Communications of the Association for Information Systems

CAIS

Current Research in Risk-aware Business Process Management—Overview, Comparison, and Gap Analysis

Suriadi Suriadi

Queensland University of Technology, Brisbane, Australia

s.suriadi@qut.edu.au

Burkhard Weiß, Axel Winkelmann

European Research Center for Information Systems, Münster, Germany

Arthur H.M. ter Hofstede

Queensland University of Technology, Brisbane, Australia

Eindhoven University of Technology, Eindhoven, The Netherlands

Michael Adams, Raffaele Conforti, Colin Fidge, Marcello La Rosa, Chun Ouyang, Anastasiia Pika, Michael Rosemann, Moe Wynn

Queensland University of Technology, Brisbane, Australia

Abstract:

The management of risk in business processes has been the subject of active research in the past few years. Potentially, many benefits can 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 scope, goals, and functionality. Through the systematic collection and evaluation of relevant literature, this article 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

Volume 34, Article x, pp. xx-xx, January 2014

The manuscript was received 08/23/2012 and was with the authors 4 months for 1 revision.

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 [ter Hofstede, van der Aalst, Adams, 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 market share movements, which may have a profound impact on organizational objectives. These uncertainties and their impact on organizations are known commonly 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 known commonly as *risk management* [Standards Australia and Standards New Zealand, 2009].

A number of recent financial scandals, such as the $US2.3bn UBS rogue trading scandal in 2011 [Howley and Thomasson, 2011] and the €4.9bn 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 [Treanor, 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, and Quirchmayr [2011]. The importance of this research also has 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 reasoning about and management of risks in business processes, a *risk-aware business process management (R-BPM) system*. Many benefits potentially can be obtained by integrating the two traditionally separated fields of risk management and BPM, including the ability to analyze risks and incorporate risk mitigation strategies into a business process model during design time [Goluch, Ekelhart, Fenz, Jakoubi, Tjoa, and Mück, 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, 2011b]. Furthermore, an integrated R-BPM system also may 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 delivering an R-BPM system 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) and the various levels at which risk management can be incorporated into the realm of business process management. Furthermore, the proliferation of underlying business process modeling approaches and automation tools, each with differing degrees of formalization [ter Hofstede et al., 2010], also adds to the variety of forms in which an R-BPM system can be manifested. To date, there has not been a systematic study investigating the state-of-the-art in this area.

The main contribution of this article 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 that have been well-studied (if any) and those that have not received much attention, but still need to be properly studied.

Through a systematic collection of literature, we identified ninety-six papers deemed relevant, out of a pool of over 20,000 papers. Research gaps in the area of R-BPM then were 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 which are illustrated in this article.

This article 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 article. 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 has been widely adopted in today's organizations [Dixon, 2011; Dixon and Jones, 2011; Vollmer et al., 2008; Gengler, 2008]. 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 to monitor and control their execution [Dumas, La Rosa, Mendling, and Reijers, 2013]. A business process typically involves different organizational aspects, ranging from human resources to business documents and technology.

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 [ter Hofstede et al., 2010; Dumas, van der Aalst, and ter Hofstede, 2005; Dumas et al., 2013], they consist of the following stages: *design, design-time analysis*, *execution*, *runtime 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 typically are 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, and technology. 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 the *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 then is monitored and analyzed in real-time during the *runtime 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 also can 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, of course, can be used as feedback to the *design* stage, again to enable further process improvement. Note that in certain literature, e.g., Dumas et al. [2013], the *runtime analysis* and *post-execution analysis* stages are referred to as the *monitoring and controlling stage.*

Unfortunately, traditional BPM systems operate *separately* from the domain of risk management [Conforti et al., 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 manage these risks directly as an *integral* part of their process execution, rather than as separate activities or as an afterthought. 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 provide support for enacting necessary risk mitigation actions. During run time, the emergence of risks should be constantly monitored. Once a risk event has occurred, it should be mitigated immediately to ensure a proper termination of the process. The logs produced from the execution of business processes also should 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 still are 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 the later approaches are indeed an evolution of one or more earlier approaches by the same authors), they are grouped together. A collection of similar approaches is also called an approach. In the remainder of this article, the term *approach,* thus, should be interpreted as a collection of similar approaches based on the criteria explained above.

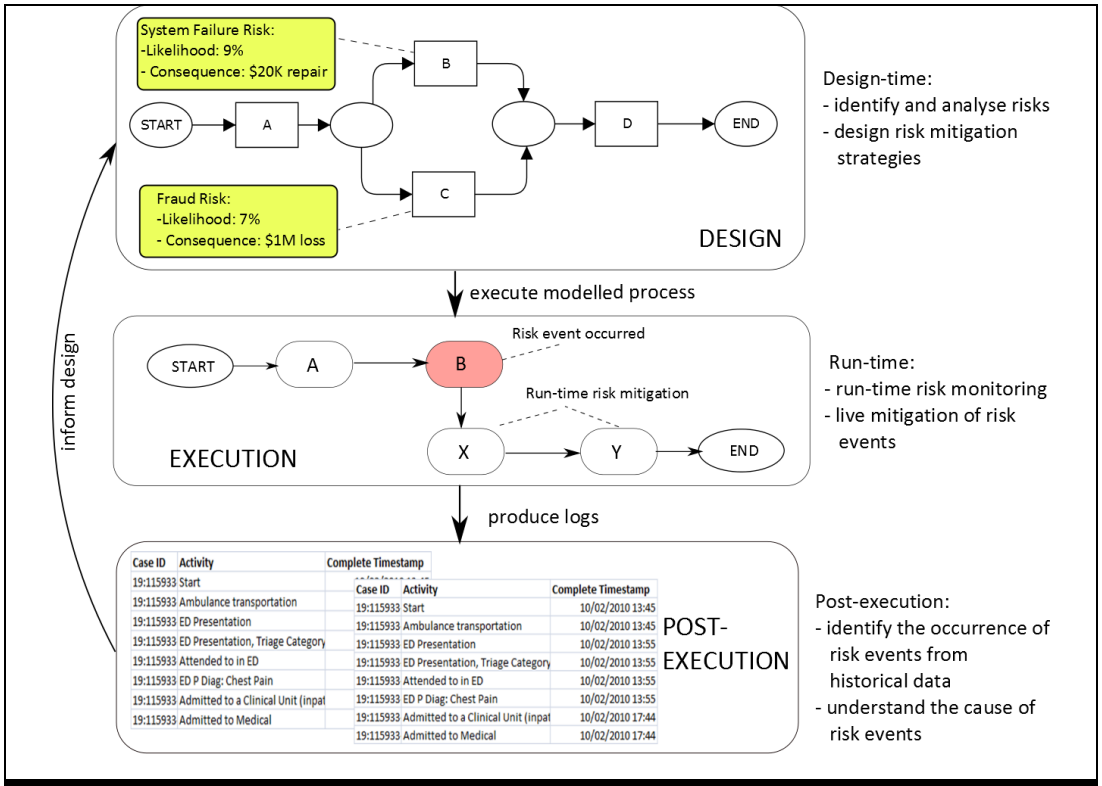

Figure 1. R-BPM in the Context of a BPM Lifecycle

III. RELATED WORK

To our knowledge, there has been only 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, 2009a]. 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 et al., 2006].

While the literature reviews just mentioned are related closely to ours, the scope differs. Jakoubi et al. [2009a] considered research papers that focus on both the issue of "security in BPM" and the issue of "risk in BPM." Similarly, the scope of Rikhardsson et al.'s [2006] literature review is also broader as it includes research papers in the area of compliance and internal control as well as risk management. In our case, however, we focus on only papers which explicitly try to reason about "risk in BPM." Carnaghan [2006] looked into the extent to which existing business process model constructs support audit risk assessment. 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. Those papers that *did meet* our selection criteria were subsequently grouped into a set of "approaches" and evaluated using the evaluation framework detailed in Section VI.

As a general rule, we consider only those papers which specifically attempt to integrate and/or reason about risks *in* business process management systems. Therefore, those papers that 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 [Lund, Solhaug, and Stolen, 2011]; the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management framework [COSO, 2004]; Cheng, Sadiq, and Indulska's [2011] work; and Iida, Denker, and Talcott's [2009] work.

Similarly, those papers that 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 [2007] and Salmela [2007].

We also excluded those papers whose main focus is on the topic of *business process-based risk management*, such as the following work: Sackmann [2008]; Cha, Liu, and Yu [2009]; Taubenberger and Jürjens [2008]; and Yu [2011]. While these papers may seem relevant, they are concerned more with the issue of risk management than with business process management—business processes are used merely 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 also are excluded in our literature review, as they are unlikely to be accessible to the whole scientific community due to language barriers. Examples of papers in this category are Brabänder and Ochs [2002]; Hengmith [2005]; Rieke and Winkelmann [2008]; and Rieke [2009].

The need for organizations to comply with legislative regulations has highlighted the need to address risks of regulatory noncompliance. Consequently, research in business process compliance increasingly has been 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 and the impacts of the occurrence of various types of risks, one of which is the risk of business processes violating some legislative regulations. Our literature is concerned with the latter, and, thus, we have excluded many papers in the area of business process compliance which do not demonstrate any strong links to the concept of risk, such as 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]; and 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 that attempt to facilitate the reasoning about security risks in business process management systems, rather than those that attempt to provide solutions to security management problems. Thus, a large number of papers concerning security management were excluded: Rodríguez, Fernández-Medina, and Piattini [2007, 2006b, 2006a]; Wolter and Schaad [2007]; Wainer, Kumar, and Barthelmess [2007]; Neubauer and Heurix [2008]; Neubauer, Klemen, and Biffl [2005, 2006]; Neubauer and Pehn [2010]; Wang and Li [2007]; Xiangpeng, Cerone, and Krishnan [2006]; Rodríguez, García-Rodríguez de Guzmán, Fernández-Medina, and Piattini [2010]; Montagut and Molva [2007]; Ayed, Cuppens-Boulahia, and Cuppens [2009]; and Aziz, Arenas, Martinelli, Matteucci, and Mori [2008].

We have excluded also zur Muehlen and Ho's [2005] paper: while this paper, at first, may 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, thus, is excluded.

Finally, we did 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]; and 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, Plattfaut, Cleven, 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 [1988]) taxonomy: 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 three well-known scholarly-article search engines, i.e., Google Scholar, Scopus, and Web of Science. To maximize the inclusiveness of our search, at this stage, any papers 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, as part of the second stage of the literature collection procedure, we also undertook a "backward reference" search 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) was searched systematically to select papers related to the topic of risk in business process management from the 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 based solely 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 classification,[1] 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 in 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 three popular scholarly-article databases: Google Scholar, Scopus, and Web of Science. These databases were selected because they are well-known sources of citations.[2] For each database, we conducted two search iterations (except for Google scholar, where three iterations were performed). Each iteration was conducted *"from the scratch*," that is, against the whole database, *instead of* the search results from the previous iteration. The search criteria used are as follows:

[1] www.arc.gov.au/xls/era2010_journal_title_list.xls

[2] 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 the three databases mentioned above (Google Scholar, Scopus, and Web of Science).

- 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)

Further engine-specific filtering rules were applied:

- Google Scholar:
  - Searches were performed within one-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 displayed only the first 1000 results).
  - 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 2005 and 2011.
  - We restricted our search to the following subject fields: *“Engineering,” “Computer Science,” “Mathematics,” “Decision Science,” “Business, Management, and Accounting,” “Economics, Econometrics, and Finance,” and “Multidisciplinary.”*
- Web of Science:
  - Searches were conducted for papers published between 2005 and 2011.
  - We restricted the search to the following subject fields: *“Economics,” “Computer Science Information Systems,” “Computer Science Theory Methods,” “Computer Science Interdisciplinary Applications,” “Computer Science Software Engineering,” “Computer Science Mathematical Methods,” “Business,” “Business Finance,” “Engineering Electrical Electronics,” “Engineering Industrial,” “Multidisciplinary Sciences,” and “Management.”*

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, seventeen 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 consider only 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 eleven papers).

At the end, we had ninety-six 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 thirty-three papers were deemed to be outside the scope for final evaluation, leaving sixty papers for thorough review and evaluation (see Section VII).

VI. LITERATURE EVALUATION FRAMEWORK

In this article, 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 also is explained.

Our evaluation framework is influenced mainly 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 et al., 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 article 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 [ter Hofstede et al., 2010]: the first two stages of our BPM lifecycle correspond to the *process (re)design and analysis* 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.[3] Based on these five stages, we define the following evaluation criteria. For evaluation purposes, 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, refer to Appendix B.

Design

Does the approach propose modeling 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 recorded from 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 et al., 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" also can be assigned if a particular criterion is not applicable to the approach being evaluated (see Appendix B for a detailed explanation).

Integrated Risk Formalization

Does the approach propose novel constructs to capture risk-related information such that we can reason about risk *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 et al., 2004]. The former states that design science research produces artifacts 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 about risks within a process 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 et

[3] In the BPM lifecycle model proposed in ter Hofstede et al. [2010], there is also another stage, called the *system configuration* stage, which sits between the *process (re)design and analysis* stage and the *process enactment and monitoring*. This stage is about the implementation and configuration of a BPM system; thus, it is considered as part of the *maturity* evaluation criteria.

al., 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"[4] 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 class diagrams [OMG, 2011a; OMG, 2011b]) or a grammar (such as the Metanot grammar [Meyer, 1990]). For example, the abstract syntax of a construct representing a *risk event* can be expressed as UML class diagram(s), 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 article 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, on the other hand, is used to indicate not only the maturity of the proposed constructs (in terms of the clarity 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, 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 supported somewhat 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 et al., 2004]. In particular, we are interested if there is an *instantiation* 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 et al., 2004] and the artifact we are interested in this evaluation criterion is of type *method*.

[4] This term is borrowed from Meyer [Meyer, 1990].

Application in Practice

Has the proposed approach been applied and validated in practice? This evaluation criterion is informed by the *design evaluation* guideline [Hevner et al., 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 also may 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 [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?

Risk Standards

By which risk standards (such as the Sarbanes-Oxley and Basel II standards), if any, have the R-BPM approaches evaluated in this article 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 ninety-six papers deemed suitable for evaluation. However, through a detailed evaluation process, thirty-three out of those ninety-six papers were considered borderline papers which were outside the scope of our literature review (as detailed in Section IV). Therefore, we excluded them. Furthermore, three out of those ninety-six papers were actually "related work" papers already discussed in Section III. The remaining sixty papers were then further grouped into twenty-seven distinct approaches. These twenty-seven distinct approaches were reviewed thoroughly using the evaluation framework discussed in Section VI.

The evaluation of the twenty-seven approaches was conducted iteratively. Preliminary evaluation results were obtained toward the end of November 2011. Throughout the writing process, new issues related to the preliminary evaluation results (such as evaluation inconsistencies) also were identified and resolved. Toward the end of March 2012, the first complete draft of this article was produced. This draft was then *circulated to the main authors of all of the twenty-seven approaches* considered in this article 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 was incorporated into this article 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 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 defining the semantics of their constructs. We addressed this challenge by adding a clarifying remark, where appropriate, in the description of each approach (in Appendices C, D, E, and F).

The list of these twenty-seven 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 twenty-seven 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 provided to summarize the types of risk-related activities that each of the twenty-seven approaches supports at each stage of the BPM lifecycle.

Table 1: Risk-aware BPM Approaches—Authors, Approach Code, and References

Authors	Approach Code	Reference(s)
Jakoubi et al., Tjoa et al.	DI01	Tjoa, Jakoubi, and Quirchmayr, 2008b; Tjoa, Jakoubi, Goluch, and Kitzler, 2010; Tjoa, Jakoubi, Goluch, and Quirchmayr, 2008a; Tjoa et al., 2011; Jakoubi, Tjoa, and Quirchmayr, 2007; Jakoubi, Tjoa, Goluch, and Kitzler, 2010a, 2010b; Jakoubi, Neubauer, and Tjoa, 2009b; Ekelhart, Fenz, Klemen, and Weippl, 2007; Jakoubi and Tjoa, 2009; Jakoubi, Goluch, Tjoa, and Quirchmayr, 2008; Goluch et al., 2008
Sienou et al.	DI02	Sienou, Lamine, Pingaud, and Karduck, 2010; Sienou, Lamine, Karduck, and Pingaud, 2008b; Sienou, Lamine, Karduck and Pingaud, 2007; Sienou, Lamine, Pingaud, and Karduck, 2009; Sienou, Lamine, and Pingaud, 2008c; Sienou, Karduck, and Pingaud, 2006; Sienou, Karduck, Lamine, and Pingaud, 2008a; Karduck, Sienou, Lamine, and Pingaud, 2007; Sienou, 2009
Cope et al.	DI03	Cope, Kuster, Etzweiler, Deleris, and Ray, 2010b; Cope, Küster, and Etzweiler, 2009; Cope, Deleris, Etzweiler, Koehler, Kuester, Ray, 2010a
Weiß and Winkelmann	DI04	Weiß and Winkelmann, 2011
Asnar and Giorgini	DI05	Asnar and Giorgini, 2008
Mock and Corvo	DI06	Mock and Corvo, 2005
Rosemann and zur Muehlen	DI07	Rosemann and zur Muehlen, 2005
Rotaru et al.	DI08	Rotaru, Wilkin, Churilov, and Neiger, 2008; Neiger, Churliov, zur Muehlen, and Rosemann, 2006; Rotaru, Wilkin, Churilov, Neiger, and Ceglowski, 2009
Betz et al.	DI09	Betz, Hickl, and Oberweis, 2011
Herrmann and Herrmann	DI10	Herrmann and Herrmann, 2006
Strecker et al.	DI11	Strecker, Heise, and Frank, 2011
Karagiannis et al.	DI12	Karagiannis, Mylopoulos, and Schwab, 2007
Taylor et al.	DI13	Taylor, Godino, and Majeed, 2008
Panayiotou et al.	DI14	Panayiotou, Oikonomitsios, Athanasiadou, and Gayialis, 2010
Lambert et al.	DI15	Lambert, Jennings, and Joshi, 2006
Bai et al.	DI16	Bagchi, Bai, and Kalagnanam, 2006; Bai, Padman, and Kirshnan, 2007, 2006
Bhuiyan et al.	DN01	Islam, Bhuiyan, Krishna, and Ghose, 2009; Bhuiyan, Islam, Koliadis, Krishna, and Ghose, 2007
Fenz et al.	DN02	Fenz and Neubauer, 2009; Fenz, Ekelhart, and Neubauer, 2009; Fenz and Ekelhart, 2009; Fenz, 2010
Muehlen et al.	DN03	zur Muehlen, Baumgart, and Junkers, 2006

Table 1: Risk-aware BPM Approaches—Authors, Approach Code, and References – Continued		
Kaegi et al.	DN04	Kaegi, Mock, Ziegler, and Nibali, 2006
Bergholtz et al.	DN05	Andersson, Bergholtz, Edirisuriya, Ilayperuma, and Johannesson, 2005; Bergholtz, Grégoire, Johannesson, Schmitt, Wohed, Zdravkovic, 2005; Schmitt, Grégoire, and Dubois, 2005
Jallow et al.	DN06	Jallow, Majeed, Vergidis, Tiwari, and Roy, 2007
Singh et al.	DN07	Singh, Gelgi, Davulcu, Yau, and Mukhopadhyay, 2008
Conforti et al.	RT01	Conforti, Fortino, La Rosa and ter Hofstede, 2011
Kang et al.	RT02	Kang, Cho, and Kang, 2009
Jans et al.	PE01	Jans, van der Werf, Lybaert and Vanhoof, 2011b; Jans, Lybaert, Vanhoof, and van der Werf, 2008; Jans, Depaire, and Vanhoof, 2011a
Wickboldt et al.	PE02	Wickboldt, Bianchin, Lunardi, Granville, Gaspary, Bartolini, 2011

Table 2: Risk Management Activities Supported by Each Evaluated Approach						
		Design	**Design-time Analysis**	**Execution**	**Runtime Analysis**	**Post-execution Analysis**
Risk Identification	*Risk Discovery Techniques*	DI02	DI03,DI06, DI09,DI10, DI11,DI12, DI14,DN03			PE01, PE02
	Annotation Techniques	DI01,DI02, DI03,DI04, DI05,DI06, DI07,DI08, DI09,DI10, DI11,DI12, DI13,DI14, DI15,DI16, RT01	DI08,DN03	RT01		PE02
Risk Analysis	*Probability Analysis*		DI16,DN02		RT01,RT02	PE01,PE02
	Impact Analysis	DN01	DI01,DI16, DN01,DN02, DN06			PE02
	Risk Propagation		DI06,DI16, DN02			
Risk Evaluation		DI02,DN07	DI05,DI10, DI11,DI12, DI13,DI14, DI16,DN02, DN04,DN07			PE02
Risk Treatment		DI02,DI10, DI12,DN05	DI01,DI05, DI08,DI09, DI10,DI16, DN07		DN07	

The evaluation of these twenty-seven approaches is summarized in the remainder of this section. 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 that 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 that 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 sixteen approaches in total in this category. All 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.

Table 3: Evaluation—Design Stage with Integrated Risk Constructs (1/2)

Approach			**DI01**	**DI02**	**DI03**	**DI04**	**DI05**	**DI06**	**DI07**	**DI08**
Domain			Generic			Finance	Generic			
Risk Type			IT	Generic						
Existing Risk Analysis			−	−	±	−	+	+	−	−
Risk Standard			−	±	−	+	−	−	−	−
Maturity	**Integrated Risk Formalization**	**Abstract Syntax**	−	+	+	+	−	−	−	+
		Concrete Syntax	+	+	+	+	+	+	+	+
		Semantics	−	−	−	−	−	−	−	±
	Implementation		±	−	−	−	−	−	±	−
	Application Methodology		±	+	+	±	−	+	−	−
	Application in Practice		−	−	−	+	±	+	−	−
BPM Lifecycle	**Design**		+	+	+	+	+	+	+	+
	Design-time Analysis		±	−	±	−	+	±	−	±
	Execution		−	−	−	−	−	−	−	−
	Runtime Analysis		−	−	−	−	−	−	−	−
	Post-execution Analysis		−	−	−	−	−	−	−	−

Overall, the approaches in this category mainly focus on defining the *concrete syntax* of the proposed risk constructs. For example, the Risk-Oriented Process Evaluation (ROPE) approach proposed by Jakoubi et al. (DI01) 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. (DI02), Mock and Corvo (DI06), Rosemann and zur Muehlen (DI07), and Rotaru et al. (DI08) 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. (DI16), propose some *concrete syntax* to capture risk-related constructs.

On the other hand, the number of approaches that attempt to formalize the deep-structure (or the *abstract syntax)* of the risk-related constructs proposed are fewer. Among those approaches, Sienou et al. (DI02), Cope et al. (DI03), Betz et al. (DI09), and Strecker et al. (DI11) use UML to define the *abstract syntax* of their constructs, while in the approaches proposed by Weiß and Winkelmmann (DI04) and Rotaru et al. (DI08), Entity Relationship (ER) diagrams are used.

The biggest gap, however, is in the formalization of the *semantics* of the constructs: only one approach (i.e., Rotaru et al.—DI08) attempts to formalize the semantics of the risk constructs proposed. Even so, the formalization of the risk constructs goes only as far as defining the rules and/or constraints with respect to the notion of a risk-aware process model, but not the *execution* semantics of the constructs. Furthermore, only around a third of all approaches in this category have some form of implementation and/or application in practice. For example, Weiß and Winkelmann (DI04) and Mock and Corvo (DI06) have applied their approaches to major banks in Germany, while the approach proposed by Karagiannis et al. (DI12) has been adopted by an insurance company in the United States.

Finally, only about a quarter of all approaches in this category apply some existing risk analysis techniques. For example, Mock and Corvo (DI06) apply the Failure Mode and Effects Analysis (FMEA) technique in their approach, while Bai et al. (DI16) 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 Weiß and Winkelmann (DI04) (which is informed by the Basel II standard [Basel, 2006]), as well as the work by Sienou et al. (DI02) (which is informed by the Generalised Enterprise Reference Architecture and Methodology (GERAM) framework [IFIP, 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, refer to Appendix C.

Table 4: Evaluation—Design Stage with Integrated Risk Constructs (2/2)

Approach			**DI09**	**DI10**	**DI11**	**DI12**	**DI13**	**DI14**	**DI15**	**DI16**
Domain			Generic			Finance	Generic	Supply	Generic	
Risk Type			Generic	Data	IT	Struc-tural	Generic			
Existing Risk Analysis			−	−	−	−	−	−	−	+
Risk Standard			−	−	−	+	−	−	−	−
Maturity	**Integrated Risk Formalization**	**Abstract Syntax**	+	−	+	−	−	−	−	+
		Concrete Syntax	+	+	+	+	±	+	+	−
		Semantics	−	−	−	−	−	−	−	−
	Implementation		+	+	−	(+)[1]	+	+	−	−
	Application Methodology		+	+	±	+	±	+	±	±
	Application in Practice		−	−	−	+	−	±	+	−
BPM Lifecycle	**Design**		+	+	+	+	+	±	±	±
	Design-time Analysis		±	±	±	±	±	±	−	+
	Execution		−	−	−	−	−	−	−	−
	Runtime Analysis		−	−	−	−	−	−	−	−
	Post-execution Analysis		−	−	−	−	−	−	−	−

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 that address design-time R-BPM *without* introducing integrated risk constructs. There are a total of seven 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 provide only partial support for design-time risk analysis. 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.

Comment [G1]: AU: Is something missing here?

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 (namely, 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 is 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 the resource criticality analysis should be used precisely 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. (DN03) has been applied to a payroll process in a university, while the works by Bhuiyan et al. (DN01) and Fenz et al. (DN02) 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* [U.S. Department of Defense, 1949]). Most of these approaches have been developed to be generic enough to be applied in any domain. Refer to Appendix D for a detailed analysis of the approaches in this category.

Table 5: Evaluation—Design Stage Without Integrated Risk Constructs

Approach			**DN01**	**DN02**	**DN03**	**DN04**	**DN05**	**DN06**	**DN07**
Domain			Generic	IT	Generic				
Risk Type			Organi-zational	IT	Generic				Struc-tural.
Existing Risk Analysis			−	+	±	−	−	+	−
Risk Standard			−	±	−	±	−	+	−
Maturity	**Integrated Risk Formalization**	**Abstract Syntax**	N/A	N/A	N/A	(N/A)[1]	N/A	N/A	N/A
		Concrete Syntax	N/A	N/A	N/A	N/A	N/A	N/A	N/A
		Semantics	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Implementation		−	±	−	−	−	(+)[2]	−
	Application Methodology		−	−	±	−	±	−	−
	Application in Practice		±	±	+	−	−	−	−
BPM Lifecycle	**Design**		±	−	−	−	+	−	±
	Design-time Analysis		±	+	±	±	−	±	±
	Execution		−	−	−	−	−	−	−
	Runtime Analysis		−	−	−	−	−	−	±
	Post-execution Analysis		−	−	−	−	−	−	−

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 that primarily focus on addressing process risks during runtime are summarized. A 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. Our systematic literature review process managed to determine only two approaches that fall into this category, namely, the works by Conforti et al. [2011] and Kang et al. [2009]. These two approaches differ in the sense that Conforti et al. (RT01) introduce a set of risk-related constructs (in the form of a language) that are executable at runtime, while Kang et al. (RT02) 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 approach. Nevertheless, neither is influenced by any existing risk standards. Both approaches are generic enough to be applied in any domain. 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. A 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 two approaches in this category are those proposed by Jans et al. [2011a, 2008, 2011b] and Wickboldt et al. [2011]. The former approach (PE01) uses a set of constructs to capture risk-related information in a process log, such that it can be used subsequently for risk analysis, while the latter approach (PE02) does not attempt to introduce any new risk constructs; rather, it simply attempts to analyze the existence of risks based on an existing log. The latter approach has been validated in practice, although this is not the case with the former.

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.'s approach. Refer to Appendix F for a detailed explanation and evaluation of these two approaches.

Table 6: Evaluation—Runtime and Post-execution

Approach			**RT01**	**RT02**	**PE01**	**PE02**
Domain			Generic		Finance	IT System
Risk Type			Organization, Data, Structural	Generic	Structural	Generic
Existing Risk Analysis			+	−	−	
Risk Standard			−	−	−	+
Maturity	**Integrated Risk Formalization**	Abstract Syntax	+	N/A	N/A	+
		Concrete Syntax	+	N/A	N/A	−
		Semantics	−	N/A	N/A	−
	Implementation		+	±	(+)[1]	+
	Application Methodology		±	±	+	±
	Application in Practice		−	−	+	−
BPM Lifecycle	**Design**		±	−	−	−
	Design-time Analysis		−	−	−	−
	Execution		+	−	−	−
	Runtime Analysis		+	+	−	−
	Post-execution Analysis		−	−	+	+

Notes: [1] Implemented in the sense that there is already an existing software tool that supports the approach.

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 degree of research contribution in the area of R-BPM per BPM lifecycle stage
- The comprehensiveness of R-BPM functionality proposed per BPM lifecycle
- The maturity of the approaches
- The level of influence of existing risk management techniques and standards on the R-BPM approaches evaluated in this article

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

Research Contribution per BPM Lifecycle Stage

As shown in Figure 2, an obvious research gap in the area of R-BPM is the lack of research addressing risks at the runtime stage, the execution stage, and the post-execution stage of the BPM lifecycle. By looking at Tables 3 to 6, we can see that out of the twenty-seven approaches evaluated, there are only three approaches that address the runtime risk analysis stage of business processes (DN07, RT01, and RT02): one approach, which addresses the execution stage (RT01), and two approaches, which focus on the post-execution stage (PE01 and PE02). In contrast, there are twenty approaches that address design-time activities and eighteen approaches that address design-time analysis activities (note that some approaches support more than one lifecycle stage).

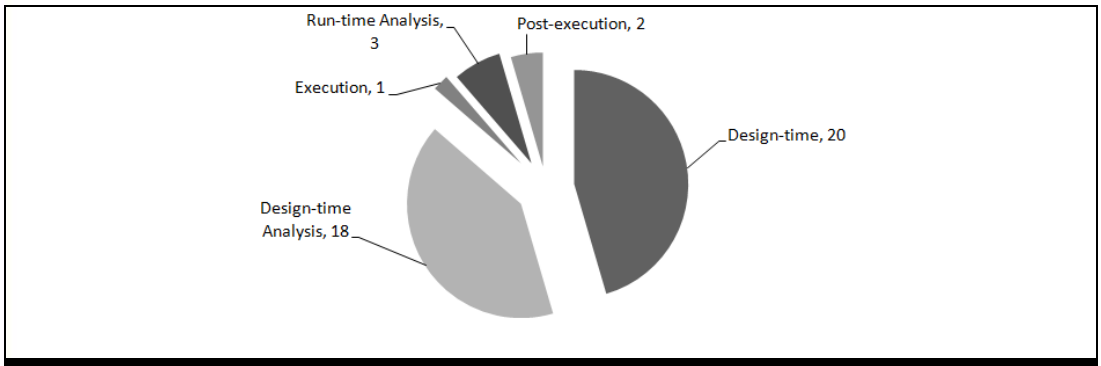

Figure 2. Distribution of Evaluated Approaches per BPM Lifecycle Stages

Having many approaches, addressing a particular BPM lifecycle stage does not mean necessarily 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 the 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 twenty-seven evaluated approaches.

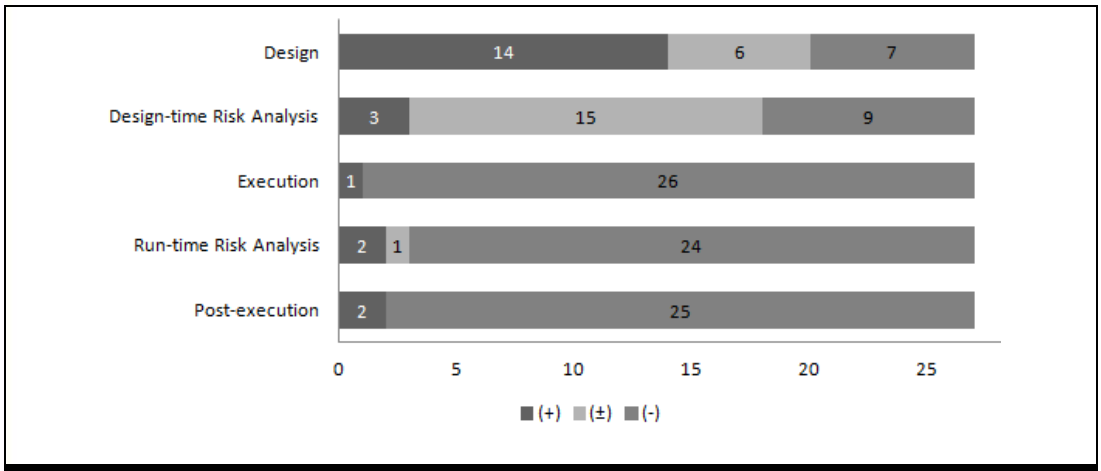

Figure 3. Support Comprehensiveness for Each BPM Lifecycle Stage

Design-time Research Gap

Of the twenty-seven approaches evaluated, twenty approaches provide either comprehensive or partial design-time support (see Figure 3). Specifically, fourteen approaches provide what we evaluated to be comprehensive (+)

support (about 52 percent of all approaches evaluated), while six approaches provide partial support (about 22 percent). 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 seventeen of the twenty 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 problems that need to be addressed in the field 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 the design-time risk analysis stage: there are about eighteen approaches that provide either comprehensive (three approaches—11 percent) or partial (fifteen approaches—56 percent) 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 [2011] approach (which attempts to perform a risk analysis via simulation) and Karagiannis et al.'s [2007] approach (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 that are precise and, ideally, exhaustive. This is likely to be a challenging research topic, given the complexity of business processes.

Furthermore, for those approaches, which propose new risk-related constructs, there also exists a research gap in the exploitation of the proposed constructs to enable design-time risk analysis. As shown in Table 2, while there are many approaches that 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 [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 a business process' risks during the execution stage of a BPM lifecycle, i.e., Conforti et al.'s [2011] approach. 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 running process instance may reach an undesirable state, a risk-informed process execution

should be able to automatically determine and subsequently divert the process instance to an alternative execution path, such that the probability of the process instance reaching the undesirable state is 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 historical data of a process. 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 for the purpose of 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 (1) the ability to tighten the reasoning about, and analysis of, risks between the design-time and runtime stages and (2) the ability to design a cleaner risk-annotated process model (as there are now fewer variations in the types of risk annotation schemes 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 that attempt to provide runtime risk analysis capability, and only two that provide adequate/convincing support.

Unfortunately, while the runtime risk analysis techniques proposed by these two approaches [Conforti et al., 2011; Kang et al., 2009] are quite convincing, they focus on a particular type of risk analysis: the probability analysis. Similarly, Singh et al.'s [2008] runtime analysis approach also focuses only 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 consequences of risk events on 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 that have not been considered during design-time.

Another research challenge related to runtime risk analysis concerns the issue of performance. Unlike design-time risk analysis, the results from a 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 that 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 in the post-execution stage tends to rely), the comprehensiveness of research in this particular BPM lifecycle stage is rather high (see Figure 3).

Nevertheless, still further research is needed, as there are still many unknowns in this area. 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 the two post-execution approaches evaluated in this article (i.e., PE01 and PE02) 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 log to inform the redesign 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 article address the design stage of the BPM lifecycle, the maturity of research in this area still needs to be improved. The overall maturity of those approaches, which propose new risk constructs (sixteen out of twenty-three approaches in this category), is quite low, as demonstrated by the fact that most of these approaches go only 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.

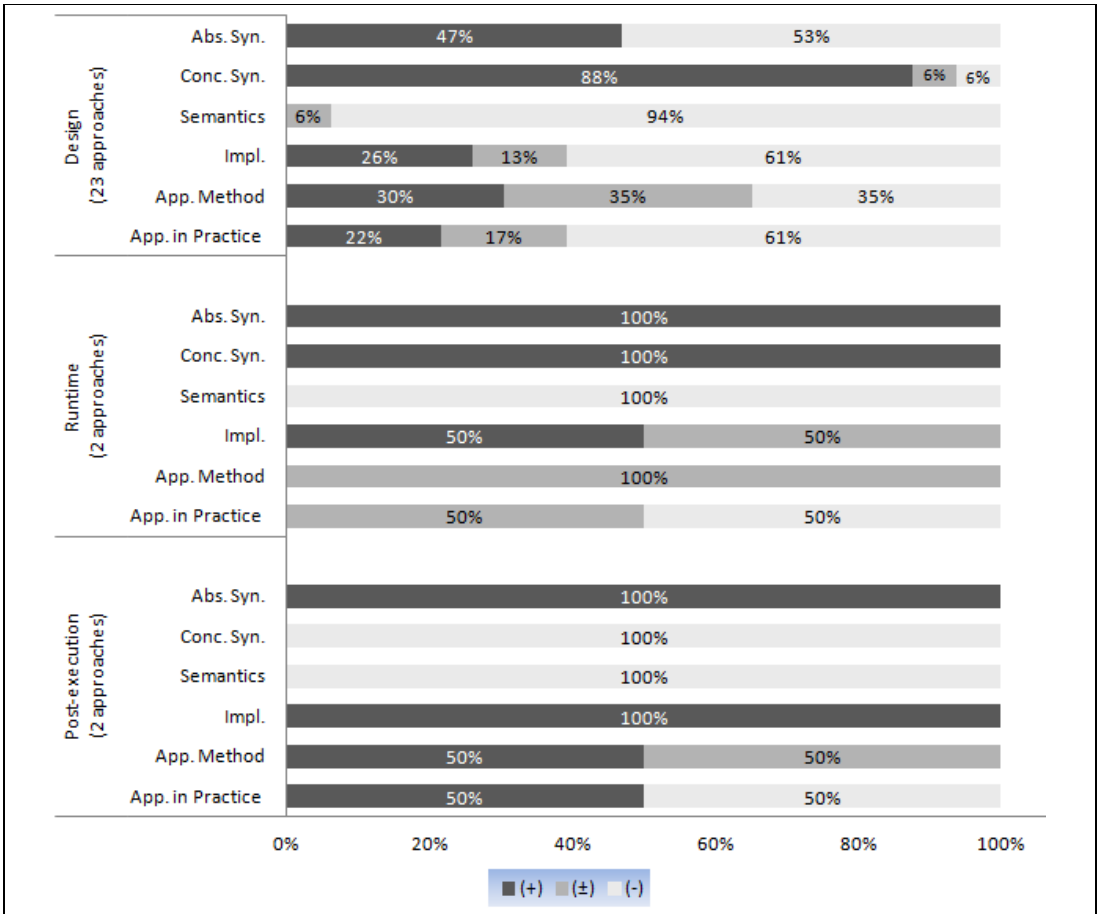

Figure 4. Percentage of Support for Each R-BPM Maturity Sub-criteria

Furthermore, the majority of approaches in this category are still "theoretical," in that they have not been implemented as tools that can be used by practitioners. In fact, less than 30 percent of the approaches actually have been implemented. Worse, the extent to which these approaches have been comprehensively validated in practice is even lower (around 22 percent).

Finally, 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 approaches that 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 et al., 2011] that attempts to provide integrated risk constructs to annotate process models 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 still can be improved.

Furthermore, all of the approaches in this category have been either 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

While there are only two approaches evaluated in this category, as can be seen from Figure 4, they are quite matured.

There is only one approach [Wickboldt et al., 2011] that 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 also have been implemented. The maturity of the application methodology of the approaches in this category can be considered quite high as well: Wickboldt et al. provide a high-level description of the application methods of their approach, while Jans et al. apply an existing (and relatively matured) methodology, namely, the process mining methodology [van der Aalst, 2011].

Out of the two approaches in this category, only one (i.e., Jans et al.—PE01) used logs from real-world organizations in its analysis and validated the findings with relevant domain experts. The other approach (i.e., Wickboldt et al.—PE02) has not been applied in practice: we could not find evidence that the approach has been validated using logs from a real-world organization.

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 to 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 twenty-seven approaches evaluated, there are only seven approaches (or 26 percent) that apply existing risk management techniques. Similarly, there are only three approaches (or 11 percent) that are clearly influenced by existing risk management standards.

Therefore, how we can apply existing risk management techniques seamlessly to reason about risks in a business process 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 toward the runtime and the post-execution stages 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 in that they can be exploited to enable formal reasoning about risks. As shown in Tables 3 to 6, there is a lack of formal semantics given to most of the risk constructs proposed by the R-BPM approaches that we evaluated in this article. Consequently, it is difficult to perform a much richer formal analysis on the effects of risks in a risk-annotated business process. At the same time, a higher degree of formalism is desirable because the mathematical foundation of a formal analysis approach provides many benefits that 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. [2010a] and Rotaru et al. [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 to the field of BPM is an area that is worth further investigation. The number of existing approaches that 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 reinvent 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 the Monte Carlo simulation, Failure Modes and Effects analysis, and Bayesian network analysis) into the BPM field. Then we can 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. 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 take this research 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 *redesign* the process model(s) for future executions (we call this a *runtime informed process redesign* 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 by the research community.[5] Given the increasing prevalence of BPM systems [Dixon, 2011], there is now a reasonable amount of process-related logs [van der Aalst, 2011] that can be analyzed to gain insights about process-related risks. However, the exploitation of post-execution logs for such a purpose is still largely unexplored. By using historical data, we enable *evidence-based* analysis 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 a 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 article 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

[5] Research in other domains, such as incident response and handling, also has been exploiting logs for analysis purposes; however, the research agenda proposed here is quite different in that it applies only to research related to the use of *event logs derived from the execution of BPM systems to shed lights on process-related risks,* instead of any generic log/data used in other domains.

models with risk information; however, there is not yet a standard that clearly specifies the types of constructs that really need to be considered for an R-BPM. The scope of an R-BPM itself still needs to be clarified, e.g., should an R-BPM system consider only *internal risks* (that is, those risks which can be controlled/minimized by design) or should it also consider *external risks* (that is, those risks that are beyond the "control-sphere" of an organization)? One may proceed with research in this area by identifying the various dimensions of an R-BPM system and then clearly specifying the functionality for each of the identified dimensions.

IX. CONCLUSIONS

In this article, we conducted a *comprehensive* survey of existing R-BPM approaches. 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, the management of risks in business processes has been the subject of an active research in the past few years; however, there are still a number of problems related to such a system that require further investigation, including the management of risks during process execution, the exploitation of post-execution data for the purpose of risk analysis, and the ability to formally reason about risks in processes. 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 from the European Research Center for Information Systems (ERCIS) for their valuable input regarding the theoretical framework underpinning the development of the evaluation framework used in this article and their advice in conducting a systematic literature review. This research was supported by the Australian Research Council (ARC) Discovery Project through grant DP110100091 and the DZ BANK Foundation, in the context of the research project IMPROVABLE, which has been conducted by the European Research Center for Information Systems at the University of Muenster.

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.

107th Congress USA (2002) "Public Law 107-204—Sarbanes-Oxley Act of 2002", http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf (current April 15, 2013).

Andersson, B., M. Bergholtz, A. Edirisuriya, T. Ilayperuma, and P. Johannesson (2005) "A Declarative Foundation of Process Models", in Pastor, O., and J. Falcão e Cunha (eds.), *Proceedings of the Seventeenth International Conference on Advanced Information Systems Engineering (CAiSE'05), volume 3520, Lecture Notes in Computer Science,* Berlin/Heidelberg, Germany: Springer, pp. 233–247.

Asnar, Y., and P. Giorgini (2006) "Modelling Risk and Identifying Countermeasure in Organizations" in López, J. (ed.), *Proceedings of the First International Workshop on Critical Information Infrastructures Security (CRITIS'06), volume 4347, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 55–66.

Asnar, Y., and P. Giorgini (2008) "Analyzing Business Continuity Through a Multi-layers Model" in Dumas, M., M. Reichert, and M. Shan (eds.), *Proceedings of the Sixth International Conference on Business Process Management (BPM'08), volume 5240, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 212–227.

Australian Bureau of Statistics (2008) "Australian and New Zealand Standard Research Classification (ANZSRC)", http://www.arc.gov.au/pdf/ANZSRC_FOR_codes.pdf (current April 15, 2013).

Awad, A., G. Decker, and M. Weske (2008) "Efficient Compliance Checking Using BPMN-Q and Temporal Logic" in Dumas, M., M. Reichert, and M. Shan (eds.), *Proceedings of the Sixth International Conference on Business*

Process Management (BPM'08), volume 5240, Lecture Notes in Computer Science, Berlin/Heidelberg, Germany: Springer, pp. 326–341.

Ayed, S., N. Cuppens-Boulahia, and F. Cuppens (2009) "Deploying Security Policy in Intra and Inter Workflow Management Systems", *Proceedings of the Fourth International Conference on Availability, Reliability and Security (ARES'09)*, Los Alamitos, CA, Washington, DC, Tokyo, Japan: IEEE Computer Society, pp. 58–65.

Aziz, B., A. Arenas, F. Martinelli, I. Matteucci, and P. Mori (2008) "Controlling Usage in Business Process Workflows Through Fine-grained Security Policies" in Furnell, S., S. Katsikas, and A. Lioy (eds.), *Proceedings of the Fifth International Conference on Trust, Privacy and Security in Digital Business (TrustBus'08), volume 5185, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany, New York: Springer, pp. 100–117.

Bagchi, S., X. Bai, and J. Kalagnanam (2006) "Data Quality Management Using Business Process Modeling", *Proceedings of the IEEE International Conference on Services Computing (SCC'06)*, Los Alamitos, CA: IEEE Computer Society, pp. 398–405.

Bai, X., R. Padman, and R. Krishnan (2006) "On Risk Management in Business Process Design", *Technical Report, The H. John Heinz III School of Public Policy and Management, Carnegie Mellon University*, http://heinz.cmu.edu/research/296full.pdf (current April 15, 2013).

Bai, X., R. Padman, and R. Kirshnan (2007) "A Risk Management Approach to Business Process Design", *Proceedings of the International Conference on Information Systems (ICIS'07)*, Association for Information Systems, http://aisel.aisnet.org/icis2007/28/ (current April 15, 2013).

Basel (2006) *Basel II: International Convergence of Capital Measurement and Capital Standards—A Revised Framework—Comprehensive Version*, Basel Committee on Banking Supervision, Basel, Switzerland.

Becker, J., D. Breuker, B. Weiß, and A. Winkelmann (2010) "Exploring the Status Quo of Business Process Modelling Languages in the Banking Sector—An Empirical Insight into the Usage of Methods in Banks", *Proceedings of the Twenty-first Australasian Conference on Information Systems (ACIS'10)*, Association for Information Systems, http://aisel.aisnet.org/acis2010/8/ (current April 15, 2013).

Becker, J., I. Thome, B. Weiß, and A. Winkelmann (2010) "Constructing a Semantic Business Process Modelling Language for the Banking Sector—An Evolutionary Dyadic Design Science Approach", *Enterprise Modelling and Information Systems Architectures*, (5)1, pp. 4–25.

Bergholtz, M., B. Grégoire, P. Johannesson, M. Schmitt, P. Wohed, and J. Zdravkovic (2005) "Integrated Methodology for Linking Business and Process Models with Risk Mitigation" in Cox, K., E. Dubois, Y. Pigneur, S. Bleistein, J. Verner, A. Davis, and R. Wieringa (eds.), *Proceedings of the First International Workshop Requirements Engineering for Business Need and IT Alignment (REBNITA'05), The Thirteenth IEEE International Conference on Requirements Engineering (RE'05)*, Sydney, Australia: University of New South Wales Press, pp. 163–168.

Betz, S., S. Hickl, and A. Oberweis (2011) "Risk-aware Business Process Modeling and Simulation Using XML Nets" in Hofreiter, B., E. Dubois, K. Lin, T. Setzer, C. Godart, E. Proper, and L. Bodenstaff (eds.), *Proceedings of the Thirteenth IEEE Conference on Commerce and Enterprise Computing (CEC'11)*, Washington, DC: IEEE Computer Society, pp. 349–356.

Bhuiyan, M., M. Islam, G. Koliadis, A. Krishna, and A. Ghose (2007) "Managing Business Process Risk Using Rich Organizational Models", *Proceedings of the Thirty-first International Conference on Computer Software and Applications (COMPSAC'07)*, Los Alamitos, CA: IEEE Computer Society, pp. 509–520.

Brabänder, E., and H. Ochs (2002) "Analyse und Gestaltung prozessorientierter Risikomanagementsysteme mit Ereignisgesteuerten Prozessketten" in Nüttgens, M., and F. Rump (eds.), *Proceedings of the Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten, GI-Workshop und Arbeitskreistreffen (EPK'02)*, Trier, Germany: GI-Arbeitskreis Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten, pp. 17–35.

Carnaghan, C. (2006) "Business Process Modeling Approaches in the Context of Process Level Audit Risk Assessment: An Analysis and Comparison", *International Journal of Accounting Information*, (7)2, pp. 170–204.

Cernauskas, D., and A. Tarantino (2009) "Operational Risk Management with Process Control and Business Process Modeling", *Journal of Operational Risk*, (4)2, pp. 3–17.

Cha, S., L. Liu, and B. Yu (2009) "Process-oriented Approach for Validating Asset Value for Evaluating Information Security Risk", *Proceedings of the Twelfth IEEE International Conference on Computational Science and Engineering (IEEE CSE'09)*, Los Alamitos, CA: IEEE Computer Society, pp. 379–385.

Cheng, R., S. Sadiq, and M. Indulska (2011) "Framework for Business Process and Rule Integration: A Case of BPMN and SBVR" in Abramowicz, W. (ed.), *Proceedings of the Fourteenth International Conference on Business Information Systems (BIS'11), volume 87, Lecture Notes in Business Information Processing*, Berlin/ Heidelberg, Germany: Springer, pp. 13–24.

Clark, N., and D. Jolly (2008) "Société Générale Loses $7 Billion in Trading Fraud", *The New York Times*, http://www.nytimes.com/2008/01/24/business/worldbusiness/24iht-socgen.5.9486501.html?pagewanted=all&_r=0 (current April 15, 2013).

Clarke, E., and W. Jeannette (1996) "Formal Methods: State of the Art and Future Directions", *ACM Computing Surveys*, (28)4, pp. 626–643.

Conforti, R., G. Fortino, M. La Rosa, and A. ter Hofstede (2011) "History-aware Real-time Risk Detection in Business Processes" in Meersman, R., T. Dillon, P. Herrero, A. Kumar, M. Reichert, L. Qing, B. Ooi, E. Damiani, D. Schmidt, J. White, M. Hauswirth, P. Hitzler, and M. Mohania (eds.), *Proceedings of the Confederated International Conferences: CoopIS, DOA-SVI, and ODBASE 2011 On the Move to Meaningful Internet Systems (OTM 2011), Part I, volume 7044, Lecture Notes in Computer Science*, Heidelberg, Germany, Dordrecht, Netherlands, London, UK, New York: Springer, pp. 100–118.

Cooper, H. (1988) "Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews", *Knowledge, Technology and Policy*, (1)1, pp. 104–126.

Cope, E., L. Deleris, D. Etzweiler, J. Koehler, J. Kuester, and B. Ray (2010a) "System and Method for Creating and Expressing Risk-extended Business Process Models", *U.S. Patent No. US2010/0179847A1*, http://images2.freshpatents.com/pdf/US20100179847A1.pdf (current April 15, 2013).

Cope, E., J. Küster, and D. Etzweiler (2009) "Risk Extensions to the BPMN 1.1 Business Process Metamodel", *Technical Report RZ3740, IBM Research*, http://domino.watson.ibm.com/library/cyberdig.nsf/papers/AF55138835E929D2852575DA003F8722/File/RZ3740.pdf (current April 15, 2013).

Cope, E., J. Kuster, D. Etzweiler, L. Deleris, and B. Ray (2010b) "Incorporating Risk into Business Process Models", *IBM Journal of Research and Development*, (54)3, pp. 4:1–4:13.

COSO (2004) "Enterprise Risk Management—Integrated Framework", http://www.coso.org/erm-integratedframework.htm (current April 15, 2013).

da Costa Cordeiro, W., G. Machado, F. Andreis, A. dos Santos, C. Both, L. Gaspary, L. Granville, C. Bartolini, and D. Trastour (2009) "ChangeLedge: Change Design and Planning in Networked Systems Based on Reuse of Knowledge and Automation", *Computer Networks*, (53)16, pp. 2782–2799.

Dixon, J. (2011) "BPM Survey Insights: Maturity Advances as BPM Goes Mainstream", *Gartner*, (G00213606).

Dixon, J., and T. Jones (2011) "Hype Cycle for Business Process Management", *Gartner*, http://www.gartner.com/id=1751119 (current April 15, 2013).

Dumas, M., M. La Rosa, J. Mendling, and H.A. Reijers (2013) *Fundamentals of Business Process Management*, Heidelberg, Germany, New York, Dordrecht, Netherlands, London, UK: Springer.

Dumas, M., W. van der Aalst, and A. ter Hofstede (2005) *Process-aware Information Systems: Bridging People and Software Through Process Technology,* Hoboken, NJ: John Wiley & Sons.

Ekelhart, A., S. Fenz, M. Klemen, and E. Weippl (2007) "Security Ontologies: Improving Quantitative Risk Analysis", *Proceedings of the Fortieth Hawaii International Conference on System Sciences (HICSS'07)*, Los Alamitos, CA: IEEE Computer Society, p. 156a.

Federal Information Processing Standards (1993) "Integration Definition for Function Modeling (IDEF0)", Publication 183, http://www.idef.com/pdf/idef0.pdf (current April 15, 2013).

Fenz, S. (2010) "From the Resource to the Business Process Risk Level" in Clarke, N., S. Furnell, and R. von Solms (eds.), *Proceedings of the Twelfth Annual IFIP Workshop on Information Security Management in South African Information Security Multi-conference (SAISMC'10)*, Plymouth, UK: University of Plymouth, pp. 100–109.

Fenz, S., and A. Ekelhart (2009) "Formalizing Information Security Knowledge" in Li, W., W. Susilo, U. Tupakula, R. Safavi-Naini, and V. Varadharajan (eds.), *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS'09)*, New York: ACM, pp. 183–194.

Fenz, S., A. Ekelhart, and T. Neubauer (2009) "Business Process-based Resource Importance Determination" in Dayal, U., J. Eder, J. Koehler, and H. Reijers (eds.), *Proceedings of the Seventh International Conference on*

Business Process Management (BPM'09), *volume 5701, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany, New York: Springer, pp. 113–127.

Fenz, S., and T. Neubauer (2009) "How to Determine Threat Probabilities Using Ontologies and Bayesian Networks" in Sheldon, F., G. Peterson, A. Krings, R. Abercrombie, and A. Mili (eds.), *Proceedings of the Fifth Cyber Security and Information Intelligence Research Workshop (CSIIRW'09)*, New York: ACM, pp. 69:1–69:3.

Frank, U. (2010) "The MEMO Meta Modelling Language (MML) and Language Architecture", *Technical Report 28, Institute for Computer Science and Business Information Systems*, http://www.icb.uni-due.de/fileadmin/ICB/research/research_reports/ICB-Report_No24.pdf (current April 15, 2013).

Fugini, M., E. Damiani, and K. Reed (2007) "Assessing Business Process Security Awareness: A Service-oriented Approach", *Proceedings of Thirteenth Americas Conference on Information Systems (AMCIS'07)*, Association for Information Systems, http://aisel.aisnet.org/amcis2007/89/ (current April 15, 2013).

Gengler, B. (2008) "BPM to Buck Slowing Spend Trend", *The Australian*, http://www.theaustralian.com.au/news/bpm-to-buck-slowing-spend-trend/story-e6frgao6-1111115998150 (current April 15, 2013).

Gerke, K., J. Cardoso, and A. Claus (2009) "Measuring the Compliance of Processes with Reference Models" in Meersman, R., T. Dillon, and P. Herrero (eds.), *Proceedings of the Confederated International Conferences—CoopIS, DOA, IS, and ODBASE 2009 On the Move to Meaningful Internet Systems (OTM'09), volume 5870, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 76–93.

Ghanavati, S., D. Amyot, and L. Peyton (2007) "Towards a Framework for Tracking Legal Compliance in Healthcare" in Krogstie, J., A. Opdahl, and G. Sindre (eds.), *Proceedings of the Nineteenth International Conference on Advanced Information Systems Engineering (CAiSE'07), volume 4495, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany, New York: Springer, pp. 218–232.

Goedertier, S., and J. Vanthienen (2006) "Compliant and Flexible Business Processes with Business Rules" in Regev, G., P. Soffer, and R. Schmidt (eds.), *Proceedings of the Seventh Workshop on Business Process Modelling, Development and Support (BPMDS'06), The Eighteenth International Conference on Advanced Information Systems Engineering (CAISE'06)*, Namur, Belgium: Presses Universitaires de Namur, pp. 94–104.

Goluch, G., A. Ekelhart, S. Fenz, S. Jakoubi, S. Tjoa, and T. Mück (2008) "Integration of an Ontological Information Security Concept in Risk Aware Business Process Management", *Proceedings of the Forty-first Hawaii International Conference on System Sciences (HICSS'08)*, Los Alamitos, CA: IEEE Computer Society, p. 377.

Gordijn, J., E. Yu, and B. van der Raadt (2006) "e-Service Design Using i* and e^3value Modeling", *IEEE Software*, (23)3, pp. 26–33.

Governatori, G., J. Hoffmann, S. Sadiq, and I. Weber (2009) "Detecting Regulatory Compliance for Business Process Models Through Semantic Annotations" in Ardagna, D., M. Mecella, and J. Yang (eds.), *Proceedings of the Fourth International Workshop on Business Process Design (BPD'08), volume 17, Lecture Notes in Business Information*, Heidelberg, Germany: Springer, pp. 5–17.

Heckerman, D. (1995) "A Tutorial on Learning with Bayesian Networks", *Technical Report MSR-TR-95-06, Microsoft Research, Advanced Technology Division, Redmond, WA*, http://ftp.research.microsoft.com/pub/tr/tr-95-06.pdf (current April 15, 2013).

Hengmith, L. (2005) "Geschäftsprozessmodellierung und -simulation als Hilfsmittel zum Management operationeller Risiken", *Banking and Information Technology*, (6)2, pp. 17–29.

Herrmann, P., and G. Herrmann (2006) "Security Requirement Analysis of Business Processes", *Electronic Commerce Research*, (6)3–4, pp. 305–335.

Hevner, A., S. March, J. Park, and S. Ram (2004) "Design Science in Information Systems Research", *MIS Quarterly*, (28)1, pp. 75–105.

Ho, D., and M. zur Muehlen (2009) "From the Stone Age to the Cloud: A Case Study of Risk-focused Process Improvement", *Proceedings of the Twentieth Australasian Conference on Information Systems (ACIS'09)*, Association for Information Systems, http://aisel.aisnet.org/acis2009/6 (current April 15, 2013).

Horwood, C., and P. Lee (2011) "Banks Have Not Learnt Lessons on Risk Management", *Euromoney*, http://www.euromoney.com/Article/2897957/Banks-have-not-learnt-lessons-on-risk-management.html (current April 15, 2013).

Howley, V., and E. Thomasson (2011) "UBS $2 Billion Rogue Trade Suspect Held in London", *Reuters*, http://www.reuters.com/article/2011/09/15/us-ubs-idUSTRE78E15I20110915 (current April 15, 2013).

IFIP (1999) *GERAM: Generalised Enterprise Reference Architecture and Methodology*, http://www.ict.griffith.edu.au/~bernus/taskforce/geram/versions/geram1-6-3/GERAMv1.6.3.pdf (current April 15, 2013).

Iida, S., G. Denker, and C. Talcott (2009) "Document Logic: Risk Analysis of Business Processes Through Document Authenticity", *Proceedings of the Enterprise Distributed Object Computing Workshop, The Twelfth IEEE International Conference (EDOCw'09)*, Los Alamitos, CA: IEEE Computer Society, pp. 54–63.

Islam, M., M. Bhuiyan, A. Krishna, and A. Ghose (2009) "An Integrated Approach to Managing Business Process Risk Using Rich Organizational Models" in Meersman, R., T. Dillon, and P. Herrero (eds.), *Proceedings of the Confederated International Conferences—CoopIS, DOA, IS, and ODBASE 2009 On the Move to Meaningful Internet Systems (OTM'09), volume 5870, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 273–285.

Jakoubi, S., G. Goluch, S. Tjoa, and G. Quirchmayr (2008) "Deriving Resource Requirements Applying Risk-aware Business Process Modeling and Simulation", *Proceedings of the Sixteenth European Conference on Information Systems (ECIS'08)*, Association for Information Systems, http://aisel.aisnet.org/ecis2008/209/ (current April 15, 2013).

Jakoubi, S., T. Neubauer, and S. Tjoa (2009b) "A Roadmap to Risk-aware Business Process Management" in Kirchberg, M., P. Hung, B. Carminati, C. Chi, R. Kanagasabai, E. Della Valle, K. Lan, and L. Chen (eds.), *Proceedings of the Fourth IEEE Asia-Pacific Services Computing Conference (APSCC'09)*, Los Alamitos, CA: IEEE Computer Society, pp. 23–27.

Jakoubi, S., and S. Tjoa (2009) "A Reference Model for Risk-aware Business Process Management" in Kalam, A., Y. Deswarte, and M. Mostafa (eds.), *Proceedings of the Fourth International Conference on Risks and Security of Internet and Systems (CRiSIS'09)*, Los Alamitos, CA: IEEE Computer Society, pp. 82–89.

Jakoubi, S., S. Tjoa, G. Goluch, and G. Quirchmayr (2009a) "A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management", *Proceedings of the International Workshops on Database and Expert Systems Applications (DEXA'09)*, Los Alamitos, CA: IEEE Computer Society, pp. 127–132.

Jakoubi, S., S. Tjoa, S. Goluch, and G. Kitzler (2010a) "A Formal Approach Towards Risk-aware Service Level Analysis and Planning", *Proceedings of the Fifth International Conference on Availability, Reliability and Security (ARES'10)*, Los Alamitos, CA: IEEE Computer Society, pp. 180–187.

Jakoubi, S., S. Tjoa, S. Goluch, and G. Kitzler (2010b) "Risk-aware Business Process Management—Establishing the Link Between Business and Security" in Xhafa, F., L. Barolli, and P. Papajorgji (eds.), *Complex Intelligent Systems and Their Applications, volume 41, Springer Optimization and Its Applications*, New York: Springer, pp. 109–135.

Jakoubi, S., S. Tjoa, and G. Quirchmayr (2007) "ROPE: A Methodology for Enabling the Risk-aware Modelling and Simulation of Business Processes" in Österle, H., J. Schelp, and R. Winter (eds.), *Proceedings of the Fifteenth European Conference on Information Systems (ECIS'07)*, St. Gallen, Switzerland: University of St. Gallen, pp. 1596–1607.

Jallow, A., B. Majeed, K. Vergidis, A. Tiwari, and R. Roy (2007) "Operational Risk Analysis in Business Processes", *BT Technology Journal*, (25)1, pp. 168–177.

Jans, M., B. Depaire, and K. Vanhoof (2011a) "Does Process Mining Add to Internal Auditing? An Experience Report" in Halpin, T., S. Nurcan, J. Krogstie, P. Soffer, E. Proper, R. Schmidt, and I. Bider (eds.), *Proceedings of the Twelfth International Conference on Business Process Modeling, Development, and Support (BPMDS'11),* and *Sixteenth International Conference on Exploring Modelling Methods for Systems Analysis and Design (EMMSAD'11), The Twenty-third International Conference on Advanced Information Systems Engineering (CAiSE'11), volume 81, Lecture Notes in Business Information Processing*, Heidelberg, Germany: Springer, pp. 31–45.

Jans, M., N. Lybaert, K. Vanhoof, and J. van der Werf (2008) "Business Process Mining for Internal Fraud Risk Reduction: Results of a Case Study", *Proceedings of the International Research Symposium on Accounting Information Systems, (IRSAIS'08)*, http://doclib.uhasselt.be/dspace/bitstream/1942/10457/1/Jansetal-paper.pdf (current April 15, 2013).

Jans, M., J. van der Werf, N. Lybaert, and K. Vanhoof (2011b) "A Business Process Mining Application for Internal Transaction Fraud Mitigation", *Expert Systems with Applications*, (38)10, pp. 13351–13359.

Jensen, K., and L. Kristensen (2009) *Coloured Petri Nets—Modelling and Validation of Concurrent Systems*, London, UK: Springer.

Kaegi, M., R. Mock, R. Ziegler, and R. Nibali (2006) "Information Systems' Risk Analysis by Agent-based Modelling of Business Processes" in Soares, C., and E. Zio (eds.), *Proceedings of the Seventeenth European Safety and Reliability Conference (ESREL'06)*, London, UK: Taylor & Francis Group, pp. 2277–2284.

Kang, B., N. Cho, and S. Kang (2009) "Real-time Risk Measurement for Business Activity Monitoring (BAM)", *International Journal of Innovative Computing, Information and Control*, (5)11, pp. 3647–3657.

Karagiannis, D., J. Mylopoulos, and M. Schwab (2007) "Business Process-based Regulation Compliance: The Case of the Sarbanes-Oxley Act" in Sutcliffe, A., P. Jalote (eds.), *Proceedings of the Fifteenth IEEE International Conference on Requirements Engineering (RE'07)*, Los Alamitos, CA: IEEE Computer Society, pp. 315–321.

Karduck, A., A. Sienou, E. Lamine, and H. Pingaud (2007) "Collaborative Process Driven Risk Management for Enterprise Agility", *Proceedings of the IEEE International Conference on Digital Ecosystems and Technologies (DEST'07)*, Los Alamitos, CA: IEEE Computer Society, pp. 535–540.

Keller, G., and T. Teufel (1998) *SAP R/3 Process Oriented Implementation: Iterative Process Prototyping,* Boston, MA: Addison-Wesley Professional.

Kriksciuniene, D., and S. Strigunaite (2010) "Self-adapting Intelligent Business Processes Execution Analysis" in Abramowicz, W., R. Tolksdorf, and K. Wecel (eds.), *Proceedings of the International Workshops on Business Information Systems (BIS'10), volume 57, Lecture Notes in Business Information*, Heidelberg, Germany: Springer, pp. 29–32.

Lambert, J., R. Jennings, and N. Joshi (2006) "Integration of Risk Identification with Business Process Models", *Systems Engineering*, (9)3, pp. 187–198.

Lee, P. (2011) "UBS Rogue Trader Exploited ETF Settlement Loophole", *Euromoney*, http://www.euromoney.com/Article/2902786/UBS-rogue-trader-exploited-ETF-settlement-loophole.html (current April 15, 2013).

Lenz, K., and A. Oberweis (2003) "Interorganizational Business Process Management with XML Nets" in Ehrig, H., W. Reisig, G. Rozenberg, and H. Weber (eds.), *Petri Net Technology for Communication-based Systems, volume 2472, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 243–263.

Loehndorf, N., E. Petzel, T. Portmannss (2007) "Effective Enterprise Risk Management—Quantifying Operational Risks and Selecting Efficient Risk Mitigation Measures", *Enterprise Risk Management Symposium*, Chicago, IL, March 28–30, 2007, http://www.ermsymposium.org/2007/pdf/papers/Loehndorf.pdf (current April 15, 2013).

Lohmann, N. (2011) "Compliance by Design for Artifact-centric Business Processes" in Rinderle-Ma, S., F. Toumani, K. Wolf (eds.), *Proceedings of the Nineth International Conference on Business Process Management (BPM'11), volume 6896, Lecture Notes in Computer Science*, Heidelberg, Germany, Dordrecht, Netherlands, London, UK, New York: Springer, pp. 99–115.

Lu, R., S. Sadiq, and G. Governatori (2007) "Compliance Aware Business Process Design" in ter Hofstede, A., B. Benatallah, and H. Paik (eds.), *Proceedings of the International Workshops on Business Process Intelligence (BPI), Business Process Design (BPD), Collaborative Business Processes (CBP), Process Support for Healthcare (ProHealth), Reference Modeling (RefMod), Advances in Semantics for Web Services (semantics4ws), The International Conference on Business Process Management Workshops (BPM'07), volume 4928, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany, New York: Springer, pp. 120–131.

Lund, M.S., B. Solhaug., and K. Stolen (2011) *Model-driven Risk Analysis—The CORAS Approach*, Berlin/Heidelberg, Germany: Springer.

Ly, L., S. Rinderle-Ma, and P. Dadam (2010) "Design and Verification of Instantiable Compliance Rule Graphs in Process-aware Information Systems" in Pernici, B. (ed.), *Proceedings of the Twenty-second International Conference on Advanced Information Systems Engineering (CAiSE'10), volume 6051, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany, New York: Springer, pp. 9–23.

Mansour, R., and U. Murthy (2007) "Consideration of Risks and Internal Controls in Business Process Modeling" in Österle, H., J. Schelp, and R. Winter (eds.), *Proceedings of the Fifteenth European Conference on Information Systems (ECIS'07)*, St. Gallen, Switzerland: University of St. Gallen, pp. 588–599.

March, S., and G. Smith (1995) "Design and Natural Science Research on Information Technology", *Decision Support Systems*, (15)4, pp. 251–266.

Metropolis, N. (1987) "The Beginning of the Monte Carlo Method", *Los Alamos Science, Special Issue*, pp. 125–130.

Meyer, B. (1990) *Introduction to the Theory of Programming Languages*, Upper Saddle River, NJ: Prentice-Hall.

Milner, R. (1999) *Communicating and Mobile Systems: The Pi Calculus*, Cambridge University Press.

Mock, R., and M. Corvo (2005) "Risk Analysis of Information Systems by Event Process Chains", *International Journal of Critical Infrastructures*, (1)2–3, pp. 247–257.

Montagut, F., and R. Molva (2007) "Traceability and Integrity of Execution in Distributed Workflow Management Systems" in Biskup, J., and J. Lopez (eds.), *Proceedings of the Twelfth European Symposium on Research in Computer Security (ESORICS'07), volume 4734, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 251–266.

Namiri, K., and N. Stojanovic (2007) "Pattern-based Design and Validation of Business Process Compliance" in Meersman, R., and Z. Tari (eds.), *Proceedings of the Confederated International Conferences—CoopIS, DOA, ODBASE, GADA, and IS, On the Move to Meaningful Internet Systems (OTM'07), volume 4803, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 59–76.

Neiger, D., L. Churliov, M. zur Muehlen, and M. Rosemann (2006) "Integrating Risks in Business Process Models with Value Focused Process Engineering", *Proceedings of the Fourteenth European Conference on Information Systems (ECIS'06),* Association for Information Systems, http://aisel.aisnet.org/ecis2006/122/ (current April 15, 2013).

Neubauer, T., and J. Heurix (2008) "Defining Secure Business Processes with Respect to Multiple Objectives", *Proceedings of the Third International Conference on Availability, Reliability and Security (ARES'08)*, Los Alamitos, CA: IEEE Computer Society, pp. 187–194.

Neubauer, T., M. Klemen, and S. Biffl (2005) "Business Process-based Valuation of IT-security" in Sullivan, K. (ed.), *Proceedings of the Seventh International Workshop on Economics-driven Software Engineering Research (EDSER'05)*, New York: ACM, pp. 1–5.

Neubauer, T., M. Klemen, and S. Biffl (2006) "Secure Business Process Management: A Roadmap", *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*, IEEE Computer Society, Los Alamitos, CA, pp. 457–464.

Neubauer, T., and M. Pehn (2010) "Workshop-based Risk Assessment for the Definition of Secure Business Processes" in Atzenbeck, C., O. Dini, M. Hitson, and B. Jerman-Blazic (eds.), *Proceedings of the Second International Conference on Information, Process, and Knowledge Management (eKNOW'10)*, Los Alamitos, CA: IEEE Computer Society, pp. 74–79.

Office of Government Commerce (2007) *Management of Risk: Guidance for Practitioners*, London, UK.

OMG (2008) *Business Process Model and Notation, V1.1,* Object Management Group, OMG Document Number: formal/2008-01–17.

OMG (2011a) *OMG Unified Modeling Language (OMG UML), Infrastructure—Version 2.4.1*, Object Management Group.

OMG (2011b) *OMG Unified Modeling Language (OMG UML), Superstructure—Version 2.4.1*, Object Management Group.

Orriëns, B., W. van den Heuvel, and M. Papazoglou (2009) "On the Risk Management and Auditing of SOA Based Business Processes" in Margaria, T., and B. Steffen (eds.), *Proceedings of the Third International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA'08), volume 17, Communications in Computer and Information Science*, Berlin/Heidelberg, Germany: Springer, pp. 124–138.

Osterwalder, A. (2004) *The Business Model Ontology*, Ph.D. thesis, Universite de Lausanne, Ecole des Hautes Etudes Commerciales, http://www.hec.unil.ch/aosterwa/phd/osterwalder_phd_bm_ontology.pdf (current April 15, 2013).

Panayiotou, N., S. Oikonomitsios, C. Athanasiadou, and S. Gayialis (2010) "Risk Assessment in Virtual Enterprise Networks: A Process-driven Internal Audit Approach" in Ponis, S. (ed.), *Managing Risk in Virtual Enterprise Networks: Implementing Supply Chain Principles*, Hershey, PA: IGI Global, pp. 290–312.

Rausch, T. (2006) "Holistic Business Process and Compliance Management", *Proceedings of the Fourteenth International Conference on Systems Integration (SI'06),* pp. 301–310, http://si.vse.cz/archive/index.asp?volume=2006 (current April 15, 2013).

Rieke, T. (2009) *Prozessorientiertes Risikomanagement—Ein informationsmodellorientierter Ansatz,* Ph.D. thesis, Westfälische Wilhelms-Universität Münster.

Rieke, T., and A. Winkelmann (2008) "Modellierung und Management von Risiken: Ein prozessorientierter Risikomanagement-Ansatz zur Identifikation und Behandlung von Risiken in Geschäftsprozessen", *Wirtschaftsinformatik*, (50)5, pp. 346–356.

Rikhardsson, P., P. Best, P. Green, and M. Rosemann (2006) "Business Process Risk Management and Internal Control: A Proposed Research Agenda in the Context of Compliance and ERP Systems", *Proceedings of the Second Asia/Pacific Research Symposium on Accounting Information Systems*, Melbourne, Australia, June 20, 2006.

Rockafellar, R., and S. Uryasev (2000) "Optimization of Conditional Value-at-Risk", *Journal of Risk*, (2)3, pp. 21–41.

Rodríguez, A., E. Fernández-Medina, and M. Piattini (2006a) "Capturing Security Requirements in Business Processes Through a UML 2.0 Activity Diagrams Profile" in Roddick, J., V. Benjamins, S. Cherfi, R. Chiang, C. Claramunt, R. Elmasri, F. Grandi, H. Han, M. Hepp, M. Lytras, V. Misic, G. Poels, I. Song, J. Trujillo, and C. Vangenot (eds.), *Advances in Conceptual Modeling—Theory and Practice, Proceedings of the ER'06 Workshops BP-UML, CoMoGIS, COSS, ECDM, OIS, QoIS, SemWAT, volume 4231, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 32–42.

Rodríguez, A., E. Fernández-Medina, and M. Piattini (2006b) "Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes" in Fischer-Hübner, S., S. Furnell, and C. Lambrinoudakis (eds.), *Proceedings of the Third International Conference on Trust and Privacy in Digital Business (TrustBus'06), volume 4083, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 51–61.

Rodríguez, A., E. Fernández-Medina, and M. Piattini (2007) "Analysis-level Classes from Secure Business Processes Through Model Transformations" in Lambrinoudakis, C., G. Pernul, and A. Tjoa (eds.), *Proceedings of the Fourth International Conference on Trust, Privacy and Security in Digital Business (TrustBus'07), volume 4657, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 104–114.

Rodríguez, A., I. García-Rodríguez de Guzmán, E. Fernández-Medina, and M. Piattini (2010) "Semi-formal Transformation of Secure Business Processes into Analysis Class and Use Case Models: An MDA Approach", *Information and Software Technology*, (52)9, pp. 945–971.

Rosemann, M., and M. zur Muehlen (2005) "Integrating Risks in Business Process Models", *Proceedings of the Sixteenth Australasian Conference on Information Systems (ACIS'05)*, Association for Information Systems. http://aisel.aisnet.org/acis2005/50/ (current April 15, 2013).

Rotaru, K., C. Wilkin, L. Churilov, and D. Neiger (2008) "Formalising Risk with Value-focused Process Engineering" in Golden, W., T. Acton, K. Conboy, H. van der Heijden, and V. Tuunainen (eds.), *Proceedings of the Sixteenth European Conference on Information Systems (ECIS'08)*, National University of Ireland, Galway, Ireland, pp. 1583–1595.

Rotaru, K., C. Wilkin, L. Churilov, D. Neiger, and A. Ceglowski (2009) "Formalizing Process-based Risk with Value-focused Process Engineering", *Information Systems and e-Business Management*, (9)4, pp. 1–28.

Ruffolo, M., R. Curia, and L. Gallucci (2005) "Process Management in Health Care: A System for Preventing Risks and Medical Errors" in van der Aalst, W., B. Benatallah, F. Casati, and F. Curbera (eds.), *Proceedings of the Third International Conference on Business Process Management (BPM'05), volume 3649, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 334–343.

Sackmann, S. (2008) "A Reference Model for Process-oriented IT Risk Management" in Golden, W., T. Acton, K. Conboy, H. van der Heijden, and V. Tuunainen (eds.), *Proceedings of the Sixteenth European Conference on Information Systems (ECIS'08),* National University of Ireland, Galway, Ireland, pp. 1346–1357.

Sadiq, S., G. Governatori, and K. Namiri (2007) "Modeling Control Objectives for Business Process Compliance" in Alonso, G., P. Dadam, and M. Rosemann (eds.), *Proceedings of the Fifth International Conference on Business Process Management (BPM'07), volume 4714, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 149–164.

Salmela, H. (2007) "Analysing Business Losses Caused by Information Systems Risk: A Business Process Analysis Approach", *Journal of Information Technology*, (23)3, pp. 185–202.

Schmitt, M., B. Grégoire, and E. Dubois (2005) "A Risk Based Guide to Business Process Design in Interorganizational Business Collaboration" in Cox, K., E. Dubois, Y. Pigneur, S. Bleistein, J. Verner, A. Davis, and R. Wieringa (eds.), *Proceedings of the First International Workshop on Requirements Engineering for Business Need and IT Alignment (REBNITA'05), The Thirteenth IEEE International Conference on Requirements Engineering (RE'05)*, University of New South Wales Press, Sydney, Australia.

Searle, S. (2011) "BPM Survey Insights: Organizations Using BPM to Reduce Costs and Improve Process Quality", *Gartner*, http://www.gartner.com/id=1729244 (current April 15, 2013).

Sienou, A. (2009) *Proposition d'un cadre méthololodogique pour le management intégré des risques et des processus d'entreprise,* Ph.D. thesis, Centre de Génie Industriel, Mines Albi, Université de Toulouse.

Sienou, A., A. Karduck, E. Lamine, and H. Pingaud (2008a) "Business Process and Risk Models Enrichment: Considerations for Business Intelligence", *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'08)*, Los Alamitos, CA: IEEE Computer Society, pp. 732–735.

Sienou, A., A. Karduck, and H. Pingaud (2006) "Towards a Framework for Integrating Risk and Business Process Management" in Dolgui, A., G. Morel, and C. Pereira (eds.), *Proceedings of the Twelfth Triennial IFAC Symposium on Information Control Problems in Manufacturing (INCOM'06)*, Elsevier, pp. 615–620.

Sienou, A., E. Lamine, A. Karduck, and H. Pingaud (2007) "Conceptual Model of Risk: Towards a Risk Modelling Language" in Weske, M., M. Hacid, and C. Godart (eds.), *Proceedings of the International Workshops on Web Information Systems Engineering (WISE'07), volume 4832, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 118–129.

Sienou, A., E. Lamine, A. Karduck, and H. Pingaud (2008b) "Towards a Semi-formal Modeling Language Supporting Collaboration Between Risk and Process Manager", *Proceedings of the Second IEEE International Conference on Digital Ecosystems and Technologies (DEST'08)*, Los Alamitos, CA: IEEE Computer Society, pp. 119–125.

Sienou, A., E. Lamine, and H. Pingaud (2008c) "A Method for Integrated Management of Process Risk", in Sadiq, S., M. Indulska, M. zur Muehlen (eds.), *Proceedings of the First International Workshop on Governance, Risk and Compliance—Applications in Information Systems (GRCIS'08), The Twentieth International Conference on Advanced Information Systems Engineering (CAiSE'08)*, pp. 16–30, http://ceur-ws.org/Vol-339/paper2.pdf (current April 15, 2013).

Sienou, A., E. Lamine, H. Pingaud, and A. Karduck (2009) "Aspects of the BPRIM Language for Risk Driven Process Engineering" in Meersman, R., P. Herrero, and T. Dillon (eds.), *Proceedings of the On the Move to Meaningful Internet Systems: OTM Confederated International Workshops and Posters, ADI, CAMS, EI2N, ISDE, IWSSA, MONET, OnToContent, ODIS, ORM, OTM Academy, SWWS, SEMELS, Beyond SAWSDL, and COMBEK 2009, volume 5872, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 172–183.

Sienou, A., F. Lamine, H. Pingaud, and A. Karduck (2010) "Risk Driven Process Engineering in Digital Ecosystems: Modelling Risk", *Proceedings of the Fourth IEEE International Conference on Digital Ecosystems and Technologies (DEST'10)*, Los Alamitos, CA: IEEE Computer Society, pp. 647–650.

Silver, M. (2011) "The Fine Line Between Bad Luck and Rogue Trades", *CNN Money*, http://finance.fortune.cnn.com/2011/09/27/the-fine-line-between-bad-luck-and-rogue-trades/ (current April 15, 2013).

Singh, P., F. Gelgi, H. Davulcu, S. Yau, and S. Mukhopadhyay (2008) "A Risk Reduction Framework for Dynamic Workflows", *Proceedings of the IEEE International Services Computing Conference (SCC'08)*, Los Alamitos, CA: IEEE Computer Society, pp. 381–388.

Standards Australia and Standards New Zealand (2009) *Risk Management: Principles and Guidelines, third edition (AS/NZS ISO 31000:2009)*, Sydney, Australia, Wellington, New Zealand.

Strecker, S., D. Heise, and U. Frank (2011) "RiskM: A Multi-perspective Modeling Method for IT Risk Assessment", *Information Systems Frontiers*, (13)4, pp. 595–611.

Taubenberger, S., and J. Jürjens (2008) "IT Security Risk Analysis Based on Business Process Models Enhanced with Security Requirements" in Whittle, J., J. Jurjens, B. Nuseibeh, and G. Dobson (eds.), *Proceedings of the First International Modeling Security Workshop (MODSEC'08), The Eleventh International Conference on Model Driven Engineering Languages and Systems (MODELS'08)*, http://ceur-ws.org/Vol-413/paper16.pdf (current April 15, 2013).

Taylor, P., J. Godino, and B. Majeed (2008) "Use of Fuzzy Reasoning in the Simulation of Risk Events in Business Processes" in Louca, L., Y. Chrysanthou, Z. Oplatkova, and K. AlBegain (eds.), *Proceedings of the Twenty-second European Conference on Modelling and Simulation (ECMS'08)*, pp. 25–30, http://www.scs-europe.net/conf/ecms2008/ecms2008%20CD/ecms2008%20pdf/ECMS2008.pdf (current April 15, 2013).

ter Hofstede, A.H.M., W. van der Aalst, M. Adams, and N. Russell (2010) *Modern Business Process Automation: YAWL and Its Support Environment*, Chapter 1, Introduction, Heidelberg, Germany, Dordrecht, Netherlands, London, UK, New York: Springer, pp. 3–19.

Tjoa, S., S. Jakoubi, G. Goluch, G. Kitzler, S. Goluch, and G. Quirchmayr (2011) "A Formal Approach Enabling Risk-aware Business Process Modeling and Simulation", *IEEE Transactions on Services Computing*, (4)2, pp. 153–166.

Tjoa, S., S. Jakoubi, G. Goluch, and G. Quirchmayr (2008a) "Extension of a Methodology for Risk-aware Business Process Modeling and Simulation Enabling Process-oriented Incident Handling Support", *Proceedings of the Twenty-second International Conference on Advanced Information Networking and Applications (AINA'08)*, Los Alamitos, CA: IEEE Computer Society, pp. 48–55.

Tjoa, S., S. Jakoubi, S. Goluch, and G. Kitzler (2010) "Planning Dynamic Activity and Resource Allocations Using a Risk-aware Business Process Management Approach", *Proceedings of the Fifth International Conference on Availability, Reliability and Security (ARES'10)*, Los Alamitos, CA, Tokyo, Japan: IEEE Computer Society, pp. 268–274.

Tjoa, S., S. Jakoubi, and G. Quirchmayr (2008b) "Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-aware Business Process Modeling and Simulation Methodology", *Proceedings of the Third International Conference on Availability, Reliability and Security (ARES'08)*, Los Alamitos, CA: IEEE Computer Society, pp. 179–186.

Treanor, J., S. Bowers, and S. Jones (2011) "'Rogue trader' Kweku Adoboli Faces Fraud Charges Dating Back to 2008", *The Guardian*, http://www.guardian.co.uk/business/2011/sep/17/kweku-adoboli-ubs-fraud-charges (current April 15, 2013).

U.S. Department of Defense (1949) *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*.

van der Aalst, W. (2011) *Process Mining—Discovery, Conformance and Enhancement of Business Processes*, Heidelberg, Germany, Dordrecht, Netherlands, London, UK, New York: Springer.

Vollmer, K., G. Leganza, M. Pilecki, and K. Smillie (2008) "The EA View: BPM Has Become Mainstream", *Forrester,* http://www.forrester.com/The+EA+View+BPM+Has+Become+Mainstream/fulltext/-/E-RES43191 (current April 15, 2013).

vom Brocke, J., A. Simons, B. Niehaves, B. Niehaves, K. Reimer, R. Plattfaut, and A. Cleven (2009) "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process", *Proceedings of the Seventeenth European Conference on Information Systems (ECIS'09)*, pp. 2206–2217.

van Dongen, B., A. de Medeiros, H. Verbeek, A. Weijters, and W. van der Aalst (2005) "The ProM Framework: A New Era in Process Mining Tool Support" in Ciardo, G., and P. Darondeau (eds.), *Proceedings of the Twenty-sixth International Conference on Applications and Theory of Petri Nets (ICATPN'05), volume 3536, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 1105–1116.

W3C (2004) *OWL Web Ontology Language—Overview,* http://www.w3.org/TR/owl-features/ (current April 15, 2013).

Wahler, B. (2005) "Process Managing Operational Risk: Developing a Concept for Adapting Process Management to the Needs of Operational Risk in the Basel II Framework", *Social Science Research Network*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=674221 (current April 15, 2013).

Wainer, J., A. Kumar, and P. Barthelmess (2007) "DW-RBAC: A Formal Security Model of Delegation and Revocation in Workflow Systems", *Information Systems*, (32)3, pp. 365–384.

Wang, Q., and N. Li (2007) "Satisfiability and Resiliency in Workflow Systems" in Biskup, J., and J. Lopez (eds.), *Proceedings of the Twelfth European Symposium on Research in Computer Security (ESORICS'07), volume 4734, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 90–105.

Weiß, B., and A. Winkelmann (2011) "Developing a Process-oriented Notation for Modeling Operational Risks—A Conceptual Metamodel Approach to Operational Risk Management in Knowledge Intensive Business Processes Within the Financial Industry", *Proceedings of the Forty-fourth Hawaii International Conference on Systems Science (HICSS'11)*, Los Alamitos, CA: IEEE Computer Society, pp. 1–10.

Weist, P., A. Deokar (2008) "A Knowledge-based Approach for Business Process Risk Management", *Proceedings of the Third Annual Midwest Association for Information Systems Conference (MWAIS'08)*, Association for Information Systems, http://aisel.aisnet.org/mwais2008/21/ (current April 15, 2013).

Wickboldt, J., L. Bianchin, R. Lunardi, L. Granville, L. Gaspary, and C. Bartolini (2011) "A Framework for Risk Assessment Based on Analysis of Historical Information of Workflow Execution in IT Systems", *Computer Networks*, (55)13, pp. 2954–2975.

Wolter, C., and A. Schaad (2007) "Modeling of Task-based Authorization Constraints in BPMN" in Alonso, G., P. Dadam, and M. Rosemann (eds.), *Proceedings of the Fifth International Conference on Business Process*

Management (BPM'07), volume 4714, Lecture Notes in Computer Science, Berlin/Heidelberg, Germany: Springer, pp. 64–79.

Xiangpeng, Z., A. Cerone, and P. Krishnan (2006) "Verifying BPEL Workflows Under Authorisation Constraints" in Dustdar, S., J. Fiadeiro, and A. Sheth (eds.), *Proceedings of the Fourth International Conference on Business Process Management (BPM'06), volume 4102, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany: Springer, pp. 439–444.

Xie, K., J. Liu, and Y. Chen (2007) "A Theoretical and Empirical Analysis of Risk Management in Business Process", *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'07)*, Los Alamitos, CA: IEEE Computer Society, pp. 6503–6506.

Yu, Z. (2011) "A Business Process-based Risk Evaluation Framework", *Advanced Materials Research*, (230), pp. 1024–1028.

Zambon, E., D. Bolzoni, S. Etalle, and M. Salvato (2007) "A Model Supporting Business Continuity Auditing & Planning in Information Systems", *Proceedings of the Second International Conference on Internet Monitoring and Protection (ICIMP'07)*, Los Alamitos, CA: IEEE Computer Society, pp. 33–33.

zur Muehlen, M., A. Baumgart, and C. Junkers (2006) "A Procedure Model for the Identification of Risk in Business Processes", Technical Report, Center of Excellence in Business Process Innovation, Stevens Institute of Technology, Hoboken, NJ.

zur Muehlen, M., and D. Ho (2005) "Risk Management in the BPM Lifecycle" in Bussler, C., and A. Haller (eds.), *Proceedings of the International Workshops, BPI, BPD, ENEI, BPRM, WSCOBPM, BPS, The Third International Conference on Business Process Management (BPM'05), volume 3812, Lecture Notes in Computer Science*, Berlin/Heidelberg, Germany, New York: Springer, pp. 454–466.

ABOUT THE AUTHORS

bio

APPENDIX A: ACADEMIC FORUMS

Relevant papers were drawn from the following journals, conferences, and workshops (2005–September 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 & 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: DETAILED EVALUATION CRITERIA DESCRIPTION

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 redesigning 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 capture only 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 provides only *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 that 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 modeling constructs that can be operationalized to *comprehensively* monitor risk and/or to influence the execution behavior of process instances.
- (±): The approach proposes a *limited* set of executable risk modeling 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 modeling constructs *cannot* be executed or 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*
  - (+): 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.
  - (±): 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.
  - (−): 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.
  - N/A: The approach does not propose any new risk-related constructs.
- *Concrete Syntax*
  - (+): The approach specifies the concrete syntax of *all* (or *most*) of the proposed risk-related constructs.
  - (±): 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).
  - (−): The approach does *not* specify *any* concrete syntax for the proposed risk-related constructs.
  - N/A: The approach does not propose any new risk-related constructs.
- *Semantics*
  - (+): The semantics of *all* (or *most*) of the proposed risk constructs is defined using proper formal technique(s).
  - (±): The approach defines only the semantics of a *small subset* of the proposed risk-related constructs (the semantics of many of the proposed constructs is left unspecified).
  - (−): 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 language.
  - 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, on the other hand, is 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 make use of, to a varying degree, risk-related construct(s).

Implementation

- (+): The approach has been fully implemented (that is, it can be used as a fully functioning tool), or is already supported by existing tool(s).
- (±): The approach has been only 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, or the approach can readily apply existing well-accepted methodology.
- (±): 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 question of 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 mentions only certain standards without any further elaboration or evidence demonstrating the incorporation of the standards in the approach.

APPENDIX C: DETAILED EVALUATION OF DESIGN-TIME R-BPM APPROACHES (WITH INTEGRATED RISK CONSTRUCTS)

This section provides a detailed evaluation of all approaches surveyed in this article 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 et al., 2008a; Tjoa et al., 2010; Tjoa et al., 2008b; Tjoa et al., 2011; Jakoubi et al., 2007; Jakoubi et al., 2010a; Jakoubi et al., 2010b; Jakoubi et al., 2009b; Jakoubi et al., 2008; Jakoubi and Tjoa, 2009; Goluch et al., 2008]. This approach proposes a three-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 [2007]) is used also to inform the design of the CARE and TIP layers. This ROPE-based model then can 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" as coined in Rosemann and zur Muehlen [2005]. This approach 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 be used also 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 process and risk elements in the three-layer model described above. The key components and structure of the proposed notations are not specified; thus, the *abstract syntax* criterion is not supported (−).[6] 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 et al., 2008]; thus, the *implementation* criterion is partially supported. A high-level application method is also described; thus, the *application method* criterion is partially supported. This approach has been applied only 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 et al., 2010, 2008a, 2007, 2009, 2008b, 2006, 2008c; Karduck et al., 2007; 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 relevant 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 and resource) and RM (such as risk event) are explicitly studied and modeled (using UML 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 (e.g., risk factor, risk probability, and risk countermeasure) is proposed.

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 (±).

[6] While no abstract syntax is provided, a security ontology was proposed [Ekelhart, Fenz, Klemen, and Weippl, 2007].

In terms of the BPM lifecycle, 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* stage criterion: while the proposed notations can be used to capture risk analysis concepts (such as the causal chain of a set of risks [Sienou, 2009]), there is no specific risk analysis technique proposed. The rest of the BPM lifecycle stages also are 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 a well-known formal technique. Similarly, the external graphical representation of these notations (that is, the concrete syntax) also is 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. 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 also is not supported, as this approach has not been applied in practice.

DI03—Cope et al.

In Cope et al.'s approach [2010b, 2009, 2010a], a number of risk-related modeling constructs are proposed. These constructs are an extension of the Business Process Modelling 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 it incorporates any specific risk standards, but it 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. The risk-annotated process model also can be translated into quantitative graphical models, such as a Bayesian network, to enable formal risk analysis of the process, although it is not clear, from the related papers, to what extent such a formal analysis has been conducted by the authors. 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 also is 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 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—Weiß and Winkelmann

In Weiß and Winkelmann's approach [2011], the Semantic Business Process Modelling Language (SBPML) [Becker, Thome, Weiß 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 types) 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 *finance* domain. It addresses a type of risk commonly encountered in the financial industry, called the *operational risk.* However, one can deduce from the original paper [Weiß and Winkelmann, 2011] that what constitutes an operational risk can include many types of risk. For example, the system failure risk and the erroneous data entry risk alluded in the paper can be mapped to the "technology risk" and the "data risk" respectively. 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. 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 also are 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 [2008] addresses business process risk in the context of business continuity management. Building on 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; 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 that manipulate this extended goal-risk framework also are proposed.

The proposed analysis techniques apply 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 a sufficient amount of risk-related information to be modeled; thus, the *design* stage criterion is fully supported (+). Furthermore, two analysis techniques that can be used to select the most cost-efficient risk countermeasure plan(s) also are proposed and formally defined. Therefore, the *design-time analysis* stage criterion also is 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 [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 also can be captured. To complement these constructs, this approach demonstrates the application of the Failure Mode and Effects Analysis (FMEA) risk analysis [U.S. 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* stage 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 also are missing; thus, the *semantics* criterion also is 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 nondisclosure 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 [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 also is 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. 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 also is 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 et al., 2008, 2009; Neiger et al., 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 et al., 2008]. Their earlier work [Neiger et al., 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* stage criterion is partially supported (±): while a risk analysis technique is proposed in their earlier work [Neiger et al., 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 also is 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 also is supported. This approach proposes several rules or constraints to formalize the notion of a risk-aware e-EPC model. These rules/constraints can be considered as the *static* semantics of the constructs [Meyer, 1990]. However, the *execution* semantics of the constructs is not given; therefore, 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 also is not supported, as there is no evidence that this approach has been applied in real-world organization(s).

DI09—Betz et al.

In Betz et al.'s work [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 the activities of a process. 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 risk construct proposed. In fact, it is not clear whether the risk construct proposed 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 also has been supported by an *implementation* using the KIT-Horus business process modeling tool.[7] This approach has not been validated in practice.

DI10—Herrmann and Herrmann

Herrmann and Herrmann's proposed approach [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 predefined 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.

[7] http://www.aifb.kit.edu/web/KIT-Horus/en

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 a *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* stage criterion is partially supported (±). The rest of the BPM lifecycle stages are not addressed by this approach.

The *concrete syntax* criterion is supported because a set of graphical notations to depict security requirements is proposed. 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 has been implemented (thus, the *implementation* criterion is supported), and there are detailed step-by-step instructions to guide users in the application of this approach (hence, the *application methods* criterion also is supported). However, there is no evidence that this approach has been applied in practice.

DI11—Strecker et al.

In Strecker et al.'s [2011] approach, 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 risk events, risk countermeasure activities, and risk propagations) is developed using the MEMO MML as the "conceptual foundation" [Strecker et al., 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 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 a UML class diagram), which 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. Nevertheless, this approach 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 a real-world organization. A high-level description of how this approach can be applied is provided, thus, the *application methods* criterion is partially supported.

DI12—Karagiannis et al.

The work by Karagiannis et al. [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 annotations can inform the modification of the process model through the addition of control activities. A six-step framework that can be used to realize a risk-aware business process management system is proposed.

This approach is mainly prescribed for the finance domain. The risk of regulation noncompliance, addressed in this approach, is a form of *structural* risk because it mainly originates from errors (such as wrong choices), committed during process design [Rosemann and zur Muehlen, 2005] that permit the noncompliant activities to occur (such as insufficient implementation of control activities in the process). This approach clearly is 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-related information within a process model. Furthermore, this approach also 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* stage 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.[8] This approach has been adopted by an insurance company based in the United States; thus, the *application in practice* criterion is also supported. Similarly, the *application methods* criterion is supported, as a detailed six-step application framework is provided.

DI13—Taylor et al.

In Taylor et al.'s approach [2008], a simulation environment is developed using the jBPM[9] stack and the jBPM Process Definition Language (JPDL). Several risk-related constructs, such as the key risk indicator (KRI), the key performance indicator (KPI), and the 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 a simulation-based technique for the purpose of risk analysis. Therefore, we consider the *design-time analysis* stage criterion to be partially supported (±). The rest of the BPM lifecycle stages are not addressed by this approach.

This approach does not support the *abstract syntax* criterion, as it does not provide a 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 shown only 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 [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), which can be used to aid the application of the proposed approach,

[8] http://www.adonis-community.com
[9] http://www.jboss.org/jbpm

are provided. A number of risk-related constructs, which can be used to annotate process models with risk-related information (such as risk mitigation activities), are also proposed.

This approach is developed mainly for the supply chain domain, and it 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 (±): while risk constructs were proposed, they are not properly explained and detailed. This approach also provides partial support for the *design-time analysis* stage criterion: it proposes a technique to perform risk evaluation during design-time; however, the proposed technique is informal. The rest of the BPM lifecycle stages are not addressed by this approach.

The graphical representation of the proposed risk constructs are shown in the approach; therefore, the *concrete syntax* criterion is supported (+). However, the deep structure of the proposed constructs (such as their attributes) is described only informally, 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 also is supported, as detailed guidelines of the application of this approach are provided (in the form of a four-stage application methodology). While this approach may have been applied in practice [Panayiotou et al., 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 [2006], the Integrated Definition (IDEF) language [Federal Information Processing Standards, 1993] is used to model business processes and is extended to allow the source of risk to be included in 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 the BPM lifecycle is partially supported 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 (±). 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 of 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 of the meaning of the proposed construct. Thus, the *semantics* criterion also is not supported. There is no evidence that this approach has been implemented; thus, the *implementation* criterion is not supported. This approach provides high-level guidance on how it 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.

DI16—Bai et al.

In Bai et al.'s work [Bai et al., 2007; Bagchi et al., 2006], business process models are represented as graphs (nodes representing tasks and arcs representing gateways). A precedence matrix is used also 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], and it is not prescribed for any particular type of risk or domain. There is no evidence that this approach is informed by any existing risk standard.

The *design* stage of the BPM lifecycle is partially supported (±): a comprehensive set of risk-related models (namely the error and control models) is proposed. However, it is not evident that the precedence matrix, used in this approach, is able to capture a more elaborate 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; therefore, the *design-time analysis* stage criterion is supported (+). 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 their structure. 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. This approach also does not provide a precise specification of the meaning of the proposed constructs; thus, no support (−) for the *semantics* criterion is given. 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: DETAILED EVALUATION OF DESIGN-TIME R-BPM APPROACHES (WITHOUT INTEGRATED RISK CONSTRUCTS)

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.

DN01—Bhuiyan et al.

In the work by Bhuiyan et al. [Bhuiyan et al., 2007; Islam et al., 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 *i** framework notations.[10] The results of this analysis then are 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 proposed.

This approach is developed mainly to address organizational risk (per the taxonomy proposed in Rosemann and zur Muehlen [2005]), and its use is not restricted to any particular domain. There is no application of any existing risk analysis technique or any risk standard.

The *design-time analysis* stage are partially supported (±). 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 focuses mainly on quantifying the *impact* of a resource unavailability event; how one can calculate the occurrence *probability* of the related resource unavailability event is not addressed. As explained earlier, this approach supports a form of *risk-informed* business process design; however, there is a lack of detail in terms of how the results of a resources criticality analysis should precisely guide the design of a process model. Therefore, the *design* stage of the BPM lifecycle is partially supported. The rest of the BPM lifecycle stages are not addressed.

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 the *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 et al., 2009; Fenz and Neubauer, 2009], a number of techniques, which can be used to analyze the risks of a business process, 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

[10] http://www.cs.toronto.edu/km/istar/

security ontology proposed by the same authors (expressed using the 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 point of view of the resources (such as IT assets). In other words, this approach addresses the "IT risk" (according to the risk taxonomy proposed in Rosemann and zur Muehlen [2005]). This approach is mainly prescribed for the IT infrastructure domain. This approach is informed somewhat by the NIST 800-30 guidelines (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 criterion is fully supported (+), as the approach provides a comprehensive set of risk analysis techniques that are informed by well-established technical foundations (such as Petri nets and Bayesian networks). 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 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 [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 influenced somewhat by the Failure Modes, Effects, and Criticality Analysis (FMECA) [U.S. Department of Defense, 1949] risk analysis technique; thus, the *risk analysis* criterion is supported.

This approach provides partial support (±) for the *design-time analysis* stage criterion, as it proposes a technique to identify risks in processes. 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-founded theory in the development of the technique. While the FMECA technique is mentioned in the paper [zur Muehlen et al., 2006], 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 is not supported by an *implementation*. The *application methods* criterion is partially supported, as high-level guidance 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 [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, also is 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 is supported by an *implementation*. The *application in practice* criterion also is not supported, as there is no evidence of the application of this approach in a real-world organization. The *application methods* criterion is not supported, as there is a lack of description of methods/guidelines to apply this approach.

DN05—Bergholtz et al.

In Bergholtz et al.'s work [Bergholtz et al., 2005; Andersson et al., 2005; Schmitt et al., 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 e^3-value model notation [Gordijn, Yu, and van der Raadt, 2006]). 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 identification 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 procedure is a *risk-informed* business process model incorporating 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. 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, this approach provides full-support (+) for the *design* stage criterion, as it facilitates a *risk-informed* business process design. 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).[11] There is no *implementation* support provided by this approach. The *application in practice* criterion also is not supported, as this approach has not been applied in a real-world organization. There is a partial support (±) for the *application methods* criterion through the provision of high-level application guidance.

DN06—Jallow et al.

In the work by Jallow et al. [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 simulation [Metropolis, 1987] is applied to assess and quantify the *impact* of the identified risk events (in terms of time, cost, performance, and other objectives) on each process activity and on the overall process.

This approach is developed to address "operational" risks in business processes. However, by studying the examples of "operational" risks used in the paper [Jallow et al., 2007], we see that an "operational" risk can be mapped to many types of risk, as per the risk taxonomy proposed in Rosemann and zur Muehlen [2005]. For example, the inadequate expertise risk and the IT equipment risk mentioned in the paper can be seen as a form of "organizational risk" and "IT risk" respectively. Thus, 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 technique (i.e., the Monte Carlo simulation).

In terms of the BPM lifecycle, this work addresses the *design-time analysis* stage criterion. However, while this approach applies a well-accepted risk analysis technique (i.e., the Monte Carlo simulation technique), it addresses only one dimension of risk analysis (that is, the impact analysis). Therefore, the *design-time analysis* stage criterion is partially 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

[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.

sense that it uses existing software (such as Crystal Ball with Microsoft Excel) to aid the analysis; therefore, the *implementation* criterion is supported. The *application methods* criterion is not supported, as there is no explanation of any guidelines or methods to apply this approach. Similarly, the *application in practice* criterion is not supported, as the approach has not been validated in practice.

DN07—Singh et al.

In the work by Singh et al. [2008], a technique to *evaluate* a workflow's non-completion risk, due to uncertain/dynamic information, is proposed. In the paper [Singh et al., 2008], 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 and the status of traffic at the time of an 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 also is 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, also is briefly described.

The type of risk addressed by this approach is "structural risk" (as per the risk taxonomy proposed in Rosemann and zur Muehlen [2005]) because it looks at how the design of a workflow may become ineffective in attaining some desired goals. The techniques proposed in this approach seem to be generic enough to be applicable to any domain. There is no evidence that this approach applies any existing risk analysis technique, nor is it informed by any existing risk standard.

In terms of the BPM lifecycle, this approach provides partial support (±) for the *design-time analysis* stage criterion because 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 that contains a combination of flow types can be calculated. This approach also describes a technique to design a backup workflow based on historical data; thus, a form of *risk-informed* business process design support is provided. However, the details of this technique are missing in the paper [Singh et al., 2008]. Thus, the *design* stage criterion is only partially supported.

Unlike other approaches considered in this section, this approach claims to allow a backup workflow to be dynamically "modified" at runtime to ensure its consistency with the main workflow. Any inconsistencies detected between the backup workflow and the current running process instance will trigger the regeneration of the backup workflow. However, there is a lack of detail regarding how such monitoring can be performed. Nevertheless, given that this approach takes into account runtime monitoring and analysis, we consider the *runtime analysis* criterion to be partially supported. This approach does not address the *execution* stage nor 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 to apply this approach. Therefore, the *application methods* criterion also is not supported.

APPENDIX E: DETAILED EVALUATION OF RUNTIME R-BPM APPROACHES

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 [2011], a language that 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 reasoned about 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 and the specific risk involved.

The language proposed allows conditions related to organizational risk, structural risk, and data risk 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 risk-related standard, it does apply an existing risk analysis technique, namely fault-tree analysis.

In terms of the BPM lifecycle, the *execution* 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* provide only limited insights into the risks of business processes 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 (−).[12] The *implementation* criterion is supported, as the proposed language and the related runtime risk monitoring capability have been implemented into the YAWL workflow system [ter Hofstede et al., 2010]. The *application in practice* criterion is not supported (−), as this approach has not been applied in a real-world organization. A detailed step-by-step instruction, 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 [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, this approach supports (+) the *runtime analysis* criterion through the proposal of a runtime risk monitoring technique. 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 method to apply this approach is provided; thus, the *application methods* criterion is partially supported (±).

APPENDIX F: DETAILED EVALUATION OF POST-EXECUTION R-BPM APPROACHES

This section provides a detailed evaluation of all surveyed approaches that address the *post-execution* stage of an R-BPM. The evaluation results are summarized in Table 6.

PE01—Jans et al.

In the work by Jans et al. [2011a, 2008, 2011b], 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 tool[14] 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 that were not detected during traditional internal audit process [Jans et al., 2011a].

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

[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.
[14] http://www.promtools.org/prom6/

In terms of the BPM lifecycle, 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 seems to follow the process mining methodology [van der Aalst, 2011]; therefore, the *application methods* criterion is supported. Finally, the *application in practice* criterion is also supported, as it has been applied in practice.

PE02—Wickboldt et al.

In Wickboldt et al's approach [2011], historical information (such as logs) from business processes is annotated with a number of risk-related constructs, such that various types of risk analyses 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 prescribed for the domain of IT, and the type of risk addressed is generic. This approach is strongly influenced by a number of risk management standards, 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, 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.

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.[15] Thus, the *abstract syntax* criterion is supported. Nevertheless, there is no specification of how these constructs are to be represented in the log. Therefore, the *concrete syntax* criterion is not supported. Similarly, this approach does not provide a precise definition of the meaning of the proposed constructs; thus, the *semantics* criterion is not supported (−). This approach is supported by an *implementation*. However, it is not evident that this approach has been applied in practice.[16] 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] The applicability of this approach has been validated within the context of the CHANGELEDGE system [da Costa Cordeiro 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, because the system was a prototype and the evaluation used emulated data.

Author writeups?

Communications of the Association for Information Systems

ISSN: 1529-3181

Communications of the Association for Information Systems