th>
<th>DN02</th>
<th>DN03</th>
<th>DN04</th>
<th>DN05</th>
<th>DN06</th>
<th>DN07</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Generic</td>
<td>IT</td>
<td>Generic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Type</td>
<td>Orgz.</td>
<td>IT</td>
<td>Generic</td>
<td>Struc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing Risk Analysis</td>
<td>-</td>
<td>+</td>
<td>±</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Risk Standard</td>
<td>-</td>
<td>±</td>
<td>-</td>
<td>±</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Maturity</td>
<td>Integrated Risk Formalization</td>
<td>Abstract Syntax</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>(N/A)</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Concrete Syntax</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Semantics</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Implementation</td>
<td>-</td>
<td>±</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>(+)</td>
<td>-</td>
</tr>
<tr>
<td>Application Methodology</td>
<td>-</td>
<td>-</td>
<td>±</td>
<td>-</td>
<td>±</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Application in Practice</td>
<td>±</td>
<td>±</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>BPM Lifecycle</td>
<td>Design</td>
<td>±</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>±</td>
</tr>
<tr>
<td></td>
<td>Design-time Analysis</td>
<td>±</td>
<td>+</td>
<td>±</td>
<td>±</td>
<td>-</td>
<td>±</td>
</tr>
<tr>
<td></td>
<td>Execution</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Runtime Analysis</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Post-execution Analysis</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Notes:
[1] A high-level ontology is provided.
[2] Implemented in the sense that they use existing software.

Runtime R-BPM

In this section, two approaches which primarily focus on addressing process risks during runtime are summarized. The summary of the evaluation results for these two approaches is provided in Table 6.

Obviously, there is a lack of approaches addressing risk issues during the runtime stage of business processes. A handful of approaches that have attempted to address this include Conforti et al.’s and Kang et al.’s [Conforti, Fortino, La Rosa and ter Hofstede, 2011] [Kang, Cho and Kang, 2009]. These two approaches differ in the sense that Conforti et al. introduce a set of risk-related constructs (in the form of a language) that are executable at runtime, while Kang et al. do not attempt to do so (instead, focusing on proposing a runtime risk analysis technique). Similar to other design-time approaches which propose new risk constructs, the semantics of the language proposed by Conforti et al. is not formalized. Both approaches have some form of implementation, although they are yet to be applied in practice.

Conforti et al.’s approach applies an existing risk-analysis technique, and it caters to a variety of risk types (e.g. organizational risk, data risk, and structural risk), while this is not the case with Kang et al.’s. Nevertheless, neither is influenced by any existing risk standards. Both approaches are generic enough to be applied in any domain. Please refer to Appendix E for a detailed explanation and evaluation of these approaches.

Post-execution R-BPM

In this section, the evaluations of two approaches which primarily focus on analyzing business process risks during the post-execution stage of the BPM lifecycle are summarized. The summary of the evaluation results for these two approaches is provided in Table 6.
Similar to runtime R-BPM, there is a lack of approaches addressing post-execution R-BPM. The handful of approaches in this category include those by Jans et al. [Jans, van der Werf, Lybaert and Vanhoof, 2011, Jans, Lybaert, Vanhoof and van der Werf, 2008, Jans, Depaire and Vanhoof, 2011] and Wickboldt et al. [Wickboldt, Bianchin, Lunardi, Granville, Gaspar et al., 2011]. Wickboldt et al. use a set of constructs to capture risk-related information in a process log such that they can be subsequently used for risk analysis. On the contrary, Jans et al.’s approach does not attempt to introduce new risk constructs; rather, it simply attempts to analyze the existence of risks based on an existing log. This approach has been validated in practice, although this is not the case for Wickboldt et al.’s.

Both approaches have been developed for a specific domain. Some risk standards have been used in Wickboldt et al.’s approach but none in the case of Jans et al. Please refer to Appendix F for a detailed explanation and evaluation of these two approaches.

<table>
<thead>
<tr>
<th>Table 6: Evaluation – Runtime and Post-execution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approach</td>
</tr>
<tr>
<td>Domain</td>
</tr>
<tr>
<td>Risk Type</td>
</tr>
<tr>
<td>Existing Risk Analysis</td>
</tr>
<tr>
<td>Risk Standard</td>
</tr>
<tr>
<td>Maturity</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Implementation</td>
</tr>
<tr>
<td>Application Methodology</td>
</tr>
<tr>
<td>Application in Practice</td>
</tr>
<tr>
<td>BPM Lifecycle</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Notes:
[1] Uses existing software.

VIII. RESEARCH GAP ANALYSIS

Based on the results of the literature evaluation, some research gaps in the area of R-BPM are identified and explained. These gaps are discussed in terms of:

- the amount of research contribution in the area of R-BPM for each stage of the BPM lifecycle,
- the comprehensiveness of the functionality proposed for each stage of the BPM lifecycle,
- the maturity of the approaches, and
- the level of influence of existing risk management techniques and standards on the R-BPM approaches evaluated in this paper.

A summary of the identified research gaps is provided at the end of this section.

**Research Contribution per BPM Lifecycle Stage**

An obvious research gap in the area of R-BPM is the lack of research addressing runtime and post-execution risk analysis/management in business process systems.
As shown in Figure 2, of the 27 approaches evaluated, there are only three approaches which address the runtime risk analysis stage of business processes, one approach which addresses the execution stage, and two approaches which focus on the post-execution stage. In contrast, there are 20 approaches which address design-time activities, and 18 approaches which address the design-time analysis activities (note that some approaches support more than one lifecycle stage).

Having many approaches addressing a particular BPM lifecycle stage does not mean that a particular BPM lifecycle stage has better support and/or maturity than another. Nevertheless, the lack of approaches addressing a particular BPM lifecycle stage indicates that research in that particular stage of BPM lifecycle is still relatively new and that there are potentially more unexplored alternatives.

**Functionality Comprehensiveness Gap Analysis per BPM Lifecycle Stage**

In this section, the research gaps for each stage of the BPM lifecycle (in terms of support comprehensiveness) are detailed. Figure 3 summarizes the overall comprehensiveness of support for each stage of the BPM lifecycle provided by all 27 evaluated approaches.

**Design-time Research Gap**

Of the 27 approaches evaluated, 20 approaches provide either comprehensive or partial design-time support - see Figure 3. Specifically, 14 approaches provide what we evaluated to be comprehensive (+) support (about 51.9% of all approaches evaluated), while 6 approaches provide partial support (about 22.2%). Based on these numbers, we argue that design-time support is one of the most researched areas of R-BPM. However, this does not mean that this is a well-studied area.
Using the interpretation provided in Section VI, we consider design-time activities to include both the annotation of business process models with risk-related constructs and the use of risk-informed design principles/guidelines to generate/modify process models. By studying Table 2 (under the ‘Design’ column), we can see that most approaches support the former activity: about 17 out of the 20 design-time approaches propose the use of annotation techniques to enrich process models with risk-related information. Support for the latter activity is low by comparison. This is reflected in Table 2: there are only a minimal number of approaches which seek to provide risk-informed design principles/guidelines (as a result of, for example, risk propagation analysis and/or risk evaluation analysis) such that risks in business processes can be mitigated/avoided by design.

Therefore, there are still many research areas that need to be addressed in the area of risk-informed business process design. Design principles/guidelines that can be applied to minimize the occurrence probability of risk events, or to contain the propagation of risk events are still subject to further research. Furthermore, as risks are discovered, best practices on business process modification such that the discovered risk can be mitigated or eliminated are yet to be proposed. In a nutshell, there are still many research opportunities in the area of risk-informed business process design.

Similarly, while there are already many approaches that attempt to provide techniques to annotate business processes with risk information, these approaches can still be improved.

**Design-time Risk Analysis Research Gap**

There is moderate support for design-time risk analysis stage: there are about 18 approaches which provide either comprehensive (3 approaches – 11.1%) or partial (15 approaches – 55.6%) support for design-time risk analysis (see Figure 3). Research efforts in this area are distributed across various types of risk analysis, including risk probability analysis, risk impact analysis, risk propagation analysis, risk identification/discovery analysis, and risk mitigation analysis.

Fenz et al.’s approach [Fenz and Neubauer, 2009] [Fenz, Ekelhart and Neubauer, 2009] [Fenz and Ekelhart, 2009] [Fenz, 2010] provides quite detailed and convincing risk analysis methods: the two dimensions of ‘risk’ (that is, the probability of the occurrence of a risk event and its impact) are studied using a combination of Petri-net based model analysis and Bayesian network analysis.

Unfortunately, most of the other approaches lack the technical and/or theoretical precision to afford a convincing design-time risk analysis approach. For example, Betz et al.’s approach [Betz, Hickl and Oberweis, 2011] (which attempts to perform a risk analysis via simulation) and Karagiannis et al.’s approach [Karagiannis, Mylopoulos and Schwab, 2007] (which proposes the use of test cases to reason about risks) lack the formal foundation to ensure the thoroughness and the exhaustiveness of their analysis. Therefore, the main research gap in this area is to refine existing, or to propose new, design-time risk analysis techniques which are precise and, ideally, exhaustive. This is likely to be a challenging research topic given the complexity of business processes.

A related research gap is in the area of exploiting risk-related constructs in facilitating static design-time risk analysis. As shown in Table 2, while there are many approaches which propose new risk constructs, most of them cannot be used for the purpose of conducting design-time risk analysis. Ideally, we would like to be able to formally exploit risk-related constructs (annotated in a process model) such that sound analysis of risks in business processes can be achieved. Therefore, it would be interesting to investigate how we could extend the already proposed risk constructs (such as Sienou et al.’s [Sienou, Lamine, Pingaud and Karduck, 2010]), such that formal design-time risk analysis can be achieved.

**Execution Research Gap**

As can be seen from Figure 3 and from Table 2, there is only one R-BPM approach which attempts to address the issue of business process’ risks during the execution stage of a BPM lifecycle, i.e. Conforti et al.’s approach [Conforti, Fortino, La Rosa and ter Hofstede, 2011]. While the comprehensiveness of the support provided by this approach is quite good, there are still plenty of research opportunities in this area.

A notable research question is how we can influence the execution behavior of a running process instance based on runtime risk information such that potentially risky events can be avoided or mitigated. For example, given the high probability that a process instance may reach an undesirable state, a risk-informed process execution should be able to dynamically ‘modify’ the sequence of activities of the related process such that the detected risk can be minimized.
A related research question is how we can enhance the runtime risk information used to influence the execution behavior of a running process by exploiting the related process’ historical data. While the use of historical data to enhance various aspects of running processes (such as the minimization of remaining cycle time) has been proposed [van der Aalst, 2011], the use of historical data to minimize/mitigate runtime risks can be explored further.

Finally, another research gap that we have identified is on the issue of proposing a single set of risk-related constructs that can be exploited both at design-time and runtime for the purpose of risk analysis. Conforti et al.’s approach in its current form does not allow the risk annotation to be exploited to perform design-time risk analysis. There are benefits that can be realized when the same modeling constructs are used for both design-time and runtime risk analysis, including the ability to tighten the reasoning of risks between the design-time and runtime stages and the ability to design a cleaner risk-annotated process model (as there are now fewer variations in the types of risk annotation schemas applied to the model).

Runtime-Analysis Research Gap
The number of approaches which attempt to provide runtime risk analysis capability in an R-BPM system is low. As can be seen from Figure 3 and Table 2, there are a total of three approaches which attempt to provide runtime risk analysis capability, and only two which provide adequate/convincing support.

Unfortunately, while the runtime risk analysis techniques proposed by these two approaches [Conforti, Fortino, La Rosa and ter Hofstede, 2011] [Kang, Cho and Kang, 2009] are quite convincing, they are focused on a particular type of risk analysis: the probability analysis. Similarly, Singh et al.’s runtime analysis approach [Singh, Gelgi, Davulcu, Yau and Mukhopadhyay, 2008] also only focuses on one particular aspect of analysis: the adequacy of their risk mitigation strategy. Nevertheless, all three approaches do provide a form of runtime risk monitoring capability.

There are still many opportunities for research in this area, including the analysis of the impact/consequences of risk events to a process (which may be different from its original design-time impact analysis), the prediction of possible risk propagation paths of process instances (which may differ from one instance to another due to different runtime variables), the overall risk-level evaluation of running process instances, and more ambitiously, the identification of new risks which have not been considered during design-time.

Another research challenge related to runtime risk analysis is on the issue of performance. Unlike design-time risk analysis, results from runtime risk analysis need to be produced within a reasonable period of time so that an informed intervention to running processes can be achieved before it is too late. This raises the issue of the trade-off between risk performance (in terms of being able to calculate an optimal risk mitigation solution) and process performance (in terms of minimizing process delays).

Post-execution Research Gap
Similar to runtime analysis, the number of approaches which attempt to facilitate post-execution risk analysis is low. There are only two approaches that attempt to reason about risks using post-execution data. Nevertheless, given the comparatively mature research in the field of data mining and process mining (upon which research the post-execution stage tends to rely), the comprehensiveness of research in this particular BPM lifecycle stage is rather high (see Figure 3).

However, there are still many unknowns in this area, which suggest the need to conduct further research. For example, it is yet to be determined if existing process execution logs do provide sufficient information to facilitate post-execution risk mining. Furthermore, while these two approaches allow the identification of risks from existing process logs (such as the risk of a ‘four-eye principle’ violation), techniques to determine the root-cause of such violations through the use of process logs are yet to be proposed.

Other interesting research gaps in this area include how we can use the historical information from a process’ logs to inform the re-design of a business process, to confirm the effectiveness of risk mitigation strategies, and to refine runtime risk analysis and monitoring techniques.

Maturity Gap Analysis
In this section, we analyze the research gap in terms of the maturity of the evaluated approaches (using the maturity criteria defined in Section VI) based on their main focus: design-time (the approaches detailed in Table 3, Table 4 and Table 5), runtime, (the first two approaches detailed in Table 6), and post-execution (the last two approaches detailed in Table 6). Figure 4 summarizes the results of our maturity evaluation.
Design Stage Maturity

While the majority of approaches evaluated in this paper belong to design-time approaches, the maturity level of research in this area still needs to be improved. The overall maturity of those approaches which propose new risk constructs (16 out of 23 approaches in this category) is quite low, as demonstrated by the fact that most approaches only go as far as specifying the concrete syntax (i.e., the forms in which concepts/constructs are represented externally, e.g. graphical notations) of the proposed constructs. Furthermore, none of the approaches actually provides a comprehensive and precise definition of the meaning of the proposed constructs (see Figure 4). Therefore, there is still room for improvement in the formalization of the concept of risk in business processes.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(23 approaches)</td>
<td>43.75%</td>
<td>87.50%</td>
<td>52.94%</td>
<td>6.25%</td>
<td>13.04%</td>
<td>60.87%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(2 approaches)</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>50.00%</td>
<td>100.00%</td>
<td>50.00%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(2 approaches)</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>50.00%</td>
<td>100.00%</td>
<td>50.00%</td>
</tr>
</tbody>
</table>

Furthermore, the majority of approaches in this category are still ‘theoretical’ in that they are not yet implemented as tools that can be used by practitioners. In fact, less than 30% of the approaches have actually been implemented. Worse, the extent to which these approaches have been comprehensively validated in practice is even lower (around 22%). Such a low maturity level is also demonstrated by the fact that only about a third of the approaches in this category provide comprehensive application methods, while the remaining approaches provide either a high-level description of how their approach can be applied, or none at all.

Runtime Stage Maturity

While there are only two 2 approaches which attempt to provide an R-BPM capability during runtime, Figure 4 suggests that these approaches demonstrate a moderate level of maturity. There is only one approach [Conforti, Fortino, La Rosa and ter Hofstede, 2011] which attempts to provide integrated risk constructs to annotate process model with risks. The formal definition of the proposed constructs is expressed rather comprehensively, although the formalization of the meaning (i.e. the semantics) of the proposed constructs can still be improved.
Furthermore, all of the approaches in this category have either been fully or partially implemented. Nevertheless, these approaches are yet to be comprehensively applied in practice, and the details of their application methods still need improvement.

Post-execution Stage Maturity

Similar to the runtime R-BPM approaches, despite the limited number of approaches evaluated in this category (only two approaches), Figure 4 suggests that these approaches demonstrate a moderate level of maturity.

There is only one approach [Wickboldt, Bianchin, Lunardi, Granville, Gaspery et al., 2011] which attempts to propose risk constructs to enrich process logs with risk-related information. The formal definition of the proposed constructs is expressed rather comprehensively, although it still lacks the formalization of the meaning (i.e. the semantics) of the proposed constructs.

All of the approaches in this category have also been implemented. The maturity of the application methodology of the approaches in this category is quite high as well, given that some of them actually make use of the relatively mature process mining tool, ProM [van Dongen, de Medeiros, Verbeek, Weijters and van der Aalst, 2005].

There is a gap in terms of the application of these approaches in practice. Out of the two approaches in this category, only one approach, by Jans et al [Jans, van der Werf, Lybaert and Vanhoof, 2011] [Jans, Lybaert, Vanhoof and van der Werf, 2008] [Jans, Depaire and Vanhoof, 2011], used logs from real-world organization in their analysis. Furthermore, there seems to be only a limited discussion and validation of the results of their approaches with the practitioners of the organizations from which the logs were obtained (this is especially true for Wickboldt et al.’s approach [Wickboldt, Bianchin, Lunardi, Granville, Gaspery et al., 2011]).

Gap in the Integration with Existing Risk Management Techniques

Given the maturity of classical risk management techniques (such as Bayesian network analysis and Monte Carlo simulation), it is a worthwhile endeavor to apply these techniques into R-BPM. However, based on the evaluation detailed in Section VII, we can conclude that the link between existing risk management techniques and standards with the BPM field is weak. Of all 27 approaches evaluated, there are only seven approaches (or 26%) which apply existing risk management techniques. Similarly, there are only three approaches (or 11%) which are clearly influenced by existing risk management standards.

Therefore, how we can seamlessly apply existing risk management techniques to reason about risks in a business processes is an interesting research topic that is worthy of further exploration. Furthermore, how best practices and requirements from existing risk-related standards (such as Basel II [Basel, 2006] and SOX [107th Congress - USA, 2002]) can be incorporated into existing BPM systems is another research topic that requires further study.

Research Agenda

Based on the gap analysis conducted thus far, we now summarize the research gaps in the area of R-BPM and provide suggestions on how to address the identified gaps where appropriate.

There is insufficient attention given to runtime risk management in BPM systems and to the exploitation of process-related logs for the purpose of risk event identification, analysis, evaluation, and mitigation. As shown in Figure 1, research efforts directed towards runtime and post-execution stage of an R-BPM system are limited. This research is needed because it provides an additional layer of risk management to detect risk-related events which may not have been considered during design time. The use of process logs to analyze, to detect, as well as to discover various risk-related events is also crucial to enable proper evaluation and improvement of a process’ risk management strategies.

Risk-informed business process design is a research area that still requires further exploration. Earlier in this section, we described the lack of research aimed at providing risk-informed business process design. The existence of guidance and/or principles to allow one to design a business process based on risk-related information (such as the discovery of risk events, the probability of the occurrence of some ‘bad’ events, etc.) obtained, for example, through design-time risk analysis or post-execution log analysis, is a highly desirable feature because it can reduce the risk level of a process by design. This in turn may minimize the cost associated with runtime risk management. One may proceed with research in this area by identifying patterns/factors that contribute to the occurrence of risk events in a particular domain. Then, through empirical studies, we can derive and validate a set of risk-informed design principles (or even patterns) that can be applied to avoid/mitigate risky events in that particular domain.
The degree to which risk constructs are formalized needs to be improved such that they can be exploited to enable formal reasoning of risks. As explained earlier, the lack of formal semantics given to the risk constructs evaluated in this paper has made it difficult to perform a much richer formal analysis of the effects of risks in a risk-annotated process model. This feature is essential as the mathematical foundation of a formal analysis approach provides many benefits which may not be realized in its absence [Clarke and Jeannette, 1996], such as the unambiguity of the meaning of risk constructs and the detection of subtle or obscure (chains of) events which may prove risky. Research in this area may move forward by extending existing risk constructs (such as those proposed by Cope et al. [Cope, Deleris, Eitzweiler, Koehler, Kuester et al., 2010] and Rotaru et al. [Rotaru, Wilkin, Churilov, Neiger and Ceglowski, 2009]) with their execution semantics such that risks in business processes can be reasoned about using these constructs.

The application of existing risk analysis techniques from the risk management domain into BPM is an area that is worth further investigation. The number of existing approaches which attempt to apply existing risk analysis techniques is low. However, given the comparatively mature risk analysis methods from the risk management domain, we may not have to re-invent the wheel by proposing new risk analysis techniques. Instead, we can focus on developing methods to allow the application of those techniques at various stages of the BPM lifecycle. This type of research may start with a closer look at the feasibility of integrating existing risk analysis techniques (such as Monte Carlo simulation, Failure modes and effects analysis, and Bayesian network analysis) into the BPM field. We can then progress the research with an investigation into the type of enhancements needed to be applied to existing process models (e.g. annotation of process models with risk constructs) to facilitate such analysis.

Research in the area of risk-informed business process execution needs to be conducted. Earlier, we explained the lack of research in facilitating risk-informed process execution. Regardless of the extent to which risk has been considered during design-time, it is likely that there will be risks which are manifested during runtime and which cannot be fully mitigated or avoided by design. This is because it is impossible to foresee every possible event and context (e.g. a simple data entry error that was not anticipated during design time). Therefore, the ability to dynamically modify the execution behavior of a running process instance based on some detected runtime risks (obtained, for example, through runtime risk analysis) may prove useful runtime risk mitigation. The scope of research in this area can be as simple as providing alerts, and perhaps enabling runtime exception handling mechanisms such that process execution can be modified at runtime. A more sophisticated, and possibly complex, approach is to develop an automated process modification technique at runtime that can reduce the impact and/or probability of detected risks. We can also take this research even further by exploring how runtime-generated risk mitigation results (such as the produced risk alerts and automatically-generated process modification recommendations) can be used as inputs to re-design the process model(s) for future executions (we call this a runtime informed process re-design capability).

While the use of post-execution/historical logs for the purpose of process risk analysis is ripe for exploration, it is still largely ignored in the research community. Given the increasing prevalence of BPM systems [Dixon, 2011], there is now a reasonable amount of process-related logs [van der Aalst, 2011] which can be analyzed to draw various risk-related facts. However, research in this area is still largely unexplored. By using historical data, we enable evidence-based analysis and verification of various risk phenomena. For example, one may be able to determine the actual root cause of some risky events based on the information in process logs. One way to proceed with research in this area is to study how existing data mining techniques can be enhanced with process ‘flavor’ to perform process-based risk analysis. Additionally, one may also proceed with enriching the log structure to record risk-related information such that richer risk analysis can be facilitated.

Proper empirical validation of approaches to R-BPM is yet to be conducted. With a few exceptions, most approaches evaluated in this paper are investigated at a theoretical level. However, research outcomes need to be applied and evaluated in practice in order to validate their actual usefulness and feasibility. Developing and managing relationships with industry-based BPM practitioners will be essential in order to enable an empirical validation of research outcomes.

A reference model for R-BPM is needed. Currently, there is no agreement about the key features that an R-BPM system should possess. For example, many approaches proposed the use of risk constructs to annotated process models with risk information; however, there is not yet a standard which clearly specifies the types of construct that we really need to be considered an R-BPM. Similarly, there are many concepts (such as being risk-aware vs. being risk-informed) which are yet to be understood in the overall scheme of an R-BPM system. The scope of an R-BPM
IX. CONCLUSIONS

In this paper, we conducted a comprehensive survey of existing approaches aimed at providing a risk-aware business process management system. We detailed the process through which relevant literature was collected, as well as the theoretical basis upon which our evaluation framework was developed. Following a systematic evaluation of each approach according to our evaluation framework, research gaps were identified, explained and summarized. In a nutshell, while there is growing research dedicated to enabling an R-BPM system, there is still a lack of research which investigates the management of risks during process execution, the exploitation of post-execution data for the purpose of risk analysis and the enablement of an integrated formal reasoning of risks in process models. Moreover, the integration of techniques from the traditional risk management domain into the BPM domain still leaves room for investigation and most of the evaluated approaches still need to be validated in practice to determine their feasibility and effectiveness. Finally, a reference model of an R-BPM system is yet to be proposed.

ACKNOWLEDGEMENTS

We thank Matthias Voigt and Mathias Eggert of the European Research Center for Information Systems (ERCIS) for their valuable input with regards to the theoretical framework underpinning the development of the evaluation framework used in this paper. This research is partly supported by the Australian Research Council (ARC) Discovery Project through grant DP110100091.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.


APPENDIX A
Relevant papers were drawn from the following journals, conferences, and workshops (2005 - Sept 2011).

Journals:

- MIS Quarterly
- Information Systems Research
- Journal of the Association of Information Systems
- European Journal of Information Systems
- Journal of Management Information Systems
- Information Systems Journal
- Journal of Information Technology
- Journal of Strategic Information Systems
- Information Systems
• Data and Knowledge Engineering
• ACM Transactions on Software Engineering and Methodology
• IEEE Transactions on Software Engineering
• IEEE Transactions on Knowledge and Data Engineering
• Information Sciences
• Information and Software Technology
• Distributed and Parallel Databases
• Business Process Management Journal
• Journal of Operational Risk
• IEEE Transactions on Dependable and Secure Computing

Conferences and Workshops:

• BPM - Business Process Management (conference and workshops)
• CAiSE - International Conference on Advanced Information Systems Engineering (conference and workshops)
• CoopIS - International Conference on Cooperative Information Systems
• ER - International Conference on Conceptual Modelling (conference and workshops)
• ICIS - International Conference on Information Systems
• AMCIS - Americas Conference on Information Systems
• ECIS - European Conference on Information Systems
• ACIS - Australasian Conference on Information Systems
• PACIS - Pacific Asia Conference on Information Systems
• ERM - Enterprise Risk Management Symposium
• GRCIS - International Workshop on Governance, Risk and Compliance - Applications in Information Systems
• ARES - International Conference on Availability, Reliability and Security
• TrustBus - International Conference on Trust, Privacy and Security in Digital Business
• CCS - ACM Conference on Computer and Communications Security
• Network and Distributed System Security Symposium
• USENIX Security Symposium
• ESORICS - European Symposium on Research in Computer Security
• ACSAC - Annual Computer Security Applications Conference
APPENDIX B
An explanation of how to interpret the meaning of (+), (±), and (−) for each evaluation criterion described in Section VI is provided below.

Process Lifecycle Evaluation

Design
- (+): The approach proposes relevant techniques or methods which are thorough and/or formal. One example can be the proposal of a set of graphical notations that are sufficient for the purpose of the approach. Another example may be the proposal of end-to-end techniques or a set of principles that can be used to guide a process modeler in re-designing a process model from its original form (which may be susceptible to the occurrence of undesirable/risky events) to another form in which risk mitigation activities are integrated in the process to minimize the occurrence of risk events.
- (±): The approach proposes relevant techniques or methods but they are somewhat incomplete, ambiguous, and/or informal, e.g. the proposal of a set of graphical notations that can only capture a subset of risk-related information into a process model.
- (−): No relevant techniques or methods are proposed at all.

Design-time Analysis
- (+): The approach provides comprehensive risk analysis/evaluation support, e.g. the proposal of techniques, based on solid/well-accepted theoretical foundations, to measure the overall risk of a process by considering the two key dimensions of risk (the probability of the occurrence of a risk event and the impact of the risk event).
- (±): The approach only provides limited risk analysis/evaluation capabilities, e.g. the proposal of techniques to analyze only one dimension of risk, the proposal of risk analysis/evaluation techniques which are not based on any solid/well-accepted theoretical foundation, or the use of a simulation technique to reason about risks.
- (−): No relevant techniques or methods are proposed.

Execution
- (+): The approach proposes risk modelling constructs that can be operationalized to comprehensively monitor risk, and/or to influence the execution behavior, of running process instances.
- (±): The approach proposes a limited set of executable risk modelling constructs and/or the approach proposes one or more techniques that can be used to influence the execution behavior of a running process instance but of limited functionality or of a preliminary nature.
- (−): The proposed risk modelling constructs cannot be executed, or if there is no approach proposed to influence the behavior of a running process instance.

Runtime Analysis
- (+): The approach proposes comprehensive runtime risk analysis technique(s), e.g. the proposal of techniques to measure the probability of the occurrence of a risk event and the impact of the risk event at runtime based on well-founded theory, or the proposal of a comprehensive runtime risk monitoring capability.
- (±): The approach proposes limited runtime risk analysis capabilities.
- (−): No runtime risk analysis is proposed.

Post-execution Analysis
- (+): Comprehensive risk analysis/evaluation technique(s) exploiting the collected post-execution information are proposed.
- (±): Only limited post-execution analysis capabilities are proposed.
- (−): No such support is proposed.
Maturity Evaluation

Integrated Risk Formalization

- **Abstract Syntax:**
  o (+): The approach specifies the abstract syntax of all (or most) of the proposed risk-related constructs using well-accepted/well-known formal description technique(s), such as those mentioned above.
  o (±): The approach defines the abstract syntax for a small subset of the proposed risk-related constructs using well-accepted/well-known formal description technique(s). In other words, the abstract syntax of many of the proposed constructs is left unspecified.
  o (−): The approach does not specify any abstract syntax for the proposed risk-related constructs, or the abstract syntax of the proposed constructs is described using techniques that are considered informal (that is, those techniques that generally allow room for ambiguous interpretation), such as natural languages or ad-hoc diagrams.
  o N/A: The approach does not propose any new risk-related constructs.

- **Concrete Syntax:**
  o (+): The approach specifies the concrete syntax of all (or most) of the proposed risk-related constructs.
  o (±): The approach specifies the concrete syntax for a small subset of the proposed risk-related constructs (the concrete syntax of many of the proposed constructs is left unspecified).
  o (−): The approach does not specify any concrete syntax for the proposed risk-related constructs.
  o N/A: The approach does not propose any new risk-related constructs.

- **Semantics:**
  o (+): The semantics of all (or most) of the proposed risk constructs is defined using proper formal technique(s) mentioned above.
  o (±): The approach only defines the semantics of a small subset of the proposed risk-related constructs (the semantics of many of the proposed constructs is left unspecified).
  o (−): The approach does not specify any semantics for the proposed risk-related constructs, or the semantics of the proposed constructs is described using techniques that are considered informal (that is, those techniques that generally allow room for ambiguous interpretation), such as natural languages.
  o N/A: The approach does not propose any new risk-related constructs.

It should be noted that the BPM lifecycle criteria are used to indicate the BPM lifecycle stage(s) addressed by a particular approach. The 'integrated risk formalization' criterion is, on the other hand, used to indicate not only the maturity of the proposed constructs (in terms of the clarity and unambiguity of the specifications of the constructs), but also the process lifecycle stages to which the constructs can be applied:

- if an approach receives a non-applicable (N/A) evaluation for the 'integrated risk formalization' criterion, then it means that the approach does not propose any new risk constructs to support the BPM lifecycle stage(s) addressed by the approach (instead, other techniques, such as Bayesian network analysis, are used to analyze and reason about risks in business processes);
- however, if an approach receives an evaluation result of no support (−), partial support (±), or full support (+) for any one of the 'integrated risk formalization' sub-criteria (abstract syntax, concrete syntax, and/or semantics), then it means that the BPM lifecycle stage(s) addressed by the approach are somewhat supported by the use of new risk constructs.

Implementation

- (+): The approach has been fully implemented (that is, can be used as a fully functioning tool).
- (±): The approach has only been partially implemented (for example, a prototype implementation).
- (−): The approach has not been implemented.
Application Method

- (+): There are step-by-step guidelines (with detailed and comprehensive explanations) on how users can apply the proposed approach.
- (±): The approach provides high-level guidelines to give readers an idea of how the approach can be applied but with 'missing steps/explanations' in the guidelines which raise the questions on how a particular step should be executed or how a particular feature of the approach can be achieved.
- (-): No application method is detailed.

Application in Practice

- (+) There is clear evidence that the approach has been fully applied and evaluated in real-world organizations.
- (±) There is a proof-of-concept or limited trial application of the approach in real-world organizations.
- (-) There is no clear evidence that the approach has been applied in real-world organizations (e.g. a claim of the applicability of the approach in practice, or a made-up example 'demonstrating' the applicability of the approach, would not suffice).

Influence of Risk Management Domain

Risk Analysis Technique

- (+): Existing risk analysis techniques (such as the Monte Carlo simulation or the Bayesian network analysis [Heckerman, 1995]) are applied directly in the approach.
- (±): The approach is somewhat inspired by existing risk analysis techniques (although the approach may not follow the techniques exactly as in their original forms).
- (-): The proposed approach does not apply any existing risk analysis techniques.

Risk Standards

- (+): There is clear evidence that one or more risk standard(s) have informed the approach.
- (±): The approach occasionally draws example clauses/statements from one or more risk standards and shows how those statements can be expressed or addressed in the approach.
- (-): There is no evidence that any risk standards have been incorporated in the approach, or the approach only mentions certain standards without any further elaboration or evidence demonstrating the incorporation of the standards in the approach.
APPENDIX C

This section provides a detailed evaluation of all approaches surveyed in this paper which address design-time R-BPM by introducing new risk-related constructs. The evaluation results are summarized in Table 3 and Table 4.

DI01 - Jakoubi et al.

The first approach we evaluated was the Risk-Oriented Process Evaluation (ROPE) approach [Tjoa, Jakoubi and Quirchmayr, 2008] [Tjoa, Jakoubi, Goluch and Kitzler, 2010] [Tjoa, Jakoubi, Goluch and Quirchmayr, 2008] [Tjoa, Jakoubi, Goluch, Kitzler, Goluch et al., 2011] [Jakoubi, Tjoa and Quirchmayr, 2007] [Jakoubi, Tjoa, Goluch and Kitzler, 2010a] [Jakoubi, Tjoa, Goluch and Kitzler, 2010b] [Jakoubi, Neubauer and Tjoa, 2009] [Jakoubi, Goluch, Tjoa and Quirchmayr, 2008] [Jakoubi and Tjoa, 2009] [Goluch, Ekelhart, Fenz, Jakoubi, Tjoa et al., 2008]. This approach proposes a 3-layer model to capture the notion of ‘risk’ within a business process model. The top layer of this model is the business process layer which consists of business process activities. These activities are decomposed into their corresponding Condition, Action, Resource, and Environment (CARE) elements to form the middle layer of the model. The bottom layer of this model, called the Threat Impact Process (TIP) layer, captures the various threats that may affect the corresponding CARE elements (at the middle layer) and the countermeasure activities that may mitigate the threats. A security ontology (based on Ekelhart et al.’s proposal [Ekelhart, Fenz, Klemen and Weippl, 2007]) is also used to inform the design of the CARE and TIP layers. This ROPE-based model can then be analyzed (via simulation) to understand the consequences of threat events on business activities and the effectiveness of the countermeasures (included in the model) in mitigating threat events.

This approach seems generic enough to be applicable to any domain, although it mainly considers risk from the resource (such as IT assets) perspective; in other words, this approach addresses the ‘IT Risk’, based on the risk taxonomy used in our evaluation framework [Rosemann and zur Muehlen, 2005]. This approach also does not apply any existing risk analysis method nor does it attempt to incorporate any particular risk standard.

In terms of the BPM lifecycle evaluation, this approach provides an annotation technique to capture risk-related information (such as threats, countermeasures, and resources); thus, the design stage criterion is supported (+). These annotations can also be used to perform a simulation-based risk analysis during design-time, thus the design-time analysis stage criterion is partially supported (±). The rest of the BPM lifecycle stages are not addressed by this approach.

This approach supports the concrete syntax criterion as it proposes a collection of graphical notations that can be used to represent elements in the 3-layer model of ROPE. The key components and structure of the proposed notations are not specified, thus the abstract syntax criterion is not supported (−). Similarly, the semantics criterion is not supported: while the proposed notations can be used for the purpose of simulation, there is no precise definition of the operations that can be applied to these notations. This approach seems to have been implemented as a prototype [Goluch, Ekelhart, Fenz, Jakoubi, Tjoa et al., 2008], thus the implementation criterion is partially supported. A high-level application method is also described throughout the literature, thus the application method criterion is partially supported. This approach has only been applied as a ‘toy example’, therefore there is no support for the application in practice criterion.

DI02 - Sienou et al.

In Sienou et al.’s approach [Sienou, Lamine, Pingaud and Karduck, 2010] [Sienou, Lamine, Karduck and Pingaud, 2008] [Sienou, Lamine, Karduck and Pingaud, 2007] [Sienou, Lamine, Pingaud and Karduck, 2009] [Sienou, Lamine and Pingaud, 2008] [Sienou, Karduck and Pingaud, 2006] [Sienou, Karduck, Lamine and Pingaud, 2008] [Karduck, Sienou, Lamine and Pingaud, 2007] [Amadou Sienou, 2009], an integrated framework combining the domain of risk management and business process management is proposed. The framework is called the Business Process Risk Management Integrated Method (BPRIM) framework. In this approach, activities that are commonly undertaken during the design stage of a business process (such as process modeling and analysis) are systematically mapped to those activities from the risk management lifecycle [Standards Australia and Standards New Zealand, 2009] to produce an integrated BPM and RM lifecycle. Furthermore, the relationships between the concepts commonly encountered in the field of BPM (such as activity, resources) and RM (such as risk event) are explicitly studied and modeled (using class diagrams). Finally, a set of graphical notations (based on the Event-driven Process Chain (EPC) language) that can be used to annotate business process models with risk-related information (such as risk factor and risk control measures) is proposed.

6 While no abstract syntax is provided, a security ontology was proposed [Ekelhart, Fenz, Klemen and Weippl, 2007] [Ekelhart, Fenz, Klemen and Weippl, 2007].
Similar to the ROPE approach, this approach is not prescribed for any specific domain nor for any specific type of risk. There is also no evidence of the application, or the influence, of any existing risk analysis technique but it is influenced by the Generalised Enterprise Reference Architecture and Methodology (GERAM) framework [IFIP, 1999]. Thus, the risk standards criterion is partially supported (±).

In terms of the BPM lifecycle evaluation, this approach proposes a comprehensive support (+) for the design stage activities of the BPM lifecycle (see Table 2): it proposes an annotation technique to enrich business process models with risk-related information and a high-level methodology to integrate design-time BPM activities with RM activities (such as risk discovery, risk evaluation, and risk treatment) in the form of an integrated lifecycle model. However, this approach does not support (−) the design-time risk analysis criterion: while the proposed notations can be used to capture risk analysis concepts (such as the causal chain of a set of risks [Amadou Sienou, 2009]), there is no specific risk analysis technique proposed. The rest of the BPM lifecycle stages are also not addressed.

This approach provides several UML diagrams to describe the key components, the structure, and the rules (‘grammar’) of the proposed graphical notations. In other words, the abstract syntax criterion is supported through the use of well-known formal techniques. Similarly, the external graphical representation of these notations (that is, the concrete syntax) is also provided, thus the concrete syntax criterion is supported. Nevertheless, there is a lack of specification in terms of the exact execution behavior of the proposed notations is missing. Therefore, the semantics criterion is not supported. The application methods criterion is supported as comprehensive illustration of the application of this approach, through the use of various case studies, is provided. There is no implementation support provided by this approach. Similarly, the application in practice criterion is also not supported as this approach has not been applied in practice.

**DI03 - Cope et al.**

In Cope et al.’s approach [Cope, Kuster, Etzweiler, Deleris and Ray, 2010] [Cope, Küster and Etzweiler, 2009] [Cope, Deleris, Etzweiler, Koehler, Kuester et al., 2010], a number of risk-related modeling constructs are proposed. These constructs are an extension of the Business Process Model and Notation (BPMN)-based [OMG, 2008] language. By applying these constructs, one can encode risk-related information into a process model, such as the various risk events that can occur and the mitigation actions that can be taken. Furthermore, this approach also introduces a state-change event notation such that the ‘causal chains of failure’ of a resource can be captured.

The application of this approach is not restricted to any specific domain, nor is it prescribed for any specific type of risk. Furthermore, there is no evidence that this approach incorporates any specific risk standards. This approach is somewhat inspired by the Bayesian network analysis technique.

This approach provides comprehensive support for design-time activities: it proposes a comprehensive set of constructs that can be used to enrich a business process model with risk-related information. Therefore, the design stage criterion is supported (+). While design-time risk analysis techniques are provided (in terms of risk identification), they are informal. This approach also claims that the risk-annotated process model can be translated into quantitative graphical models, such as a Bayesian network, to enable formal risk analysis of the process. Nevertheless, such a feature is reserved for future work. Therefore, the design-time analysis stage criterion is only partially supported (±). The rest of the BPM lifecycle stages are not addressed by this approach.

The abstract syntax and concrete syntax criteria are supported: the structure of the proposed constructs, including their attributes, are specified using UML class diagrams and a set of graphical notations in which the proposed constructs are represented externally is also provided. While this approach also describes the meaning of the proposed constructs, as well as the operations that can be executed on the proposed notations (that is, the semantics of the constructs), they are specified informally (using natural language), thus the semantics criterion is not supported. This approach has not been supported with an implementation, but the application method criterion is supported as it provides a sufficiently-detailed step-by-step application instructions. Finally, there is no evidence that this approach has been applied in real-world organization, hence, the application in practice criterion is not supported.

**DI04 - Weiβ and Winkelmann**

In Weiβ and Winkelmann’s approach [Weiβ and Winkelmann, 2011], the Semantic Business Process Modelling Language (SBPML) [Becker, Thome, Weiβ and Winkelmann, 2010] is extended with a number of risk-related constructs such that the inclusion of risk-related information (such as risk events, risk control actions, and risk type) into business process models can be achieved. These constructs are expressed as a set of graphical notations.
This approach has been developed in the context of the financial domain. It addresses a type of risk commonly encountered in the financial industry, called the 'operational risk'. However, one can deduce from the literature [Weiβ and Winkelmann, 2011] that what constitutes an operational risk can include many types of risk according to the risk taxonomy used in our evaluation framework. For example, the system failure risk and the erroneous data entry risk alluded in the literature can be respectively mapped to the 'technology risk' and the 'data risk' in the risk taxonomy used in our evaluation framework. Thus, we classify the type of risk being addressed by this approach to be 'generic'. This approach is strongly influenced by the Basel II [Basel, 2006] standard. There is no evidence that this approach applies any existing risk analysis technique.

The design stage criterion is supported as this approach focuses on providing annotation techniques to enrich existing process models with risk-related constructs during design-time. Furthermore, the proposed notations seem to be sufficient to capture the risk information needed. This approach does not support the design-time analysis stage as there is no evidence of the proposal of any risk analysis technique. The rest of the BPM lifecycle stages are not addressed by this approach.

This approach provides an ER diagram to specify the key building blocks of the proposed graphical notations. The graphical symbols that can be used to express the proposed constructs are also provided. Thus, the abstract syntax and concrete syntax criteria are supported (+). This approach does not provide a clear and unambiguous specification of the execution behavior of the proposed notations. Therefore, the semantics criterion is not supported (−). This approach has been validated through its application in a real-world bank, thus the application in practice criterion is supported. There is no evidence that this approach has been implemented, thus the implementation criterion is not supported. The application methods criterion is partially supported (±) as this approach provides very high-level instructions on the application of the approach.

**DI05 - Asnar and Giorgini**

Asnar and Giorgini’s work [Asnar and Giorgini, 2008] addresses business process risk in the context of business continuity management. Building upon the Troops Goal-Risk Framework [Asnar and Giorgini, 2006], also by the same authors, and the Time Dependency and Recovery Model [Zambon, Bolzoni, Etalle and Salvato, 2007], an extended goal-risk framework is proposed. This framework consists of three layers, namely, the asset layer which consists of business process goals, activities, and business artifacts; the event layer which consists of various events (including risk events) that can impact the asset layer; and the treatment layer which consists of a set of risk treatment activities that can mitigate the impact of the occurrence of the risky events modeled in the event layer. Several risk analysis techniques which manipulate this extended goal-risk framework are also proposed.

The proposed analysis techniques applied existing risk analysis techniques (notably the Cost-Benefit analysis technique and the Treatment analysis technique). This approach is not prescribed for any particular domain and its applicability is not restricted to a particular type of risk. There is no evidence that this approach attempts to comply with, or be guided by, risk standards.

In terms of the BPM lifecycle evaluation, this approach addresses the design stage activities through the use of the extended goal-risk framework. The constructs available in the proposed framework are generic enough to allow sufficient amount of risk-related information to be modeled, thus the design stage criterion is fully supported (+). Furthermore, two analysis techniques which can be used to select the most cost-efficient risk countermeasure plan(s) are also proposed and are formally defined. Therefore, the design-time analysis criterion is also fully supported. The rest of the BPM lifecycle stages are not addressed by this approach.

The symbols that can be used to represent the concepts in the extended goal-risk model are provided (hence, full support for the concrete syntax criterion). However, this approach does not provide a specification of the deep structure of the notations used in the model, thus there is no support (−) for the abstract syntax criterion. Similarly, while the extended goal-risk framework can somewhat be operationalized for the purpose of risk analysis and the meaning of the notations are more or less described, there is no formal specification of the meanings of these constructs and their operations. In other words, the semantics criterion is not supported. Similarly, this approach is not supported by an implementation. We found no guidance/instructions on the application of this approach; hence, the application methodology criterion is not supported. This approach has been validated in a simplified industry-based case study, resulting in a partial (±) support for the application in practice criterion.

**DI06 - Mock and Corvo**

In Mock and Corvo’s approach [Mock and Corvo, 2005], a number of risk-related constructs are proposed. These constructs can be used to annotate an EPC-based process model with risk events. The severity of each risk event (also called the risk priority number) and the causal chains of risk events can also be captured. To complement
these constructs, this approach demonstrates the application of the Failure Mode and Effects Analysis (FMEA) risk analysis [US Department of Defense, 1949] to identify the risk events in a process and the propagation of those events.

This approach is not prescribed for any specific domain, nor is it developed specifically to address a particular type of risk. This approach does apply an existing risk analysis technique (the FMEA method), although it does not attempt to conform to any particular risk standard.

In terms of the BPM lifecycle evaluation, this approach addresses the design stage activities through the proposal of a risk annotation technique (also see Table 2). The proposed constructs are sufficient to capture the risk information needed by this approach and they are sufficiently elaborated, therefore the design stage criterion is supported (+). While this approach demonstrates the application of the FMEA technique, there is a lack of information in terms of how the occurrence probability and the impact of a risk event can be calculated (instead, it is assumed that such information is already available). Thus, the design-time analysis criterion is only partially supported (±). The rest of the BPM lifecycle stages are not addressed by this approach.

A set of graphical notations is introduced to represent the proposed risk constructs. Therefore, the concrete syntax criterion is supported. The exact components and/or attributes that the proposed graphical notations should contain are not specified, thus the abstract syntax criterion is not supported (−). Similarly, the details of the operations that can be executed on the proposed constructs are also missing, thus the semantics criterion is also not supported. The application methods criterion is supported as rather detailed guidance on how the approach may be applied, especially in terms of the application of the FMEA technique to identify risks in a process model, is provided. This approach is claimed to have been applied in practice through a feasibility study with a major German bank, thus the application in practice criterion is supported. It should be noted that due to the non-disclosure agreement, the detailed results of the study are not published. This approach has not been supported by an implementation.

**DI07 - Rosemann and zur Muehlen**

In Rosemann and zur Muehlen’s work [Rosemann and zur Muehlen, 2005], a risk taxonomy is proposed. This risk taxonomy describes five errors in which various types of risk can manifest (goal error, structural error, data error, technological error, and organizational error.) This approach also extends the EPC notation with a number of modeling constructs to capture risk-related information in process models. Furthermore, this approach also introduces various modes (such as risk structure mode and risk state mode) in which these risk constructs can be used to provide a range of insights of risks in business processes [Rosemann and zur Muehlen, 2005].

This approach is not developed specifically for any particular domain, nor is it prescribed for any particular type of risk. There is also no evidence of the application of any existing risk analysis technique or risk standard.

In the context of the BPM lifecycle evaluation, the design stage criterion is supported (+) through the proposal of new risk-related constructs to annotate process models with risk information. While the proposed risk constructs are limited (two new constructs are proposed), they are versatile enough to capture the various modes in which business process risk can be represented. However, the design-time analysis criterion is not supported (−). The rest of the BPM lifecycle stages are not addressed by this approach.

The concrete syntax criterion is supported as this approach does specify the graphical notations that can be used to represent the proposed constructs. The exact structure and the components (in other words, the abstract syntax) of which these notations are composed are not specified. Similarly, the exact execution operations of these notations are not specified. Thus, the abstract syntax and semantics criteria are not supported. Some of the features proposed in this approach have been implemented, thus the implementation criterion is partially supported (±). However, the application methods criterion is not supported as this approach does not provide any guideline or instruction that one can follow to apply it. Similarly, the application in practice criterion is also not supported as there is no evidence that this approach has been applied in any industrial domain.

**DI08 - Rotaru et al.**

In Rotaru et al.’s work [Rotaru, Wilkin, Churilov and Neiger, 2008] [Rotaru, Wilkin, Churilov, Neiger and Ceglowski, 2009] [Neiger, Churilov, zur Muehlen and Rosemann, 2006], the Value-Focused Process Engineering (VFPE) model [Keller and Teufel, 1998] (which is based on the extended EPC model) is further extended in order to formalize the concept of risk within business process models. In particular, this approach attempts to provide a syntax to represent risk in goal-oriented process models [Rotaru, Wilkin, Churilov and Neiger, 2008]. Their earlier work [Neiger, Churilov, zur Muehlen and Rosemann, 2006] also proposes a utility calculation technique that can be used to determine optimal risk countermeasure solutions.
This approach is not prescribed for any specific type of risk or for any specific domain. There is no evidence that this approach applies any existing risk analysis technique, nor does it attempt to conform to any risk standard.

This approach supports (+) the design stage criterion as it provides comprehensive constructs to enrich process models with risk-related constructs. The design-time analysis criterion is partially supported (±): while a risk analysis technique is proposed in their earlier work [Neiger, Churliov, zur Muehlen and Rosemann, 2006], there is no evidence that this technique is based on any well-accepted foundation/ theory. The rest of the BPM lifecycle stages are not addressed by this approach.

An ER diagram depicting the relationships between the proposed risk extension to the extended EPC constructs is provided. Furthermore, the structure of these constructs is also specified using set theory. Therefore, the abstract syntax criterion is supported. This approach also specifies the graphical representations of the proposed constructs, thus the concrete syntax criterion is also supported. This approach proposes several rules or constraints to formalize the notion of a risk-aware e-EP C model. These rules/constraints can be considered as the static semantics of the constructs [Meyer, 1990]. However, in our evaluation framework, we are mainly interested in the execution semantics of the constructs, which is absent in this approach. Thus, we consider the semantics criterion to be only partially supported. This approach has not been supported by an implementation (−). There is no support for the application methods criterion as there is a lack of guidelines to allow users to apply the approach. Finally, the application in practice criterion is also not supported as there is no evidence that this approach has been applied in the industry.

DI09 - Betz et al.

In Betz et al.’s work [Betz, Hickl and Oberweis, 2011], XML Nets [Lenz and Oberweis, 2003] - a variant of Petri Nets - are used to model risk-aware BPM systems. In this approach, a risk construct (representing a risk event) is proposed. These risk constructs are linked to a process’ activities. Then, risk countermeasure activities are explicitly captured, in the same process model, as sub-processes of the activities affected by the risk events. If there is more than one countermeasure activity that can be applied to address a particular risk event, several process models will be generated, each capturing a particular countermeasure activity. Through simulation, this approach then proposes a method to select the optimum process model variant based on process cost and flow time information.

This approach focuses on risk events that are caused by resources. However, mapping resource-based risk events to the risk taxonomy used in our evaluation framework can result in various types of risk. For example, a malfunctioning computer (a resource) can be mapped to the IT risk category in our risk taxonomy, while mistyped data by data entry personnel (also a resource) can be mapped to the data risk category in our risk taxonomy. Therefore, we do not consider this approach to be prescribed for a particular type of risk. Similarly, this approach does not seem to be developed specifically for any particular domain. There is no evidence that this approach attempts to conform with any particular risk standard nor does it attempt to apply any existing risk analysis technique.

In the context of the BPM lifecycle evaluation, this approach proposes a design-time annotation technique to enrich a process model with risk information. Furthermore, an approach to decide on the optimal process model that is guided by the risk countermeasure activities applied in the model is also proposed. In other words, this approach provides full-support (+) for the design stage as it facilitates a form of risk-informed business process design. This approach provides partial support (±) for the design-time analysis stage as the technique proposed is mainly based on simulation. The rest of the BPM lifecycle stages are not addressed by this approach.

A UML class diagram is provided to specify the structure of the risk event construct (hence, full support for the abstract syntax criterion). Similarly, a graphical notation representing the risk event construct is also specified (hence, full-support for the concrete syntax criterion). While this approach is based on XML Nets (a formal technique), there is no precise definition of the meaning (that is, the semantics) of the proposed risk construct. In fact, it is not clear whether the proposed risk construct actually exploits the existing semantics of XML Nets. Therefore, this approach does not support the semantics criterion. This approach fully supports the application methods criterion as it provides step-by-step application guidelines. This approach has also been supported by an implementation using the KIT-Horus business process modeling tool. This approach has not been validated in practice.

7 http://www.aifb.kit.edu/web/KIT-Horus/en
DI10 - Herrmann and Herrmann

Herrmann and Herrmann’s proposed approach [Herrmann and Herrmann, 2006] focuses on data security risks of business processes.

A set of graphical notations representing the security requirements of business processes is proposed. These security requirements then guide the evaluation of the security risk of the business processes (in terms of the non-satisfaction of the requirements). If the security risk is higher than a pre-defined tolerance level, a set of risk mitigation activities are added to the model as *risk treatment* such that the security risk of the processes can be reduced to an acceptable level.

This approach focuses on data security risk, although it is not prescribed for any specific domain. There is no evidence of the application of any existing risk analysis technique or any risk standard.

In the context of the BPM lifecycle evaluation, the *design* stage criterion is supported (+): this approach provides an annotation technique to express design-time security requirements of UML-based business processes, and a form of *risk-informed* business process design approach is also proposed (the results of the security risk evaluation guided by the annotated security requirements are used to guide the selection of risk mitigation activities to be applied in the processes). This approach also proposes a method to perform design-time risk evaluation using an evaluation matrix. However, the derivation of this evaluation matrix is not detailed. Therefore, the *design-time analysis* criterion is partially supported (±). The rest of the BPM lifecycle stages are not addressed by this approach.

The concrete syntax criterion is supported as a set of proposed graphical notations to depict security requirements. However, there is no clear specification of the key components or the structure of these notations, thus the abstract syntax criterion is not supported (−). The paper gives a short informal description of the use of a graphical rewrite system to specify how security requirement notations can be integrated into a process model. However, this graphical rewrite system does not define the meaning (or the semantics as defined in Section VI) of the security requirement notations. Hence, the semantics criterion is not supported. This approach is supported with an implementation, and there are detailed step-by-step instructions to guide users in the application of this approach (hence, a support for the application methods criterion). However, there is no evidence that this approach has been applied in practice.

DI11 - Strecker et al.

In Strecker et al.’s approach [Strecker, Heise and Frank, 2011], a multi-perspective risk modeling method for an IT infrastructure based on the Multi-Perspective Enterprise Modeling (MEMO) Meta Modeling Language (MML) [Frank, 2010], called RiskM, is proposed. In this approach, a risk modeling language (RiskML) that can be used to express risk-related information (such as the risk events, risk countermeasure activities, and risk propagation) is developed using the MEMO MML as the ‘conceptual foundation’ [Strecker, Heise and Frank, 2011]. The constructs proposed by this approach can then be used to add risk-related information to existing organizational models at different levels of granularity (strategic level, business process/operational level, and IT/infrastructure level).

The RiskM approach is not prescribed for any particular domain, although it does focus specifically on risks related to IT infrastructure. There is no evidence of the application of any existing risk analysis technique. Similarly, this approach does not attempt to address any particular risk standard.

The design stage criterion is supported (+) by this approach as it proposes a comprehensive set of constructs to capture intended risk information in a process model. The authors of this approach also suggest the possibility of performing a semi-automated transformation of the model into other visual representations. While the paper also explains approaches to *identify and evaluate risks* in a process model, they are brief and seem informal. Therefore, the *design-time analysis* stage criterion is partially supported (±). The rest of the BPM lifecycle stages are not addressed by this approach.

A meta-model of the proposed constructs (expressed in an UML class diagram) that describes the key attributes and components of the RiskML language is provided. The corresponding graphical notations representing the proposed constructs are also specified. Thus, the abstract syntax and concrete syntax criteria are supported. This does not specify the execution behavior of the proposed constructs in an unambiguous/precise manner. Therefore, the semantics criterion is not supported (−). There is no support for the implementation of this approach. Similarly, there is no support for the application in practice criterion as there is no evidence that the approach has been applied in real-world organizations. A high-level description on how this approach can be applied is provided, thus the application methods criterion is partially supported.
DI12 - Karagiannis et al.

Karagiannis et al.’s proposal [Karagiannis, Mylopoulos and Schwab, 2007] focuses on addressing the (non-)compliance risk of business processes to the SOX Act [107th Congress - USA, 2002] standard. This approach introduces several risk-related constructs to capture risk-related information. These constructs can then be used to annotate business process models with information related to the business processes’ risks. This approach also describes how risk annotation can inform the modification of the process model through the addition of control activities. A 6-step framework that can be used to realize a risk-aware business process management system is proposed.

This approach is mainly prescribed for the financial domain. The risk of regulation non-compliance addressed in this approach is a form of structural risk because it is mainly originated from the errors (such as wrong choices) committed during process design [Rosemann and zur Muehlen, 2005] that permit the non-compliant activities to occur (such as insufficient implementation of control activities in the process). This approach is clearly informed by a few risk-related standards, including the SOX and the Basel II standards. There is no evidence that this approach applies any existing risk analysis technique.

This approach supports (+) the design stage criterion as it proposes risk constructs that are sufficient to capture key risk information within a process model. Furthermore, this approach always proposes a form of risk-informed business process design in terms of how the annotated risk information guides the selection and enactment of control activities in a process. The design-time analysis criterion is partially supported (±) because while this approach supports the automated execution of test plans to analyze the effectiveness of the control activities used, the analysis method used is still simulation-based. The rest of the BPM lifecycle stages are not addressed by this approach.

This approach shows how the risk constructs can be represented/viewed in a process model, thus the concrete syntax criterion is supported. However, this approach does not detail the deep structure of these constructs (such as the key components and attributes of the constructs). Therefore, the abstract syntax criterion is not supported. Similarly, there is no clear and unambiguous definition of the meaning of the proposed constructs. It is not even clear if the risk constructs are somewhat ‘operated’ during simulation. Therefore, the semantics criterion is not supported. This approach has been supported with an implementation in the sense that it extends the ADONIS platform. This approach has also been adopted by an insurance company based in the United States, thus application in practice criterion is also supported. Similarly, the application methods criterion is also supported as a detailed 6-step application framework is provided.

DI13 - Taylor et al.

In Taylor et al.’s approach [Taylor, Godino and Majeed, 2008], a simulation environment is developed using the jBPM® stack and the jBPM Process Definition Language (JPDL). Several risk-related constructs, such as key risk indicator (KRI), key performance indicator (KPI), and risk event, are proposed. These constructs are used to annotate process models with risk information. Both qualitative measurement and quantitative measurement of KPI and KRI are supported. Through the application of simulation and fuzzy logic, the effects of risk events on some predefined KPIs and KRIs are evaluated.

This approach is not prescribed for any specific type of risk or for any particular domain. There is no evidence of the application of any existing risk analysis technique. Similarly, this approach is not informed by any risk standard.

In terms of the BPM lifecycle evaluation, the design stage criterion is supported (+) because the proposed constructs seem to be sufficient to capture the intended risk-related information (such as risk probability and impact). This approach introduces the use of simulation for the purpose of risk analysis; however, it is a simulation-based technique. Therefore, we consider the design-time analysis criterion to be partially supported.

This approach does support the abstract syntax criterion as it does not provide precise definition of the key components and/or attributes of the proposed constructs. The external representation (that is, the form) of the proposed constructs is only shown for a limited number of constructs. For example, the representation of the proposed risk event construct is shown as a graphical user interface whereby the name, probability, the affected task, and other attributes of a risk event can be displayed. However, the forms in which other constructs, such as the KRI and KPI constructs, can be represented are not specified. Thus, the concrete syntax criterion is partially supported (±). Similarly, while it is implied that the proposed constructs are somewhat exploited in the simulation
analysis, the precise definition of the meaning of these constructs and the operations that can be applied to them is not given. Hence, the *semantics* criterion is not supported (−). This approach has been implemented, hence the *implementation* criterion is supported. A high-level description of how to use this approach is also provided, hence, a partial evaluation is given to the *application methods* criterion. The *application in practice* criterion is not supported as there is no evidence that this approach has been implemented in practice.

**DI14 - Panayiotou et al.**

Panayiotou et al.'s approach [Panayiotou, Oikonomitsios, Athanasiadou and Gayialis, 2010] proposes an internal audit process as a method to perform risk assessment and to identify relevant risk mitigation actions for virtual enterprise networks. In particular, this approach proposes a technique to collect relevant information about processes in a structured manner such that it can be subsequently filtered and reported for the purpose of risk analysis. Relevant templates and tools (developed using the Sybase PowerDesigner enterprise modeling software) that can be used to aid the application of the proposed approach are provided. A number of risk-related constructs that can be used to annotate process models with risk-related information (such as risk mitigation activities) are also proposed.

This approach is mainly developed for the supply chain domain, although this approach is not prescribed for any particular type of risk. Similarly, there is no evidence of the application of any existing risk analysis technique. This approach is not informed by any relevant risk standard.

The BPM lifecycle activities supported by this approach mainly belong to the design stage and design-time analysis stage. The *design* stage criterion is partially supported (±) in that while risk constructs were proposed, they are not properly explained and detailed. This approach also provides a partial support for the *design-time analysis* criterion: it proposes a technique to perform risk evaluation during design-time, however, the proposed technique is informal.

The graphical representation of the proposed risk construct is shown in the approach, therefore the *concrete syntax* is supported (+). However, the deep structure of the proposed constructs (such as their attributes) is only informally described and there is no precise definition of the meaning of the proposed constructs. Thus, the *abstract syntax* and *semantics* criteria are not supported (−). This approach has been supported with an *implementation*. The *application methods* criterion is also supported as detailed guidelines of the application of this approach are provided (in the form of a 4-stage application methodology). While this approach may have been applied in practice [Panayiotou, Oikonomitsios, Athanasiadou and Gayialis, 2010], it is not clear if the ‘virtual enterprise’ to which this approach has been applied is an actual organization or a made-up example. Thus, we consider the *application in practice* criterion to be partially supported.

**DI15 - Lambert et al.**

In Lambert et al.'s work [Lambert, Jennings and Joshi, 2006], the Integrated Definition (IDEF) language [Federal Information Processing Standards, 1993] is used to model business processes and is extended to allow the concept of origin of risk to be included into the business process models. Several examples demonstrating the use of the proposed construct are shown.

This approach is not prescribed for any specific type of risk or for any particular domain. There is no evidence of the application of any existing risk analysis technique. Similarly, this approach is not informed by any risk standard.

The design stage of a BPM lifecycle is addressed in this approach by the proposal of a new risk construct to capture the concept of ‘risk source’. However, there is a lack of depth in the elaboration of the actual purpose and functionality of this new construct (especially in relation to how it affects the design of a process model). Therefore, the *design* stage criterion is only partially supported (±). There is no evidence that this approach attempts to address design-time risk analysis task, thus the *design-time analysis* criterion is not supported (−). The rest of the BPM lifecycle stages are not addressed by this approach.

The graphical representation of the proposed new construct is shown, thus the *concrete syntax* criterion is supported (+). While there is a short ‘formal’ specification about the structure of the construct, there is insufficient information conveyed by the specification. In other words, the *abstract syntax* criterion is not supported. There is also no precise definition given to the meaning of the proposed construct. Thus, the *semantics* criterion is also not supported. There is no evidence that this approach has been implemented (hence, no support for the *implementation* criterion). This approach provides a high-level guidance on how their approach can be applied, thus the *application methods* criterion is supported. This approach is claimed to have been applied in practice across three different industries. Hence, the *application in practice* criterion is also supported.
In Bai et al.’s work [Bai, Padman and Kirshnan, 2007] [Bagchi, Bai and Kalagnanam, 2006], business process models are represented as graphs (nodes representing tasks and arcs representing gateways). A precedence matrix is also used to capture process models’ topology. Process-related errors and error-mitigation activities are annotated in the corresponding error and control models proposed by this approach. These models are then used to reason about processes’ risks. This approach makes use of optimization techniques in order to determine the best place(s) in the workflow graph to place relevant error mitigating tasks. This approach applies several existing risk analysis techniques to evaluate risks by taking into consideration the probability of the occurrence of the risk events modeled, the consequences of the events, the propagation of the risk events, and the risk mitigation activities applied. The ultimate goal of the analysis is to ensure that an optimal placement of risk mitigation activities is achieved.

This approach applies existing risk analysis techniques, such as the Conditional Value-at-Risk technique [Rockafellar and Uryasev, 2000]. This approach is not prescribed for any particular type of risk or domain. Furthermore, there is no evidence that this approach is informed by any existing risk standard.

This approach provides a partial (±) support for the design stage of a BPM lifecycle. A comprehensive set of risk-related models (namely the error and control models) is proposed. However, a drawback of this approach is that it is not evident that the precedence matrix used in the approach is able to capture complex process model topology (such as XOR-split or OR-join). Consequently, it is unlikely that one can study business processes’ risks in a more realistic and complex process model. Nevertheless, the risk analysis techniques proposed in this approach are worthy of consideration, formal, and comprehensive (hence, a full-support (+) for the design-time analysis criterion). The rest of the BPM lifecycle stages are not addressed by this approach.

The structure of the proposed concepts is defined as a set of purely mathematical equations, thus facilitating a precise and unambiguous definition of the structure of the concepts. In other words, the abstract syntax criterion is fully supported. However, there is no support for concrete syntax in the form of graphical symbols or vocabulary to give the ‘forms’ in which the concepts can be represented externally. This approach also does not provide a precise specification of the meaning of the proposed constructs, thus no-support (−) for the semantics criterion. A high-level description of how this approach can be applied is provided, thus the application methods criterion is partially supported. This approach is not supported by an implementation and it has not been applied in practice (it uses a made-up case study).

APPENDIX D

This section provides a detailed evaluation of all surveyed approaches which address design-time R-BPM without using any risk-related constructs. The evaluation results are summarized in Table 5.

In this work [Bhuiyan, Islam, Koliadis, Krishna and Ghose, 2007] [Islam, Bhuiyan, Krishna and Ghose, 2009], a technique to quantify the criticality and vulnerability of actors in a business process is proposed. This is achieved by analyzing the incoming and outgoing edges of actors in an actor dependency model represented using the J* framework notations.10 The results of this analysis are then used to inform the design of the corresponding BPMN-based business process models in order to reduce/mitigate the negative consequences resulting from the failure/unavailability of critical actors. Therefore, a form of risk-informed business process design is also proposed.

This approach is developed mainly to address organizational risk based on Rosemann and zur Muehlen’s taxonomy [Rosemann and zur Muehlen, 2005]. This approach is not prescribed for any particular domain. There is no application of any existing risk analysis technique or any risk standard.

This approach provides partial support (±) for the design stage and design-time analysis stage criteria. As explained earlier, a type of risk analysis technique (namely, the resource criticality analysis) is proposed. However, it is an incomplete analysis technique in the sense that it mainly focuses on quantifying the impact of a resource failure event; how one can calculate the occurrence probability of the related resource failure event is not addressed by this approach. Similarly, this approach also supports a form of risk-informed business process design; however, there is a lack of details in terms of how the results of resources criticality analysis should precisely guide the design of a process model.

http://www.cs.toronto.edu/km/istar/
This approach does not propose any new risk-related constructs, therefore the abstract syntax, the concrete syntax, and the semantics criteria are not applicable (N/A). There is no implementation support for this approach, nor is there any support for application methods criterion since the approach does not provide any application instructions or guidelines. The application in practice criterion is partially supported, as the approach has been empirically evaluated in a workshop setting.

DN02 - Fenz et al.

In Fenz et al.’s approach [Fenz, 2010] [Fenz and Ekelhart, 2009] [Fenz, Ekelhart and Neubauer, 2009] [Fenz and Neubauer, 2009], a number of techniques that can be used to analyze a business process’ risks are proposed. In particular, this approach proposes techniques to analyze the consequences of a risk event, the occurrence probability of a risk event, the propagation of risk events, and the overall risk level of a business process. The consequence analysis of a risk event is achieved through the application of the ‘resource importance’ calculation. The formula used in the calculation is derived from the structure of the Petri-nets model in which the corresponding business process is depicted. The analysis of the occurrence probability of a risk event (and the propagation of risk events) is achieved through the application of a Bayesian network analysis. The development of the Bayesian network is based on the security ontology proposed by the same authors (expressed using Web Ontology Language (OWL) [W3C, 2004]). This ontology contains concepts related to information security and risk, such as vulnerabilities, threats, and countermeasures.

This approach mainly considers risk from the resources’ (such as IT assets) point of view. In other words, this approach addresses the ‘IT risk’ based on the risk taxonomy [Rosemann and zur Muehlen, 2005] used in our evaluation framework. This approach is mainly prescribed for the IT infrastructure domain as suggested by the case study used in the empirical assessment. This approach is somewhat influenced by the NIST 800-30 recommendations (risk management for IT systems), therefore the risk standards criterion is partially supported (±). The risk analysis criterion is supported as this approach applies the existing Bayesian network analysis technique to analyze the occurrence probability of risk events.

In terms of the BPM lifecycle evaluation, the design stage criterion is not supported (−) as there is no proposal of risk-related constructs or any form of risk-informed business process design guidelines. The design-time analysis stage is, however, fully supported (+) as it provides a comprehensive set of risk analysis techniques that are informed by well-established technical foundations (such as Petri nets, Bayesian network, and OWL-based ontology). The rest of the BPM lifecycle stages are not addressed by this approach.

The abstract syntax, the concrete syntax, and the semantics criteria are not applicable (N/A) as this approach does not introduce any new integrated risk-related constructs. A proof-of-concept implementation of this approach is provided, thus the implementation criterion is partially supported (±). This approach has also been validated through a workshop-based empirical assessment, thus the application in practice criterion is partially supported. Finally, there are no guidelines provided in terms of the application of this approach. Thus, the application methods criterion is not supported.

DN03 - zur Muehlen et al.

In zur Muehlen et al.’s work [zur Muehlen, Baumgart and Junkers, 2006], a taxonomy of faults related to process elements (such as data, technology, and organization) is proposed. A pseudo-algorithm (informed by the proposed taxonomy) to identify risks in a business process model is also proposed.

This approach is not prescribed for any particular type of risk or any domain. There is no evidence that this approach is informed by any risk standard. The approach is somewhat influenced by the Failure Modes, Effects, and Criticality Analysis (FMECA) [US Department of Defense, 1949] risk analysis technique.

This approach provides partial support (±) for the design-time analysis criterion as it proposes a form of risk identification technique. Nevertheless, there is a lack of thoroughness in the proposed algorithm in the sense that it does not clearly demonstrate the use of any well-acceptable theory/techniques as the foundations from which the algorithm is built. While the FMECA technique is alluded to in the literature, the link between the FMECA technique and the proposed algorithm is not evident. This approach does not propose any new risk-related constructs nor does it introduce any risk-informed business process design guidelines/principles. Consequently, the design stage criterion is not supported (−). The rest of the BPM lifecycle stages are not addressed by this approach.

The abstract syntax, the concrete syntax, and the semantics criteria are not applicable (N/A) as this approach does not introduce any new integrated risk-related constructs. This approach has not been supported with an implementation. The application methods criterion is partially supported as a high-level guidance on the application
of this approach is provided. This approach has been evaluated in practice through its application in a real-world university payroll process. Therefore, the application in practice criterion is supported (+).

**DN04 - Kaegi et al.**

In Kaegi et al.’s approach [Kaegi, Mock, Ziegler and Nibali, 2006], process models described in BPMN are simulated via an agent-based modeling technique to analyze business process-related risks. A risk estimation formula, proposed by the same approach, is also used in the analysis of process’ risks.

There is no evidence to suggest that this approach is prescribed for any particular type of risk or domain. Similarly, there is no evidence that this approach is informed by any risk standard. There is also no application of any existing risk analysis technique in this approach.

In terms of the BPM lifecycle evaluation, the agent simulation approach and the proposed risk calculation formula are considered design-time risk analysis support. However, due to the lack of clarity in the presentation of this approach, we consider the design-time analysis stage criterion to be only partially supported (±). This approach does not propose any new risk-related construct or any risk-informed business process design guidelines/principles. Therefore, the design stage criterion is not supported (−). The rest of the BPM lifecycle stages are not addressed by this approach.

The abstract syntax, the concrete syntax, and the semantics criteria are not applicable (N/A) as this approach does not introduce any new integrated risk-related constructs. This approach has not been supported with an implementation. The application in practice criterion is also not supported as it has not been validated in practice. Similarly, the application methods criterion is also not supported as there is a lack of description of methods/guidelines through which this approach can be applied.

**DN05 - Bergholtz et al.**

In Bergholtz et al.’s work [Bergholtz, Grégoire, Johannesson, Schmitt, Wohed et al., 2005] [Andersson, Bergholtz, Edirisuriya, Ilayperuma and Johannesson, 2005] [Schmitt, Grégoire and Dubois, 2005], an approach to facilitate risk-informed business process design (driven by risk treatment activities) is detailed. Their approach starts with a business model (described using Business Model Ontology (BMO) [Osterwalder, 2004] language which is then transformed into a value-web model (described using the e²-value model notation [Gordijn, Yu and van der Raadt, 2006]). Then, through the aid of the corresponding activity-dependency diagram, the value-web model is then transformed into a BPMN-based process model. At each stage of the model transformation, the approach suggests the determination of risk events that may occur in the model being studied, and the modification of the model such that relevant risk mitigation activities are integrated into the final (derived) business process model. In other words, the end product of such a process is a risk-informed business process model which already contains relevant risk mitigation activities.

This approach is generic enough to be applied to any domain. There is no evidence that this approach is prescribed for any specific type of risk. Similarly, this approach does not apply any existing risk analysis technique nor is it informed by any existing risk standard.

In terms of the BPM lifecycle evaluation, this approach provides a full-support (+) for the design stage as it facilitates a risk-informed business process design. However, this approach does not support any design-time risk analysis. The rest of the BPM lifecycle stages are not addressed by this approach.

As with other approaches evaluated in this section, there is no new integrated risk construct proposed. Therefore, the abstract syntax, concrete syntax, and semantics criteria are not applicable (N/A). There is no implementation support provided by this approach. The application in practice criterion is also not supported as this approach has not been applied in real-world organizations. There is a partial support (±) for the application methods criterion through the provision of high-level application guidance.

**DN06 - Jallow et al.**

In Jallow et al.’s work [Jallow, Majeed, Vergidis, Tiwari and Roy, 2007], an approach to analyze risks in business processes is proposed. Given a set of identified risk events and their occurrence probabilities, a Monte Carlo

---

11 Note, however, that this approach does provide a risk-enriched chaining ontology which links the modeling concepts that exist in a business model to those in a value web model.
simulation [Metropolis, 1987] is applied to assess and quantify the impact/consequences of those risk events (in terms of time, cost, performance, and other objectives) on each process activity and on overall process.

This approach is developed to address ‘operational’ risks in business processes. However, by studying the examples of ‘operational’ risks used in the literature, we see that an ‘operational’ risk can be mapped to many types of risk according to the risk taxonomy used in our evaluation framework. For example, the risk of inadequate expertise alluded in the literature can be mapped to the ‘organizational risk’ category in our taxonomy; the IT equipment risk mentioned in the literature can be mapped to the ‘IT risk’ category in our taxonomy. Consequently, we consider this approach to be generic enough to be applicable to many types of risk. Similarly, there is also no evidence that this approach is specific to any domain. This approach is informed by the COSO framework [COSO, 2004] and it applies an existing risk analysis standard (the Monte Carlo simulation).

In terms of the BPM lifecycle evaluation, this work addresses the design-time analysis stage (also see Table 2). However, while this approach applies a well-accepted risk analysis technique, it only addresses one dimension of risk analysis (the impact analysis). Therefore, the design-time analysis stage criterion is partially supported (±). This approach does not propose any new risk-related construct nor does it propose any risk-informed business process design guidelines. Thus, the design stage criterion is not supported (−). The rest of the BPM lifecycle stages are not addressed by this approach.

The abstract syntax, the concrete syntax, and the semantics criteria are not applicable (N/A) as this approach does not introduce any new integrated risk-related constructs. This approach is supported with an implementation in the sense that it uses existing software (such as Crystal Ball with Microsoft Excel) to aid the analysis. However, this approach does not support the application methods criterion as there is no description of the methods through which it can be applied. Similarly, the application in practice criterion is not supported as it has not been validated in practice.

**DN07 - Singh et al.**

In Singh et al.’s approach [Singh, Gelgi, Davulcu, Yau and Mukhopadhyay, 2008], a technique to evaluate a workflow’s non-completion risk due to uncertain/dynamic information is proposed. In the literature, the term ‘non-monotonic predicate’ is used to refer to such information. Examples of non-monotonic predicates include the number of injured passenger(s) in a car accident, or the status of traffic condition at the time of the accident. This information is not likely to be known until runtime. A method to quantify the confidence level of the non-monotonic predicates of a workflow is also proposed. When the confidence level of a non-monotonic predicate of a workflow is below a certain threshold, the workflow is considered to be risky. In this situation, this approach suggests the use of a backup workflow such that the non-completion risk of the related workflow instance is mitigated. An approach to generate a backup workflow based on workflow execution history is also briefly described.

The type of risk addressed by this approach is the structural risk (based on the risk taxonomy used in our evaluation framework) because it looks at how the design of a workflow may become ineffective in attaining some desired goals [Rosemann and zur Muehlen, 2005] due to non-monotonic predicates. This approach uses an accident response scenario for illustration; however, the techniques proposed seem to be generic enough to be applicable to other domains. There is no evidence that this approach applies any existing risk analysis technique. Similarly, this approach is not informed by any existing risk standard.

In terms of the BPM lifecycle evaluation, this approach provides partial support (±) for the design-time analysis criterion: it proposes a form of risk calculation technique; however, the proposed risk calculation uses a separate formula for each type of control flow (unconditional workflow, alternative workflow, conditional workflow, and parallel workflow). It is not clear how the risk of a workflow which contains a combination of control flows can be calculated. This approach also describes a technique to generate a backup workflow based on historical data (thus providing a form of risk-informed business process design). However, the details of this technique are missing in the literature. Thus, the design stage criterion is also partially supported. Unlike other approaches considered in this section, this approach claims to allow the runtime generation of a backup workflow which is constantly monitored to ensure consistency with the main workflow. Any inconsistencies between the generated backup workflow and the current running process instance will trigger the re-generation of the backup workflow. However, there is a lack of detail of how such monitoring can be performed. Consequently, we consider the runtime analysis criterion to be only partially supported. This approach does not address the execution stage and the post-execution stage of the BPM lifecycle.

The abstract syntax, the concrete syntax, and the semantics criteria are not applicable (N/A) as this approach does not introduce any new integrated risk-related constructs. There is no evidence that this approach has been implemented, nor is there evidence that it has been applied in practice. Hence, the implementation and application in
**practice** criteria are not supported (−). Similarly, there is no description of any methods through which this approach can be applied. Therefore, the **application methods** criterion is also not supported.

**APPENDIX E**

This section provides a detailed evaluation of all surveyed approaches which address **runtime** R-BPM. The evaluation results are summarized in Table 6.

**RT01 - Conforti et al.**

In Conforti et al.’s work [Conforti, Fortino, La Rosa and ter Hofstede, 2011], a language which can be used to annotate a process model with risk conditions is proposed. These risk conditions draw information from both current running process instances and historical data such that the occurrence probability of the related risk events can be estimated. These annotations can be executed and monitored during runtime. When a risk condition is fulfilled, relevant alert(s) are triggered to notify users of the existence of the risky process instance.

The language proposed allows conditions related to organizational risk (e.g. the role of the resource working on a task), structural risk (e.g. the total repetition of a particular task), and data risk (e.g. the size of an order) to be specified. This approach is generic enough to be applicable to any domain. While there is no evidence that this approach is informed by any existing risk standard. Similarly, there is no application of any existing risk standard. It does apply an existing risk analysis technique, namely a fault-tree analysis.

In terms of the BPM lifecycle evaluation, the **design** stage criterion is fully supported (+) as it allows the execution of risk-annotated process models. This approach also supports a form of runtime risk analysis through the evaluation of risk conditions and the generation of risk alerts at runtime. The annotation of process models with risk conditions is a design stage activity. However, the language proposed is runtime-oriented: the notations per se only provide limited insights of business processes’ risks at design time. Thus, the **design** stage criterion is only partially supported (±). This approach does not address the design-time analysis and the post-execution analysis stages of the BPM lifecycle.

The structure/grammar of the proposed language (in other words, the abstract syntax of the language) is detailed using Meyer’s abstract syntax notation [Meyer, 1990]. Therefore, the **abstract syntax** criterion is supported (+). The representation of this language in the form of code-like statements is also specified; thus, the **concrete syntax** criterion is also supported. The definition of the execution behavior of the proposed constructs is described using natural language, thus the **semantics** criterion is not supported (−). The **implementation** criterion is supported as the proposed language and the related runtime risk monitoring capability have been implemented into the YAWL workflow system [van der Aalst, Adams, ter Hofstede and Russell, 2010]. This approach has been partially (±) validated in practice in the sense that experiments aimed at evaluating the performance of the approach have been conducted. Furthermore, the process model used in the experiments was developed following an industry standard, namely the Voluntary Inter-industry Commerce Standard (VICS). The **application in practice** criterion is not supported (−) as this approach has not been applied in real-world organizations. A detailed step-by-step tutorial explaining the application of this approach is provided, thus the **application methods** criterion is supported.13

**RT02 - Kang et al.**

In Kang et al.’s work [Kang, Cho and Kang, 2009], a technique to estimate the probability of a process instance entering an abnormal termination state is proposed. Process-related historical data is used to inform the probability estimation calculation. Then, a runtime risk estimation algorithm is developed such that appropriate risk alerts can be produced when risky situations are detected.

This approach does not seem to be prescribed for any specific type of risk. It is also generic enough to be applicable to any domain. There is no evidence that this approach is informed by any existing risk standard. Similarly, there is no application of any existing risk analysis technique in this approach.

In terms of the BPM lifecycle evaluation, this approach supports (+) the **runtime analysis** criterion through the proposal of a runtime risk monitoring technique. The **execution** criterion is not supported (−) as it does not propose

---

12 It may be argued that due to the relatively ‘simple’ constructs proposed in Conforti et al.’s work, using natural language to define the execution semantics of the constructs is sufficient; however, to ensure consistency with our evaluation framework, we have to provide a negative evaluation for the **semantics** criterion.

13 The tutorial is available at [http://www.yawlfoundation.org/sensor/index2.html](http://www.yawlfoundation.org/sensor/index2.html).
any new risk-related constructs that are executable, or any risk-informed business process execution guidelines/principles. The rest of the BPM lifecycle stages are not addressed by this approach.

Since there is no new risk constructs being introduced by this approach, the abstract syntax, concrete syntax, and semantics criteria are not applicable (N/A). A prototype implementation of this approach is provided, hence, the implementation criterion is partially supported (+). While some experiments using the prototype implementation have been carried out, this approach has not been tested in any real-world organizational settings. Therefore, the application in practice criterion is not supported (−). A high-level description of the methods through which this approach can be applied is provided, thus the application methods criterion is partially supported.

APPENDIX F

This section provides a detailed evaluation of all surveyed approaches which address the monitoring and controlling stage of an R-BPM. The evaluation results are summarized in Table 6.

PE01 - Jans et al.

In Jans et al’s work [Jans, van der Werf, Lybaert and Vanhoof, 2011] [Jans, Lybaert, Vanhoof and van der Werf, 2008] [Jans, Depaire and Vanhoof, 2011], business processes’ logs are analyzed such that risks related to financial fraud can be identified and the occurrence probability of those risks can be estimated. In particular, the ProM tool¹⁴ is used to aid the reasoning about the inadequacy of internal controls and the estimation of the likelihood of a user subverting existing processes such that transaction fraud can be committed. Interesting fraud-related properties, such as segregation of duty, were verified using the logs. This approach managed to uncover suspicious process instances which were not detected during traditional internal audit process [Jans, Depaire and Vanhoof, 2011].

This approach mainly addresses risks related to finance domain. The type of risk addressed is mainly the structural risk as this approach attempts to discover loopholes in the design of a process which may permit the occurrence of financial frauds. Nevertheless, this approach does not apply any existing risk analysis technique. It is also not informed by any risk standard.

In terms of the BPM lifecycle evaluation, this approach supports (+) the post-execution stage as evidenced by the use of logs from business processes in the analysis of fraud-related risks. The rest of the BPM lifecycle stages are not addressed.

This approach attempts to analyze existing process logs without the introduction of any new risk-related constructs, thus the abstract syntax, concrete syntax, and semantics criteria are not applicable (N/A). This approach supports an implementation in the sense that it exploits an existing process mining tool (ProM) [van Dongen, de Medeiros, Verbeek, Weijters and van der Aalst, 2005]. Similarly, this approach also follows a clear application methodology as necessary to apply the ProM tool. Therefore, the application methods criterion is supported. Finally, the application in practice criterion is also supported as it has been applied in practice: two applications in procurement/finance domain.

PE02 - Wickboldt et al.

In Wickboldt et al’s approach [Wickboldt, Bianchin, Lunardi, Granville, Gaspary et al., 2011], historical information (such as logs) from business processes is annotated with a number of risk-related constructs such that various types of risk analysis can be conducted. In particular, techniques to identify and evaluate risks in business processes (including risk probability estimation and impact analysis) are proposed.

This approach is mainly applied in the domain of IT systems, although the type of risk addressed is quite generic. This approach is strongly influenced by a number of risk management standard, such as the Management of Risk (M_o_R) standard [Office of Government Commerce, 2007]. This approach does not apply any existing risk analysis technique.

In terms of the BPM lifecycle evaluation, this approach supports (+) the post-execution stage because it proposes methods to reason about risks by focusing on the use of logs from business processes that have been annotated with risk-related information. The rest of the BPM lifecycle stages are not addressed.

¹⁴ http://www.promtools.org/prom6/
This approach introduces new risk-related constructs which are used to enrich the process logs. The structure and the attributes of the proposed constructs are specified using the Common Information Model (CIM) technique. Thus, the abstract syntax criterion is supported. Nevertheless, there is no specification of how these constructs are represented in the log. Therefore, the concrete syntax criterion is not supported. Similarly, this approach does not provide precise definition of the meanings of the proposed constructs, thus the semantics criterion not supported (−). This approach has been supported with an implementation. However, it is not evident that this approach has been applied in practice. Hence, the application in practice criterion is not supported. There is a high-level description of the methods through which this approach can be applied, thus the application methods criterion is partially supported (±).

15 http://dmtf.org/standards/cim
16 This approach has been evaluated on the CHANGELEDGE system [da Costa Cordeiro, Machado, Andreis, dos Santos, Both et al., 2009] [da Costa Cordeiro, Machado, Andreis, dos Santos, Both et al., 2009] [da Costa Cordeiro, Machado, Andreis, dos Santos, Both et al., 2009] which is an industry-funded research project; however, it is not considered a proper ‘real-world’ system according to our evaluation criteria.