

# A Method for Integrated Management of Process-risk

Amadou Sienou<sup>1</sup>, Elyes Lamine<sup>1</sup>, Hervé Pingaud<sup>1</sup>

<sup>1</sup>Université de Toulouse-Mines d'Albi, Centre de Génie Industriel  
Campus Jarlard Route de Teillet, 81 013 Albi Cedex 09, France  
{sienou, lamine, pingaud}@enstimac.fr

**Abstract.** Process management techniques such as process modeling contribute to improve organization's maturity with regard to the achievement of agility, performance, and value creation. However, today's organizations are exposed to frequent changes and incidents, which constrain performance, and value preservation. These constraints are addressed in the context of risk management, which is an approach to make informed decisions under uncertainties. Given that risk management contributes to increase the level of confidence with regard to value preservation, management of uncertainties in the context of business processes is inevitably based on an improvement of the relations between process management and risk management. We suggested a multi-layer integration of both management processes. Emphasizing the design phase of business processes, a method support for robust process management is proposed.

**Keywords:** Risk management, process design, conceptual modeling, modeling language, method engineering, meta model.

## 1 Introduction

Nowadays organizations are exposed to frequent changes requiring continuous alignment of business processes on business strategies. This agility requires management practices, methods, tools and technologic enabler. The Business Process Management paradigm is as a potential enabler affecting technologies and business processes.

A business process is an asset for value creation [1-4], which is exposed to incidents that may even imply a business interruption. A business process is also a context for various interactions and a source of incidents. Thus, business processes are exposed to the same quality requirements as material and human resources. Industrial Engineering approaches, however, seem to handle processes from the perspective of goal alignment and performance improvement instead of value preservation. In contrast, from the perspective of governance and compliance, a business process is considered as the main entity of analysis, which needs to be understood in order to achieve value preservation. In fact, practitioners of business continuity [5] and approaches to enterprise risk management [6, 7] suggested risk management within the context of business processes. These visions also support a cross-organizational approach to risk management, improving therefore organization wide common visibility of risks.

Observing that process management improves agility, and risk management provides robustness regarding decisions; an integration of both management processes shall imply an effective maturity. Actually, the ability to successfully achieve objectives continuously despite incidents is the main characteristic of maturity [8]. The outcome of an integrated approach is a robust management process, which should be less sensitive to changes in the business environment. A robust management process helps organization in the successful pursuit of objectives given changes; e.g. regulations, markets, suppliers; which inevitably imply some business adaptations.

Because, in many cases, process management and risk management are applied quite independently in the form of an organization, the basic idea of our work is to improve integration of the two domains. Integration is performed by tackling conceptual and organizational challenges at different levels of the system [9]. A first approach to conceptual challenges is considered in a previous paper [10], where we proposed a conceptual model of risk and argued the possibility to support this solution with a visual risk modeling language. This paper extends the previous conceptual model to the concepts related to business processes and proposes a method in order to support the operational deployment of the approach. First, we discuss works related to risk considerations in business processes. We then argue about the importance of a methodological support to the integrated management of process-risks. Subsequently, a method is proposed. The main constituents of this method are introduced in part 4, 5, and 6 before illustrating with a simple case and concluding.

## 2 Related Work

The well known Failure Modes, Effects and Criticality Analysis (FMECA) is a classical technique often used in risk analysis. FMECA is an approach to the analysis of failures modes of components of principally technical systems in order to evaluate their effects on the system and to classify these modes with regard to their criticality [11]. Concerning FMECA, in [12] some limits are noticed: focus on single causal event, lack of human factors considerations, negative vision of risk (risk is only a threat), the outcome of the analysis depends on an given operational mode of the system; and finally the method focuses only on events, which are internal to the system of analysis. In addition, FMECA as a general purpose method needs to integrate specificities related to risk in the context of business processes.

In [13], a process taxonomy as well as a risk taxonomy are proposed. The authors adopt an approach to integrate risk models in process models. Risk is considered as “*the probability with which an error will lead to an (unwanted) consequence*”. The concept of error is therefore the fundamental component of risk. The integration of risk models in process models is a mapping between process based errors and risks. This approach is a systematic way to understand probable process level errors and the related unwanted consequences. Given that errors [14] are the causes of failures modes, addressing process risks with the vision of potential failure due to error is comparable to the FMECA approach. Actually, here, it is not explained why the case is perceived as a risk and how an error emerges from the business context. It is assumed that a forecast is available and defines some expected and wanted

organizational trajectories. But, this is not always the case. In addition, the internal structure of risk and the relations between a risk and the affected objects are indeed missing. However, this contextual information is important for risk assessment and risk treatment. For this reason, we consider risk as a concept with a well defined structure in term of a causal component, an impact component, an interpretation context, and a decision component. We then analyse the relations between these components and the concepts of business processes in order to understand the effort required for the management of this complexity. This is clearly an integration philosophy.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) expresses the objective of supporting management in balancing expectations and possible variations of these in order to deploy resources to achieve business objective. For this purpose, the committee developed an integrated framework for Enterprise Risk Management (ERM) [6], which consists of eight risk management components, and control objectives. The whole is organised according to different levels of abstraction. It is an industrial driven structural framework, which can be instantiated and populated with tools in order to support a particular business case. It should be noted, that the framework does not provide facilities for modelling. However, researches such as [15, 16] are proposing theoretical foundations and modelling tools to address this shortcoming.

In the literature, it is possible to point out three classes of approaches: risk centred approaches, which emphasize only risk management. Process oriented approaches, which consider risks from the information and simulation points of view neglecting therefore the relations between the concepts and lifecycles of both management processes. The class of industrial frameworks, suggest the management of business process risks without providing tools for the analysis of the relations between risks and processes. But within the business context, risks are complex because:

- Risks affect multiples interrelated objectives,
- risks are perceived differently depending on stakeholders' views,
- risks have various and variables relations (source, target, interpretation, treatment) to enterprise objects and to each others,
- risks have different manifestation depending on the level of abstraction (strategic level, domain level, process level, activity level).

Actually, business events depend from specific business contexts and are subject to causal, temporal, even logical relations, which vary with time, space and stakeholders. In addition, handling a risk at the business level may imply process changes with side effects to other processes. This natural complexity of business risks makes risk management a laborious task, which requires approaches and tools to master the complexity.

### **3 A Method for Integrated Management of Process-risk**

The concept of method is widely used in different communities such as management, information technologies (IT), formal analysis, and modelling. The IT views of methods suite our research problem. Here, a method can be defined as "*a way of*

*performing something according to a plan to obtain reproducible results in a systematic and traceable manner*" [17]. A method consists of *"(1) an underlying model of development, (2) a language, or languages, (3) define, ordered steps, and (4) guidance for applying these in a coherent manner"* [18]. As shown in Fig. 1 (top part) a method is more than just a process model, which states how to produce results that conformed to a schema or meta model [18-20].

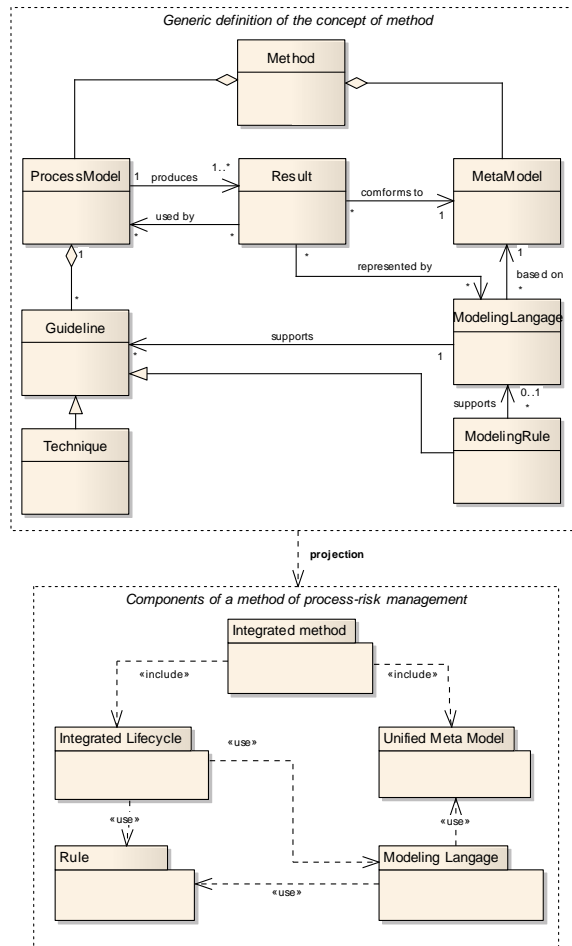
Methods provide consistent information about the state of the lifecycle of the object under analysis and resources to support activities. They provide therefore a framework to structure the work regarding the objectives while considering the most important aspects of the system and constraints. In this way, methods contribute greatly to manage the complexity due to the system under analysis. In addition, when a method is defined in form of a process model, it promotes knowledge capitalization and continuous improvement of the work process. As experienced in information system engineering, quantitative measures of a method support optimization of the work and improved quality.

The even defined vision of method is instantiated as shown in Fig. 1. The result is a method for the integrated management of process-risks including a lifecycle model, a meta model, a modeling language and a set of usage rules. The lifecycle model states how to use the tools in a consistent manner in order to produce robust enterprise models, which are compliant to the conceptual model. Since the method is used by both, risk experts and business experts, one needs to consider some integration challenges:

- Incompatibilities in the organization structure of risk management and process management. Process management is a horizontal concern with three levels of organization. However, risk management is a monolithic system, which may be implemented at different levels in the organization.
- Semantic incompatibilities of risk and process related information, which are exchanged between both processes of the lifecycle model.

In order to deal with these conceptual, organizational and coordination challenges, we suggested the following approach:

1. Synchronization of the lifecycles of process management and risk management into a single coordinated process model addressing coordination and organizational issues.
2. Conceptual unification of risks and processes into a common meta model in order to address semantic incompatibilities.
3. Operational developments of languages and rules to make things more concrete.



**Fig. 1:** Instantiation of the concept of method

#### 4 Synchronization of lifecycles

In [13], two kinds of relations between risk and process management are pointed out: risk-oriented process management, which consists in managing processes by considering risks in order to improve decisions regarding alternatives processes; and process-oriented risk management, which emphasizes the management of the risk management process. In addition to these observations, where the authors identified two unidirectional relations, in the practice, there is also a bidirectional relation between instances of process and risk management lifecycles. As shown in the lifecycle model presented in [10], from one hand, the risk management process triggers the process management lifecycle in order to revise processes once the level

of risk is over a predefined risk appetite. From the other hand, the process management lifecycle triggers the risk management process in order to receive instructions for context analysis and risk cartography. Our research considers as a whole these bidirectional relations, because the risk and process management lifecycles interchange the master-slave roles depending on the state of each lifecycle model.

At the highest level, similar to [21], as stated in [10, 22], the risk management process is instantiated in each step of the process management lifecycle. At the conceptual level, as illustrated in Fig. 2, the design phase of business processes is merged with the risk management lifecycle into a single coordinated process.

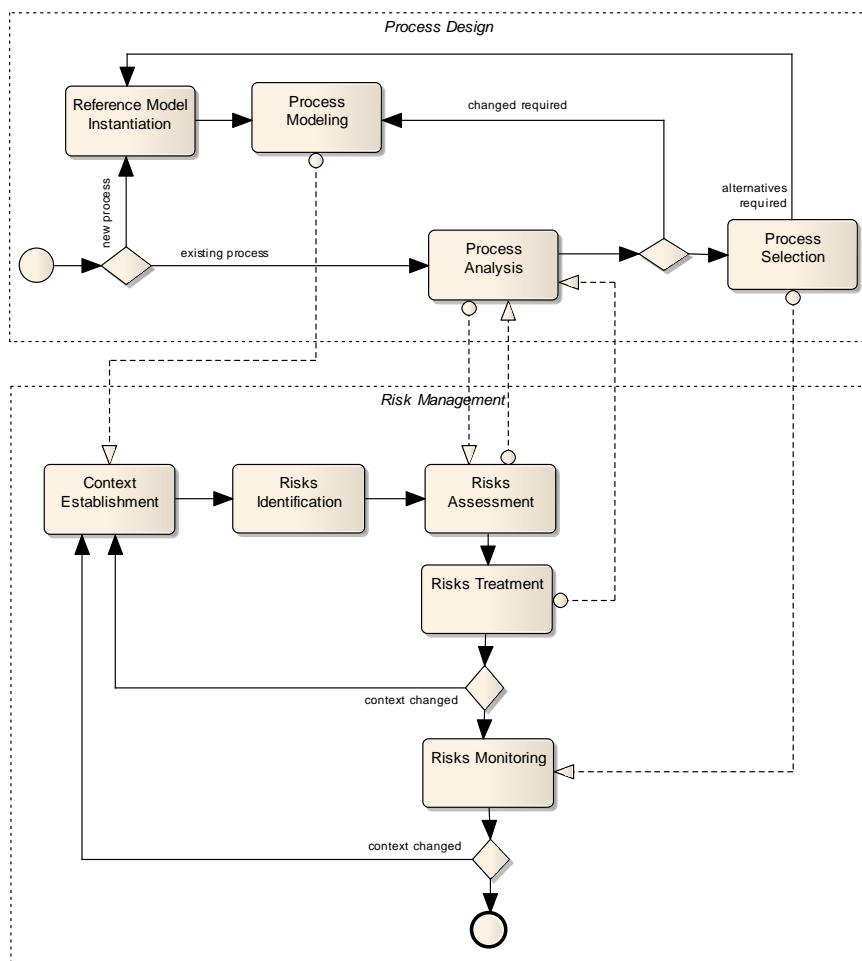


Fig. 2: Synchronized lifecycle: focus on process design.

Business analysts define the process model with regard to the level of analysis. In case of a new process, a reference model shall be instantiated and adapted to the situation. The information, organization, resource and functional aspects of the

process model provide context information, which is required for risk management. Existing processes are directly analyzed with regard to their capability and stability. The Process Modeling activity triggers the risk management process. The context for risk management is set up by enriching process models with statements about assets (name, value, type, and risk tolerance), stakeholder and the relations between assets and stakeholders in term of interest including the risk appetite of each stakeholder. Risks are identified in the basis of the contextual information. The risk assessment phase consists of risk evaluation and risk identification. This phase is supported with the process analysis activities and techniques such as process simulation. Selected risks are treated and analyzed with regard to process specific requirements.

## 5 Conceptual Unification

Conceptual modeling is a well known practice in enterprise modeling, which provides foundations for understanding concepts, relations, and constraints in complex phenomenon. It is an enabler for simulations, enterprise integration and design of modeling language. Conceptual unification promotes meta model level unification of concepts and relations of two domains and provides semantic correspondences between these [9].

In order to promote organization between process experts and risk experts by enabling them to work on the same models without changing their semantics, a conceptual unification of both domains is proposed. The adopted unification is based on a mapping technique; which is “*a way to trace correspondences between two models without modifying them*”[23]. First, we proposed a conceptual model of risk (appendix Fig. 5) [10]. Subsequently, as shown in (appendix Fig. 6) we extended the conceptual model of business process defined by ISO/DIS 19440 [24]. The choice of ISO/DIS 19440 as a basic model has two justifications: (1) ISO/DIS 19440 as a standard, is a consensus based on various approaches to enterprise modeling such as EN ISO 19439, ISO/IEC 15414, CIMOSA, GRAI, GERAM etc. (2) ISO/DIS 19440 associates an organizational role to each enterprise concepts. This role is played by the resource having responsibility for the concept. Because of this relation, each enterprise concept is a potential asset since there is at least one internal stakeholder (the responsible) who is concerned with.

We finally identified and analyzed the mapping relations between risk and process, which are explained subsequently.

A) Semantic abstracting mapping (mapping based on generalization<sup>1</sup> i.e. *is-a* relation): This mapping supports the interpretation of the causes and impacts of risks with regard to business processes. Generalization is a modeling technique selected to establish relations between both domains. The direction of the generalization (Fig. 3) is defined with regard to the ambition to highlight (visual annotation) process models

---

<sup>1</sup> “specific concept modified for a more general extent, use or purpose, or the act of removing or modifying detail from a specific concept to produce a generalization thereof” ISO/DIS 19440.

with risk concepts without changing the process semantic. The following table illustrates the generalization relations.

**Table 1.** Semantic abstracting mapping between process and risk.

Process concepts (special)	Risk concepts (general)	Comment
Enterprise Object	Asset, Risk Factor	
Business Process	Asset	
Enterprise Activity	Asset	
State	Risk Situation	The state of a business process or an enterprise activity can be defined as a risk situation.
Process Structure	Risk Factor	
Objective	Asset	
Person Profile or role	Stakeholder	
Organizational Unit	Stakeholder	
Functional Entity or actor	Stakeholder, Asset	

B) Semantic invariant mapping: The perception of risk is based on a context, which materializes the risk and shows relations between objects, which are interpreted. Various processes related concepts are involved in this context. Enterprise activity, business process, and domain generate events, respectively are triggered by events that cause risks. This relation is an association, which does not imply semantic changes.

C) Semantic equivalent mapping: From the process perspective, an event is an “*unique occurrence*” [24], which “*represents the initiation of a state change in the enterprise or its environment, to be used to initiate the execution of one or more processes*”. An event is characterized by its identity, the information about its source and destination. Events also have a behavior, and conditions of occurrences. The later is considered for the estimation of the likelihood of occurrence. The risk view is exactly based on this aspect. Here, an event is the “*occurrence of a particular set of circumstances*” [25] and “*can be certain or uncertain*”. An event is characterized by an identity, a source and a probability, which is “*estimated for a given period of time*”. Extended with the concept of probability, a given model of event can appear in process model as well as in risk model without causing any semantic ambiguity. The concept of event keeps the same semantic in both models process and risk

Based upon these correspondences, the meta model of Fig. 3 is proposed. For clarity, only concepts and relations, which are necessary to understand our approach, are represented.



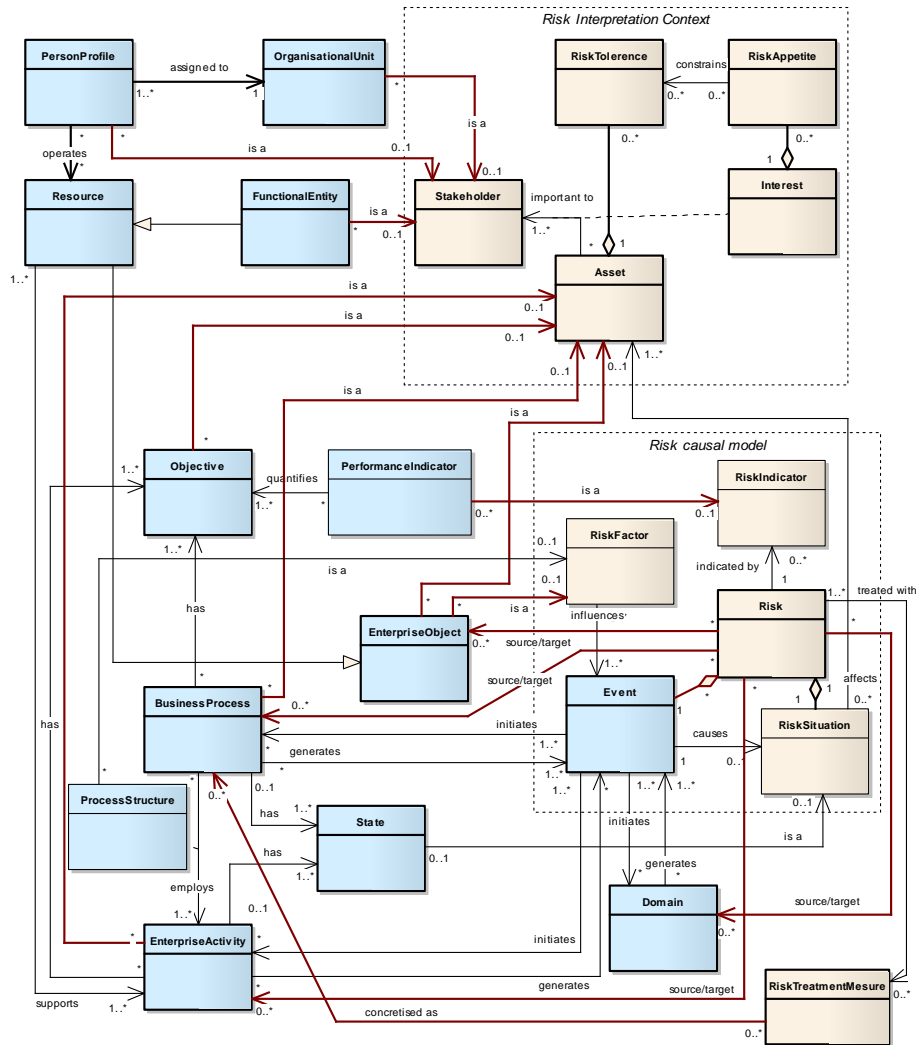


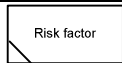



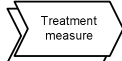
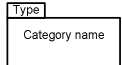
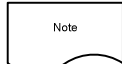
Fig. 3: Selected correspondences between Business process and Risk

## 6 Modeling Language Unification







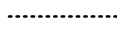


In a previous paper [10] a high level graphical modeling language, which integrates the unified concepts of both domains risks and processes was suggested. The conceptual unification, discussed in the previous section, led to the definition of visual representation of the relations between domain and risk, process and risk, enterprise activity and risk, enterprise object and risk.

The following tables illustrate the visual representation with adapted concepts and new relations. Given our intention to couple processes and risks, an effort is made to re-used representation formalism of process modelling languages, and to extend the semantic and/or syntax. The Even-driven Process Chain (EPC) language [26] is considered for process specific part and will not be detailed.

**Table 2.** Graphical notation of concepts in the visual risk modeling language

Notation	Description
	Risk factor: Characteristics of the system affecting the probability or the impact of risk.
	Risk situation: the state in which a causal event may lead the system.
	Concern: an asset which may be affected by the risk situation.
	Risk: the possibility of a situation affecting an asset.
	Risk handling: activities planned or executed in order to face a risk.
	Category to classify risk, event or factors.
	

**Table 3.** Graphical notation of relations in the visual risk modeling language

Notation	Description
	Influence relation of a factor on an event. Inter-event influence relation.
	Classification relation.
	Aggregation relation between risks. Aggregation is a parameterized relation, which can be customized by defining an aggregation criterion.
	Generalisation relation
	Causality relation between an event and a risk situation.
	Impact relation between risk situation and asset.
	General association relation between concepts.
	Relation between risk and process concepts (process, activity, and object): the direction indicates the target component.
	Interest relation between a stakeholder and an asset.

---

→	Treatment relation between risk and risk treatment measure.
---	-------------------------------------------------------------

---

**Table 4.** Graphical notation of operators in the visual risk modeling language

notation	Description
⋀	AND operator
⋁	OR Operator
⊕	XOR Operator

During the evolution of the synchronized lifecycle (Fig. 2), elements of process vocabulary and risk vocabulary are combined in various staged in order to produce sentences which are diagrams.

## 7 Illustration

A simple case study shall illustrate how our extended language supports risk-oriented analysis of activities: In Fig. 4 the activity “assemble computer components” is able to generate three events. A disjunction between the resources “computer assembly manual” and “hardware requirement” is a factor, which influences the event “computer assembly manual out-of-date”. The later is the cause leading to the unwanted state “computer components not assembled”. The performance objectives “warehouse schedule”, “assembly schedule”, “target workload” are affected. These are of value to “manufacturing supervisor”, “component assembler” and “construction supervisor”.

From the representation point of view, process specific concepts such as event, goal, and operational role are labeled with icons representing the risk view and summarized into a risk scenario diagram. The risk scenario diagram is one of the outputs of the risk assessment phase in our integrated lifecycle of Fig. 2.

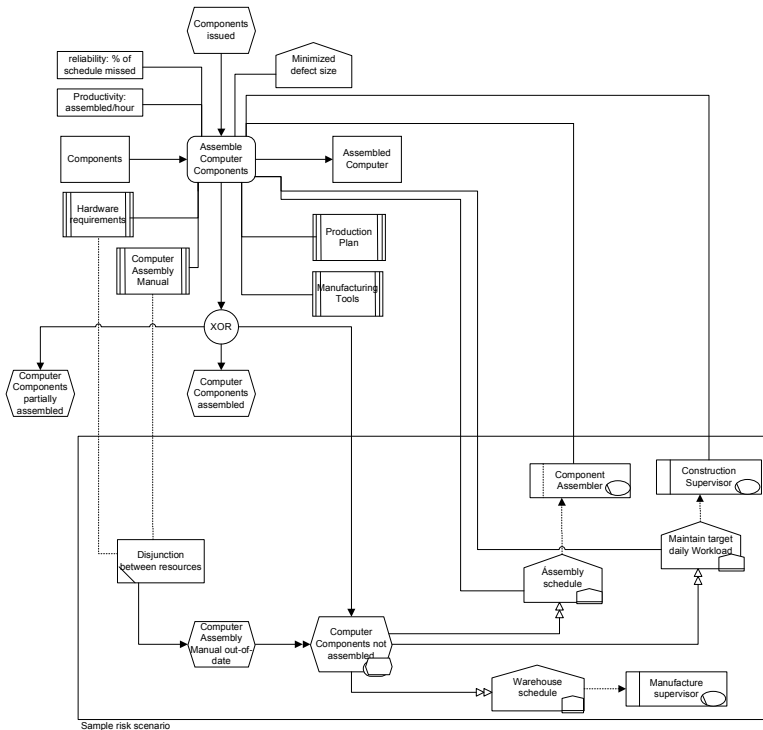


Fig. 4: Sample risk scenario and relations with an activity

## 8 Conclusions and future work

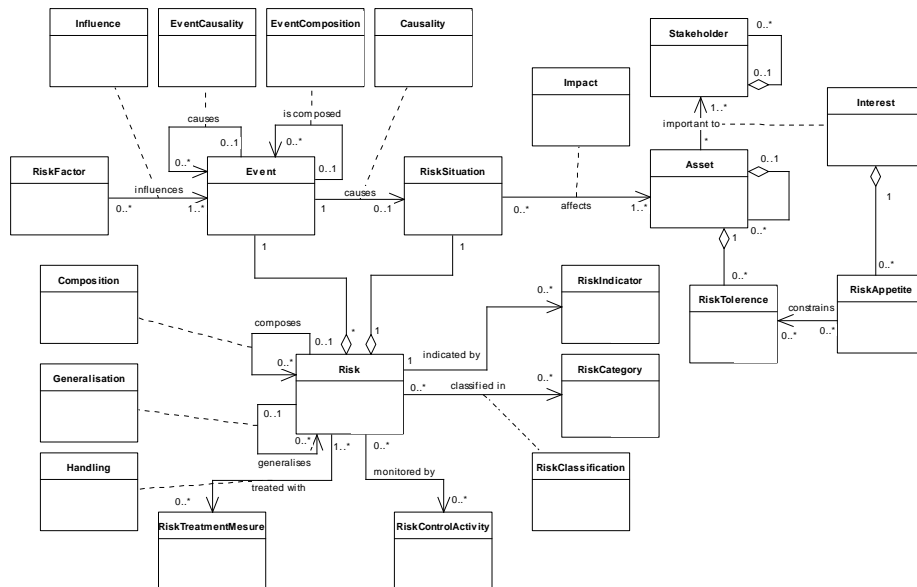
Based upon the observation, that process management improves agility, and risk management provides robustness; in this paper we suggested an integration of risk and process management in order to enable robust process management, which contributes to increase organizational maturity. Given the complexity of business process risks, and the management context of these kinds of risks, a method shall provide the guidance necessary to deploy an integrated process-risk management. Adopting a vision of method from information technologies perspective, we suggested an integration approach with three components: design phase lifecycle synchronization into a single process model, conceptual unification of risk and process and proposition of a notation for a visual modeling language. The concept of method and the conceptual unification extends previous publications. This research is in progress and shall be subject to improvement and evaluation. Currently, we further investigate on the visual modeling language in order to propose a core formal model. Scenarios will then be defined and evaluated in business cases. An industrial application to business continuity planning is planned. We try to define a set of generic models that will give opportunities to represent both the risk management results and the process behavior in an integrated manner.

## References

1. Hammer, M., Champy, J.: *Reengineering the Corporation: A Manifesto for Business Revolution*. Harper Business, New York (NY) (1993)
2. Davenport, T.H.: *Process Innovation. Reengineering Work through Information Technology*. Harvard Business School Press, Boston (MA) (1993)
3. Burlton, R.T.: *Business Process Management: Profiting From Process*. Sams publishing, Indianapolis, USA (2001)
4. Hill, J.B., Sinur, J., Flint, D., Melenovsky, M.J.: *Gartner's Position on Business Process Management*. Gartner (2006)
5. The Business Continuity Institute: *Good Practice Guidelines (2005) - A Framework for Business Continuity Management*. In: Smith, D.J. (ed.). *The Business Continuity Institute (2005)*
6. COSO: *Enterprise Risk Management - Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission (2004)
7. Basel Committee on Banking Supervision: *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*. Bank for International Settlements (2004)
8. Christis, M.B., Konrad, M., Shrum, S.: *CMMI: Guidelines for Process Integration and Product Improvement*. Addison Wesley (2003)
9. Chen, D., Dassisti, M., Elvesæter, B.: *Enterprise Interoperability Framework and knowledge corpus*, Final report. INTEROP (2007)
10. Sienou, A., Lamine, E., Karduck, P.A., Pingaud, H.: *Conceptual model of risk: towards a risk modeling language*. In: Weske, M., Hacid, M.-S., Godart, C. (eds.): *Web Information Systems Engineering – WISE 2007 Workshops*, LNCS, vol 4832, pp. 118-129. Springer Berlin / Heidelberg (2007)
11. US Department of defense: *Military standard: procedures for performing a failure mode, effects and criticality analysis*. Washington, DC (1980)
12. RBDM: *Risk-based Decision-making guidelines*. U.S. Coast Guard, Homeland Security (1997)
13. zur Muehlen, M., Rosemann, M.: *Integrating Risks in Business Process Models*. *Proceedings of the 2005 Australian Conference on Information Systems (ACIS 2005)*, Manly, Sydney, Australia (2005)
14. Algirdas, A., Jean-Claude, L., Brian, R., Carl, L.: *Basic Concepts and Taxonomy of Dependable and Secure Computing*. *IEEE Transactions on Dependable and Secure Computing* 01 (2004) 11-33
15. Sadiq, S., Governatori, G., Naimiri, K.: *Modeling Control Objectives for Business Process Compliance*. In: Alonso, G., Dadam, P., Rosemann, M. (eds.): *Business Process Management*, Vol. LNCS 4714, pp. 149-164. Springer Berlin / Heidelberg (2007)
16. Governatori, G., Milosevic, Z., Sadiq, S.: *Compliance Checking Between Business Processes and Business Contracts* 10th International Enterprise Distributed Object Computing Conference (EDOC 2006). IEEE, Hong Kong (2006) 221-232
17. ISO/IEC 15414: *Information Technology—Open Distributed Processing—Reference Model—Enterprise Language - ISO/IEC 15414 | ITU-T Recommendation X.911*. ISO/IEC JTC1/SC7 Secretariat (2006)
18. Kelly, J.C., Kemp, K.: *Formal Methods Specification and Analysis Guidebook for the Verification of Software and Computer Systems, Volume II: A Practitioner's Companion*. NASA, Office of Safety and Mission Assurance (1997)
19. Backlund, P., Ralyté, J., Lillehagen, F., Kühn, H., Goossenaerts, J., Elvesæter, B., Wäyrynen, J.: *State of the Art: Exploration of Methods and Method Engineering Approaches*. INTEROP (2005)

20. Gutzwiller, T.: Das CC-RIM-Referenzmodell für den Entwurf von betrieblichen, transaktionsorientierten Informationssystemen. Physica-Verlag, Heidelberg (1994)
21. zur Muehlen, M., Ho, D.T.-Y.: Risk Management in the BPM Lifecycle. In: Davenport, T., Reijers, H., Rosemann, M. (eds.): Proceedings of the First International Workshop on Business Process Design: Past, Present, Future, Nancy, France (2005)
22. Sienou, A., Karduck, A.P., Pingaud, H.: Towards a Framework for Integrating Risk and Business Process Management. In: Dolgui, A., Morel, G., Pereira, C.E. (eds.): Information Control Problems in Manufacturing - A Proceedings volume from the 12th IFAC International Symposium, Saint-Etienne, France, Vol. I. Elsevier Science, Oxford, UK (2006) 615-621
23. D'Antonio, F.: TG MoMo Roadmap. INTEROP (2005)
24. ISO/DIS 19440.2: Enterprise integration — Constructs for enterprise modelling. ISO, Genève (2005)
25. ISO/IEC Guide 73: ISO/IEC Guide 73:2002 - Risk management — Vocabulary — Guidelines for use in standards. ISO, Geneva, Switzerland (2002)
26. Scheer, A.-W.: ARIS – Business Process Modeling. Springer, Berlin (2000)
27. Sienou, A., Lamine, E., Pingaud, H., Karduck, A.P.: Vers un langage de modelisation des risques et des processus. Modélisation et interopérabilité des entreprises et des systèmes d'information, MOSIM'08, Paris, France (2008).

**Appendix:**



**Fig. 5:** proposed Risk Meta model [27]

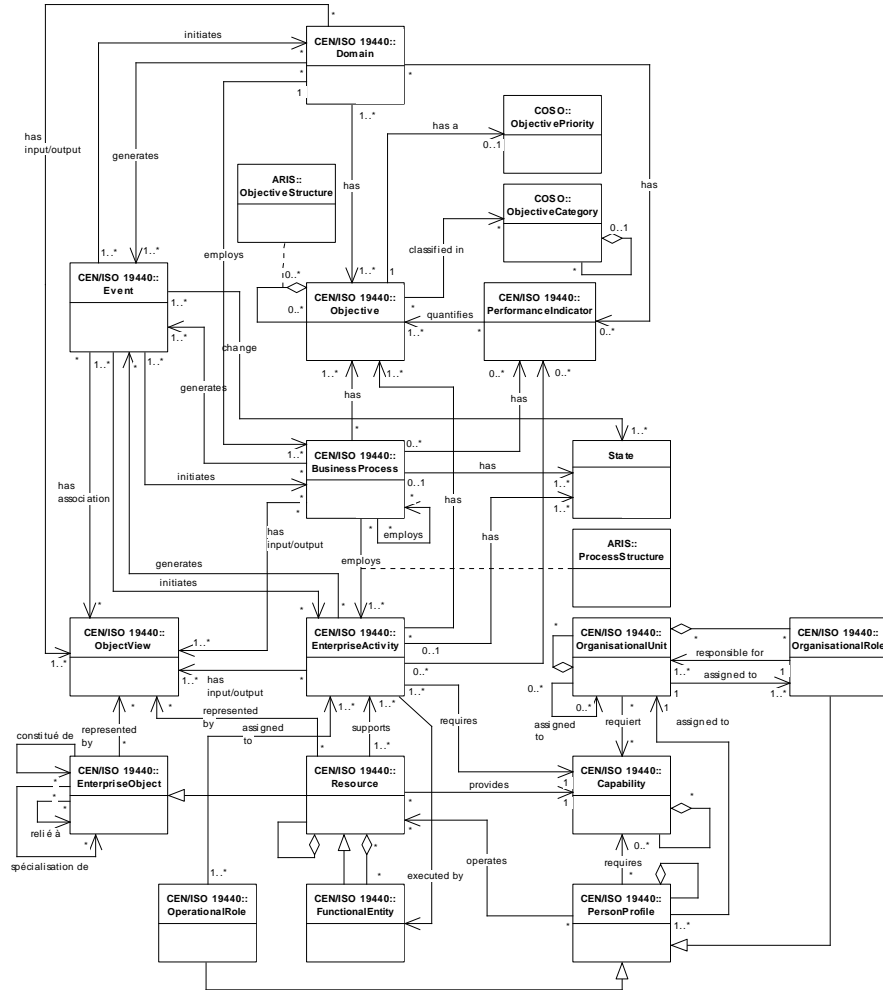


Fig. 6: proposed Business Process Meta model [27]