2

A model for process oriented risk management

Giancarlo Nota and Maria Pia Di Gregorio
Dipartimento di Matematica e Informatica, Università di Salerno
Italy

1. Introduction

Every enterprise can be affected by risks with potential impact on their single organizational parts or on their organizations as a whole. The awareness of consequences deriving from threats, omissions or adverse events drives enterprises to support risk management programs whose aim is to reduce undesirable consequences.
The need to identify, assess, and manage risks has motivated organizations to develop integrated frameworks to improve enterprise risk management. ERM is a framework designed by the Committee of Sponsoring Organizations of Treadway Commission (COSO, 2004) that helps business to assess and enhance their internal control systems. COSO defines ERM as "… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regard in the achievement of entity objectives".
The literature about risk proposes various techniques to identify and classify risks in different fields of knowledge or descriptions of various innovative approaches for managing risks. For example, in (Alberts&Dorofee, 2009) two approaches for managing risks are compared: tactical risk management and systemic risk management. Tactical risk is traditional, bottom-up analysis defined as a measure of the likelihood that an individual potential event will lead to a loss coupled with the magnitude of loss. This approach has the limit that does not readily scale to distributed environments. In contrast to the bottom-up analyses employed in tactical risk management, systemic risk management approach starts at the top with the identification of a program's key objectives. Once the key objectives are known, the next step is to identify a set of critical factors, called drivers that influence whether or not the key objectives will be achieved.
In order to minimize the impact of risks Enterprise Risk management frameworks typically includes four major areas corresponding to the achievement of enterprise objectives:

- Strategic: high-level goals, aligned with and supporting its mission
- Operations: effective and efficient use of its resource
- Reporting: reliability of reporting
- Compliance: compliance with applicable laws and regulations

Many organizations are reluctant to support risk management programs, probably because of the high cost of human resources necessary for acquisition, manipulation and analysis of risk data. However, the management of operational risks is being given increasing attention as a fundamental part of monitoring, controlling and decision support systems because of the opportunity that Workflow Management Systems (WfMS) provides in terms of automatic collection of business process execution data.
The problem of process measurement is considered to be important in several fields such as banking risks, insurance and industry; it can be an effective instrument to single out risks in different fields in order to avoid disastrous consequences. In fact, the Basel Committee encourages industry to develop methodologies and techniques to collect data for managing, measuring and monitoring operational risks; the Committee has also adopted a common industry definition of operational risk, namely:" the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events". (Basel Committee, 2001).
The perspective on business process models is adopted by (Zur Muehlen et al., 2005). Through the application of value-focused process engineering principles to risk management models, the authors propose a framework that enables risk-oriented process management to incorporate a multi-disciplinary view of risk. This approach is useful especially in Business Process Reengineering scenarios, where a decision about the best process to reengineer must be taken on the basis of risk criteria.
The importance of acquiring quantitative risk data is suggested by the UK's Financial Service Authority (FSA, 2002):
"Due to both data limitations and lack of high-powered analysis tools, a number of operational risks cannot be measured accurately in a quantitative manner at the present time. However, we would encourage firms to collect data on their operational risks and to use measurement tools where this is possible and appropriate".
The lack of models and systems in the field of real time management of operational risks encourage new research activity. In this chapter we propose a model that integrates WfMS and Risk Management System (RMS) functionalities in order to represent operational risk management. The process oriented approach to continuous risk management, based on a top level model for the representation of qualitative and quantitative risks, is able to reduce effort and cost necessary to implement a risk management program. The capability to continuously measure executable process instances provided by a Workflow Management System (WfMS) is assumed as a major premise for the design of a workflow based risk management system. We will show how the typical WfMS capabilities, in terms of process enactment and performance evaluation, can be represented within an augmented model that integrates WfMS capabilities and continuous risk management aiming at the monitoring and control of operational risks. The benefits deriving from this approach are manifold: a) the cost reduction for the risk management systems due to the automatic process execution data recoding provided by the WfMS; b) the definition and management of qualitative and quantitative risks within the unifying framework of process management; c) the definition of a proactive policy for the treatment of operational risks.

2. Modeling process oriented risk management systems

This section introduces the rationale and the building blocks of a model that can be exploited for the design and implementation of a process oriented risk management system. When the management decides to follow a risk management program, one of the hurdle hindering the success of such initiative is that many roles, e.g. business administration or IT, perceive different views of risks (Stankosky, 2005). This separation is mainly due to different goals pursued by different roles (Neef et al., 1998), (Nonaka, 2005). On the one hand, management roles adopt, more or less consciously, a system thinking approach (Weinberg, 2001) to the understanding of organizational structures, processes, policies, events, etc. This approach allows, once business processes have been designed and implemented, to monitor them at a high abstraction level relieving the manager from the details and the mechanics necessary to process execution. Watching at 'the big picture' and transcending organizational boundaries, the manager focuses himself on business goals and on risks that could threat their achievement. On the other hand, operational roles have a completely different view of risks. For example, IT personnel are usually concerned about how data and information can be stored/retrieved and how to provide access to ICT services over the organization's 'digital nervous system'. In this case, the perception of risks mainly concerns the availability and performances of communication/database systems, application programs, access policies, etc.
As pointed out by Leymann and Roller (Leymann & Roller, 2000), workflow technology helps to bridge the gap between these different views of business processes because: a) management roles typically look at the process models and at their execution instances eventually asking for execution data to evaluate the process performance, b) operational roles implement process activities and perform them with the support of a workflow management system.

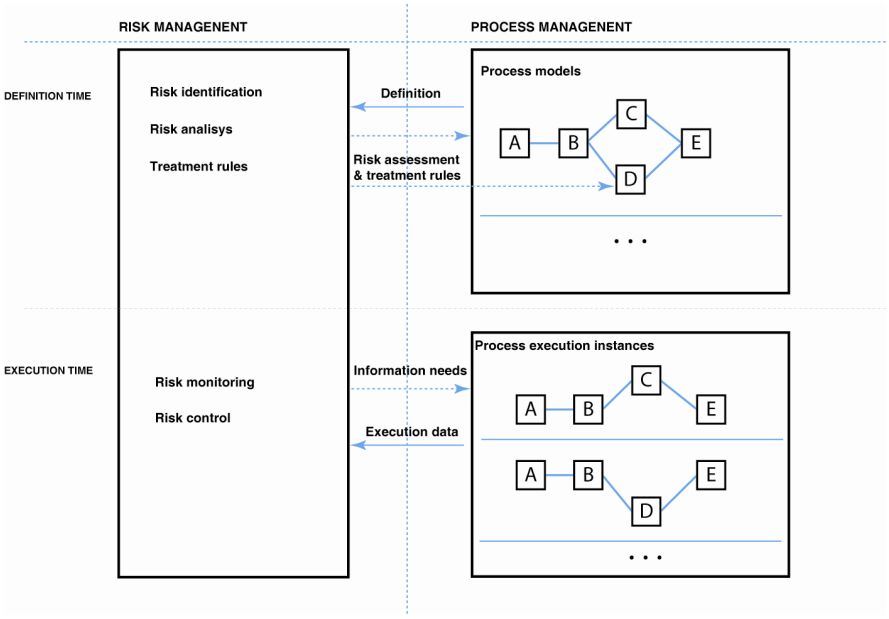

Fig. 1. Top level model for process oriented risk management.

The model shown in fig. 1 represents an integrated system aiming at the management of operational risks in a context where processes are enacted with the support of a workflow management system.
The process management subsystem comprises the usual tools for process definition, process instance creation and execution as well as maintenance services. One of the most appealing features of workflow management systems is the measurement capability offered by this class of products. Both research and industrial applications are mature enough and provide measurement tools concerning workflow measurable entities (zur Muehlen M., 2004), (Oracle, 2002). Several kinds of duration measures about activities/processes, waiting queues, produced deliverable and human resource efforts are frequently evaluated and can provide quantitative knowledge about business processes. However, current workflow products do not take into account risk management. Indeed, the workflow log collects automatically raw execution data that can be used for process monitoring and performance evaluation. These log data are invaluable to lay out a process oriented risk management system.
The premise behind the process oriented risk management system is similar to other widely accepted approaches to assessment and measurement: there exists information need that, when satisfied, increases the decision capability.
A widely accepted approach to project measurements in the field of software engineering is GQM (Goal-Question-Metrics) (Basili et al., 1994), (Mendoça & Basili, 2000). The GQM model is structured as a three level hierarchy: 1. conceptual level (GOAL); 2. operational level (QUESTION) and quantitative level (METRIC). The goal states a viewpoint for an object of measurement (e.g. products, processes, resources) that can be refined into several questions, in their turn refined into several metrics that, when evaluated, provide quantitative information about the viewpoint to be measured. The GQM approach is based upon the assumption that an organization must first specify the goals for itself and its projects in order to measure in a powerful way. Subsequently the organization must trace the goals and the relative operational data and finally provide a framework for interpreting the data according to the stated goals.
Another well-known method for software measurement is PSM (Practical software and systems measurement) (McGarry et al., 2001). PSM describes how to define and implement a measurement program to support the information needs of the software and system acquire and supplier organization. It describes an approach to management based on integrating the concepts of a Measurement Information Model and a Measurement Process Model. A Measurement Information Model defines the relationship between the information needs of the manager and the objective data to be collected, commonly called measures. The Measurement Process Model describes a set of related measurement activities that are generally applicable in all circumstances, regardless of the specific information needs of any particular situation and provides an application (McGarry et al, 2001).
From the point of view of the risk management system, there exists an information need about process instances that a WfMS can help to satisfy. The left side of the model shown in fig. 1 describes how a risk management system can be integrated with a WfMS. At definition time, when the process model is established, risk data are stated and relied to the process model. Note that the risk statement can be relied to both process and activity. This choice reflects the different process perspectives that managers and operational staff have on processes. Managers look at the process level and think in terms of risks at this level in order

to provide support for continuous monitoring of risks deriving from the execution of workflow instances.

3. Case study

The "call for tender" case study that we will refer in the following sections, is an open procedure managed by a public agency in order to select the provider of goods and services on the basis of award criteria stated in the tender specifications. The procedure usually involves a number of different Organizational Units starting from the proposal phase, in which the procurement is planned, to the selection of a winner, and the subsequent public announcement. In fig. 2 the BPMN model that represents the call for tender is shown. Assuming that the acquisition act has already been stated, the procedure begins when an Organizational Unit is charged to plan the procurement. This activity is devoted to the writing of procurement documents such as:

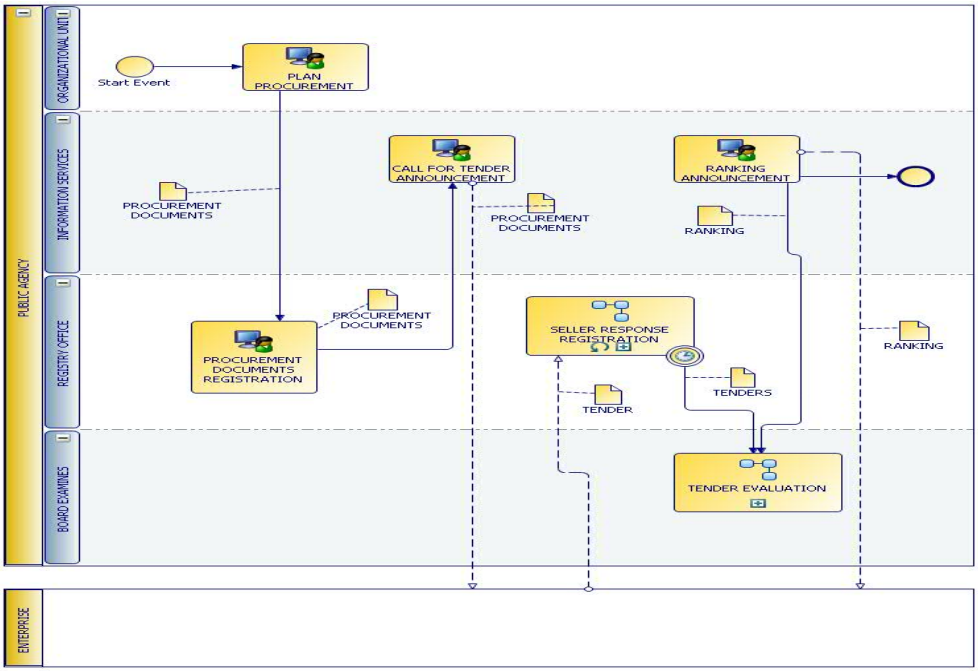

Fig. 2. Call for tender process: the BPMN model.

Contract Notice. It includes the name, address and contact point of the contracting authority, a short description of the contract or purchase(s), and its estimated value.
Tender Specifications. Guidelines and general information related to the tender, time limit for receipt of tenders, offer evaluation rules, specific information related to the tender, and award criteria.
Invitation to Tender. This document includes the submission modalities and the procedure for the request of additional information.

The procurement documents are first sent to the Registry Office that proceeds to a formal registration of the call for tender. Then, the Information Services OU publishes the call for tender announcement enabling the interested enterprises to download the procurement documents. The Registry Office awaits the incoming request to participate until the time limit for receipt of tenders is reached. Afterward, the Board of Examiners is involved in the sub-process of "tender evaluation" that produces the ranking to be published by the Information Services.

4. Workflow quantitative measurement

A risk assessment methodology normally comprises a combination of qualitative and quantitative techniques. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification or when sufficient reliable data required for quantitative assessments are not available. Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities to supplement qualitative techniques. (COSO a,b).
Starting from these premises, we build on the top level model for process oriented risk management shown in fig. 1 to determine quantitative and qualitative measures inspired by the GQM approach applied to the domain of business processes and in compliance with the 3 layer PSM measurement model.
First, let us discuss the method that faces with the quantitative approach. Since the adoption of a Workflow Management System is assumed as an automated support to the execution of business processes, we review some fundamental workflow concepts necessary to understand the measurement framework taken as reference in the following.

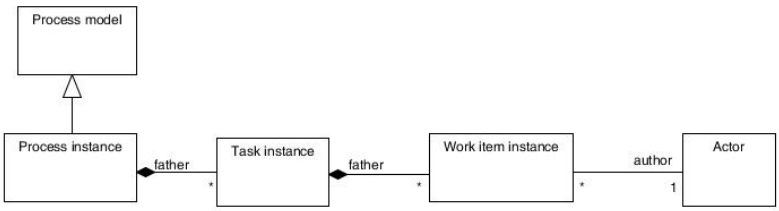

Fig. 3. Relationship between process model, model instances and actors.

According to the main terms and concepts of the Workflow Reference Model (P. Lawrence Ed, "WfMC Workflow Handbook", J. Wiley & Sons 1997), a WfMS is "a pro-active system for managing a series of tasks defined in one or more procedures. The system ensures that the tasks are passed among the appropriate participants in the correct sequence and completed within set times". As shown in the UML diagram of fig. 3. a WfMS allows the definition, the computerized representation and the execution of business processes wherein each process can be seen as a network of tasks. A single process model can generate different processes instances where each process instance can generate a network of task instances; each instance provide context for the work done by an actor on one or more work item instances. Considering the call for tender discussed in the previous section and following the GQM approach that defines in a top down fashion Goals, related Questions

and Metrics, in the scenario of WfMS supported business processes we could be interested to obtain general goals stated in terms of *efficiency*, *effectiveness* and *control costs*. These goals are then refined into process oriented queries that, in their turn, are related to metric in order to provide a precise evaluation about the degree of goals achievement.

Goals:
G1) *efficiency*: the comparison of what is actually produced or performed with what can be achieved with the same consumption of resources (money, time, etc)
G2) *effectiveness*: the degree to which objectives are achieved and the extent to which targeted problems are resolved.
G3) control cost: the application of investigative procedures to detect variance of actual costs from budgeted costs, diagnostic procedures to ascertain the causes of variance and corrective procedures to effect realignment between actual and budgeted costs.

Questions:
some typical questions addressed by an analyst during the process evaluation are:

Q1. What is the duration of a given task instance of "tender evaluation"? *(G1)*
Q2. What is the global throughput (process stared and completed) over the past years? *(G1)*
Q3. How many work items has a given employee completed? *(G1)*
Q4. How many procurements have been done with respect to the procurement plan? *(G2)*
Q5. What is the exception rate in the WfMS after the deployment of processes? *(G2)*
Q6. What is the average cost of "call for tender"? *(G3)*
Q7. How much is the difference between the planned costs and the real costs of a process instance? *(G3)*

To obtain precise answers to the queries such as those above, we need to develop a measurement framework by means of which numbers can be assigned to the various entities represented within the WfMS. The following examples are representative of a three levels measurement framework: *primitive*, *fundamental* and *derived measures* whose complete definition can be found in (Aiello, 2002). It will be used as a fundamental model for a risk management system based on workflow execution data.
Two *primitive* operators for measuring work and time are:

$$\#(X) = |X| \tag{1}$$

the cardinality of a set, and

$$\Delta(e_i, e_j) = \mathrm{abs}\left(\mathrm{time}(e_i) - \mathrm{time}(e_j)\right) \tag{2}$$

the length of the time interval between the occurrence times of two events e_i and e_j . Let I be the set of process, task and work item instances and i a generic instance, i∈I. We assume that each instance, at a given time, can be in one among the states: `created`, `running`, `suspended`, and `completed`; furthermore, a state transition is a consequence of a suitable event such as `completedInstance` that happens when a task instance is completed or

when a process instance completes its last task. The *fundamental* measures arise from the composition of primitive operators. For example, by means of the operator Δ, it is possible to build different fundamental measures such as `instanceDuration` that evaluates the total duration of an instance from its creation to its completion.

$$\begin{aligned} \text{instanceDuration}(i) = \Delta(&\text{event}(i, e\_type(i,e) = \text{createdInstance})), \\ &\text{event}(i, e\_type(i,e) = \text{completedInstance})) \end{aligned} \tag{3}$$

`instanceDuration` can be used to answer the question Q1. The operator filter is the standard operator for the choice of elements from a set I, according to a first order predicate `p`:

filter(I, p)=I′ with I′⊆I

$$\forall i \in I \begin{cases} p(i) = true & \text{if } i \in I' \\ p(i) = false & \text{if } i \notin I' \end{cases} \tag{4}$$

The following example refers to the case study introduced in section 3. According to the predicate `p`, `filter` returns all the tasks instances named "`procurement document registration`" in the context of the process "`call for tender announcement`".

$$\begin{aligned} &filter(I,p1): \\ &p1=i\_type(i)= task \wedge \\ &i\_name(i)= \text{"procurement document registration"} \wedge \\ &i\_name(father(i))=\text{"call for tender announcement"} \end{aligned} \tag{5}$$

A frequently used fundamental measure evaluates the workload in the scope provided applying a suitable filter to the set of all workflow instances. Queries of this kind require the capability to isolate within the WfMS the set of objects with the desired properties and then to evaluate its cardinality. By the combination of the operators # and `filter` we define the measure `work`;

$$\text{work}(I,p) = \#(\text{filter}(I,p)) \tag{6}$$

the example below shows how the measure `work` can be applied to evaluate the question Q3.

$$\begin{aligned} &work(I,p2): \\ &p2= p1 \wedge \\ &\quad actor\_ name(i)= \text{"Brown"} \wedge \\ &\quad current\_state(i)= completed \end{aligned} \tag{7}$$

The need of a derived measure (the third level of measured framework) becomes evident if we consider the evaluation of contribution that resources, especially human resources, make

to the progress of a process. Given a process P, the contribution of the generic actor to P is considered. The evaluation can be done from the point of view of time overhead, work overhead or cost and is expressed in percentage.
In order to define some kind of contribution measures, it is necessary to introduce the auxiliary function `sigma` that is itself defined in terms of `sum` and `map`. `sigma` implements the concept of "summation of measures" where the input parameter measure gets as a value the measurement definition to apply to the elements of a set `X`. The function `sum`, given a set of values, returns the sum of all the members in the set.

$$\text{sigma}(\text{measure}, X) = \text{sum}(\text{map}(\text{measure}, X)) \tag{8}$$

where map is a function that denotes the usual operator for the application of a function to a set of values

$$\text{map}(f\{x_1, x_2, \ldots x_n\}) = \{f(x_1), f(x_2), \ldots f(x_n)\} \tag{9}$$

$$\text{timeContribution}(\text{timeMeasure}, x_1, x_2) = \frac{\text{sigma}(\text{timeMeasure}, x_1)}{\text{sigma}(\text{timeMeasure}, x_2)} * 100 \tag{10}$$

$$\text{costContribution}(\text{costMeasure}, x_1, x_2) = \frac{\text{sigma}(\text{costMeasure}, x_1)}{\text{sigma}(\text{costMeasure}, x_2)} * 100 \tag{11}$$

$$\text{workContribution}(I, p_1, p_2) = \frac{\text{work}(I, p_1)}{\text{work}(I, p_2)} * 100 \tag{12}$$

Care must be taken to specify the set X_1 and X_2 and the predicates p_1 and p_2 since a proportion requires that the numerator is less than or equal to the denominator.
Let t_{actor_k} be the working time spent by the generic actor on `P`. In general, to actor_k can be assigned more than one work item even in the context of a single process `P`. Given a process `P`, the actor time contribution `(atc)` of `actor_k` on `P` is

$$\text{atc}(P) = \frac{t_{actor\_k}(P)}{\sum_{j=1}^{n} t_{actor\_j}(P)} * 100 \tag{13}$$

```
timeContribution(workingDuration,filter(I,p1),filter(I,p2));

p2 = i_type (i)= workitem ∧ current_state(i)= completed ∧

     i_name(father(father(i))="P";

p1= p2 ∧ actor_name(i)="actor_k"
```

Let c_k the hourly cost of `actor_k`; a particular case of (11) provides the definition of actor cost contribution `(acc)` of `actor_k` on a process P:

$$acc = \frac{t_{actor\_k}(P) * c_k}{\sum_{j=1}^{n} t_{actor\_j}(P) * c_j} * 100 \quad (14)$$

5. Workflow qualitative measurement

Qualitative analysis is usually pursued relating likelihood and consequences of risks; a widely used model for this kind of analysis is the *priority-setting matrix* (Cooper et al. 2008), also known as *risk matrix* where cells, representing fuzzy *risk exposure values*, are grouped in a given number of risk classes. In the matrix shown in fig. 4, the risk exposure classes are represented by: **L** means low, negligible risk, **M** indicates a moderate risk, **H** a risk with high impact and probably high loss, and **E** represents the class of intolerable, extreme risk with very likely loss. Obviously, when the impact or likelihood grows, or both, the risk consequently grows; therefore a risk can modify its position from a lower category to an upper category. For each category of risk exposure, different actions have to be taken: values **E** and **H** involve a necessary attention in priority management and a registration in the Mitigation plan; a value **M** requires to be careful during the whole process management; a value **L** falls within ordinary management.

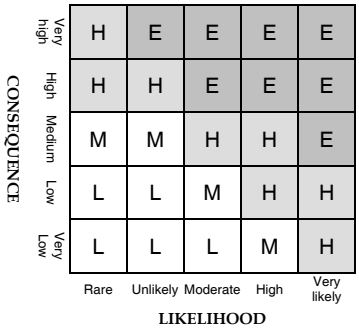

Fig. 4. A risk matrix.

The qualitative analysis is very useful either when a preliminary risk assessment is necessary or when a human judgement is the only viable approach to risk analysis. However, since a risk state (likelihood and/or consequence) might change continuously, the data collection about it is a time consuming activity often perceived as an unjustified cost. Another problem is the timing; if data are not collected according to a real time modality, they are of little or any value as the actions anticipated by the contingency plan could be no more effective. These considerations inhibit the implementation of risk management systems. The top level model for process oriented risk management suggests how, at definition time, the organization of questionnaires and checklists can be arranged. For example, within the scope of "call for tender", if we are interested in the following goals:
G4. *Transparency:*
Lack of hidden agendas and conditions, accompanied by the availability of full information required for collaboration, cooperation, and collective decision making.

Minimum degree of disclosure to which agreements, dealings, practices, and transactions are open to all for verification,
G5. Impartiality
Impartiality is a principle holding that decisions should be based on objective criteria rather than on the basis of bias, prejudice, or preferring the benefit to one person over another for improper reasons,
G6.Correctness
Conformity to laws

then, the related questions and checklists can be:

call for tender: quality assessment			
goal	*question*	*checklist*	*Task*
G4	Q8. Are the full information available and published on the web site?	[yes, no]	call for tender announcement
	Q9. Are the evaluation criteria for call for tenders complete and non ambiguous?	[poor, sufficient, good, very good]	plan procurement
G5	Q10. Are all tenders evaluated with the same criteria?	[yes, no]	tender evaluation
G6	Q11. Is the announcement compliant with the current laws?	[compliant, not compliant]	plan procurement
	Q12. Has the call been registered at the registry office?	[yes, no]	procurement registration
	Q13. Does the winner provide the right solution?	[poor, sufficient, good, very good]	tender evaluation

Table 1. Quality assessment specifications for the tasks of "call for tender"

where we associate to each task a set of goals together with the corresponding set of questions (at least one question for each goal, according to the GQM approach) and a checklist that suggests the judgment to be expressed.. Generally, the question is aimed at assessing a quality criterion and is evaluated against a list of fuzzy values such as {compliant, not compliant} or {poor, sufficient, good, very good}. Human judgments collected as soon as possible can feed the risk matrix. In other words, we can define task quality criteria whose satisfaction provides a contribution in the direction of quality goals for the task and in general for the whole process. When given criteria are not satisfied, the risk relied to the task increases and the task monitoring rules react raising the risk status and invoking the appropriate risk treatment. We will return to this point in the next section.
A WfMS usually provides a suitable definition and execution environment that allows with little implementation effort the set up of a subsystem devoted to the collection of qualitative process execution data. Indeed, applications for the exposition of questionnaires and checklist can be easily designed and implemented because the WfMS usually allows the launch of a complementary software application both at scheduling time and at completion time of a task instance.

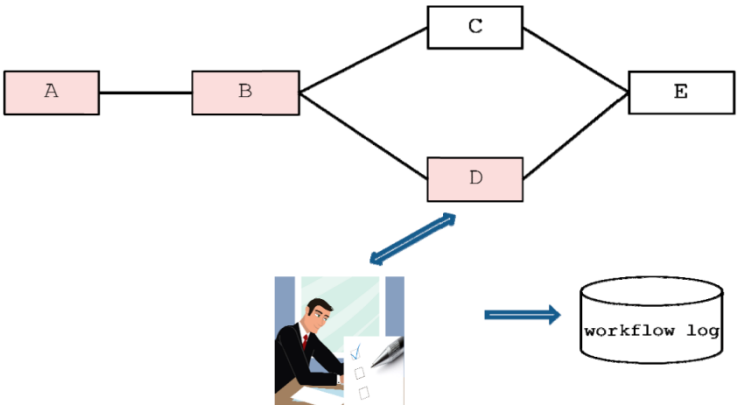

Fig. 5. Qualitative data collection through questionnaires and checklists.

This scenario is represented in fig. 5; after the execution of tasks A and B, the WfMS decides that the next task to schedule is D putting the task in the work list of a role charged to execute it. As soon as an actor with those roles completes the task D, the workflow engine will launch the software application that allows the interaction with a questionnaire. The answers are collected and then stored in the workflow execution log feeding the part of the risk management system that has the responsibility for the monitoring and control of qualitative risks.

6. Process oriented risk assessment

To show how the top level model for process oriented risk management allows continuous operational risk management with respect to tasks and processes, let us consider the phases of a generic risk management methodology that encapsulates the concepts discussed so far:

- *Define the context*: goals, processes, stakeholders, evaluation criteria
- *Identify the risks*: what events can have an impact on tasks and processes?
- *Analyze the risks*: state the likelihoods, consequences, measures, thresholds, prioritization
- *Write the contingency plan*: define the approach – avoidance, minimization, transfer-about risk or a set of a related risks
- *Monitoring*: collect qualitative and quantitative execution data, acquire risk status and record it, evaluate risk indicators
- *Control*: decide for the best reaction when the risk probability increases or when unwanted events happen
- *Communication:* is a cross activity in the sense that data or information handled by a certain task/process can be communicated to the involved stakeholders.

To be useful a sound risk management system must be reactive; in other words, it must provide real time responses to unwished events that might happen in an unpredictable way. To specify the behaviour of a risk management system charged to manage events with a

possible negative impact on the correct execution of tasks and processes, we shall use a rule based logic language called RSF (Degl'Innocenti e*t* al., 1990*); (*Nota &Pacini, 1992). With this language a reactive system can be defined in terms of event-condition-transition rules able to specify systems requirements subjected to temporal constraints. As shown in fig. 6, at risk definition time the risk manager has the possibility to access the process model database in order to link behavioral rules to tasks and processes that state how to react when the risk exceeds a given threshold.

At process execution time, critical task or process attributes are evaluated against the measurement framework and/or the risk matrix discussed in the previous sections. Then, if the current risk state is acceptable the process enactment proceeds regularly, otherwise the dangerous situation is immediately notified at the appropriate responsibility role, e.g. the task executor, the process owner or the risk manager.

At each time, the risk management system records a state concerning various kinds of data about risks. When an unwished event with a negative impact on an activity is recognized, the system reacts adjusting the state and eventually taking some risk treatment action.

At risk definition time, as shown in figure 6, the risk manager defines a questionnaire containing, for example, two questions q10 and q11 (cfr. the case study "call for tender") and establishes four risk assessment values for the activity D. At execution time, when D completes its execution, the workflow engine presents the questionnaire to the user, collect the answers and sends them to the RMS in order to associate the appropriate risk status for D depending on the collected responses. The rule for the treatment of qualitative risks linked to D states that: if the risk assumes the value E, then send an alert to the actor who executed D and activate an escalation procedure. The escalation signals a "process risk" to the process owner (the role responsible for the process instance that provide execution context for D) and an "organizational risk" to the appropriate business manager.

In section 4 we outlined a three level measurement framework for performance evaluation when business process are supported by a WfMS that, during the execution of workflows, stores raw execution data in log files using them to feed the measurement framework.

By the coupling of a WfMS with a RMS we can obtain an additional value in terms of capability to manage operational risks through quantitative techniques. Consider again the opportunity that a risk manager has at definition time to define the reactive behavior of a RMS. The rule b) in fig. 6 shows how a reactive behavior can be relied to a task D. The rule states that when the workflow engine creates an instance of D assigning it to the worklist of an actor, a check has to be done. If the instance of D is created at a time greater than 50 time units after the instance creation of its father, (the process P to which D belongs) then two messages highlighting a schedule risk for the task D are produced, one to the actor that is executing the task and the other to the process owner.

The measurement framework can bring more than a reactive behavior. The need to assess the risk relied to the missing process completion is one of the characteristic that we could require to a system that integrates a WfMS with a RMS. Such proactive behavior lays on the availability of execution data automatically collected by the WfMS and on the risk analysis data represented within the RMS.

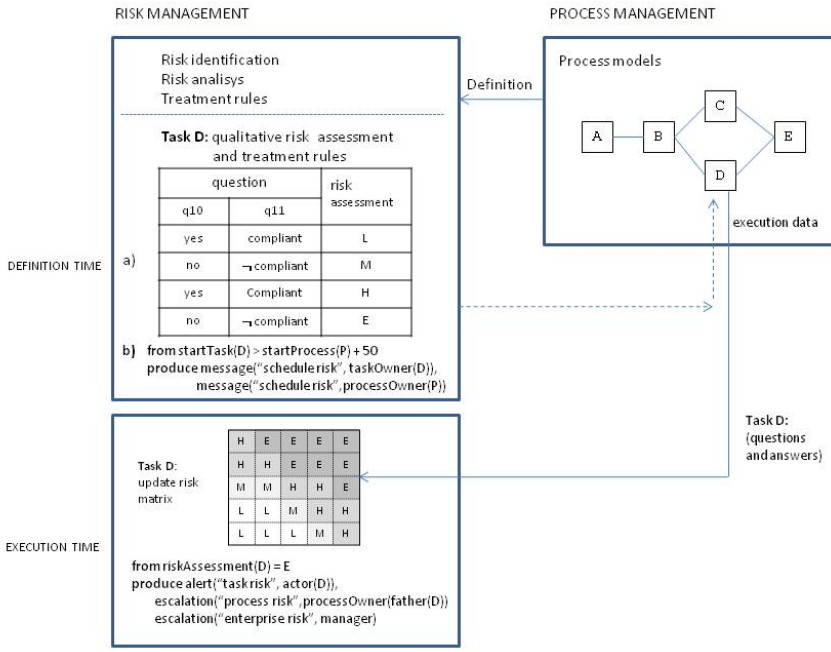

Fig. 6. Relations between process management and risk management

Let P be a process and ip an instance in the execution of P. The WfMS can assess the residual duration of i_p by considering the difference between the average duration of already completed instances of P and the current duration of i_p. Remembering that `sigma` evaluates the sum of measures of instances (filtered by means of p) and that work counts the number of such instances we have:

$$\texttt{residual\_duration}(i_p) = \frac{\texttt{sigma(instance\_duration, filter(I,p))}}{\texttt{work(I,p)}} - \texttt{current\_duration}(i_p) \quad (15)$$

$$\texttt{p= i\_name(i)=i\_name}(i_p) \wedge \texttt{current\_state(i)=completed.}$$

Depending on the value returned by the application of residual_duration, the RMS has three possible alternative interpretations of the expected residual duration of P. When the value is equal to 0 we have an indication that from now on delay will be accumulated; if the value is less than 0, the process is late, otherwise, the residual duration represents an assessment of the time needed to complete the process. The measure `residual_duration` should be evaluated by the WfMS at the completion of each task instance in i_p thus providing in real time to the RMS the information necessary to eventually choose the best reaction to the current situation.

Apart from the workflow measurement framework used in this paper, the risk manager can take advantage of other existing set of risk indicators. It is sufficient to plan at risk definition time both: a) the link between expected value of measures and tasks b) the rules for the risk treatment.
In this way standard measures can be used and evaluated locally to put under control potential risks engraving on tasks. The following ones are two simple measures chosen among a set of widely accepted measures (Hillson, 2004) to evaluate the progress of a project from the cost perspective:

CV = BCWP-ACWP (cost variance)

CPI = BCWP / ACWP (cost performance index)

where BCWP is the Budgeted Cost of Work Performed at a time t_0 and ACWP stands for Actual Cost for Work Performed at tn. Again, the enterprise can receive real time support by the integrated system WfMS+RMS because at task execution time the task cost can feed, for example, the cost variance. This evaluation provides input for the risk treatment rules that define the best reaction to take when the value of cost variance falls below a given threshold.

7. Conclusions

Enterprise risk management is an emergent research field. Apart from application area such as banking, insurance and health where risk management has traditionally been considered a primary management discipline, more and more organizations are planning today the introduction of a risk management system. The model for process oriented risk management proposed here arises from the consideration that the degradation of process execution in terms of poor performances/effectiveness, high costs and low quality can cause great difficulties even undermining the survival of organizations. It can be taken as a reference model by process focused enterprises for the implementation of advanced risk management systems. As a matter of fact, from the coupling of a WfMS with a risk management system we obtain an integrated system capable of managing risks that could have an impact on the regular execution of workflows. Any deviation from the prescribed workflow behavior implies a missed deadline, an increased execution cost or even a danger or an illegal situation. The basic information needs concerning the workflow execution, from the point of view of risk management, can be satisfied by the workflow engine either automatically recording relevant events during the process execution (i.e. creation, completion of work items, task and processes) or collecting qualitative data before or after the examination of each scheduled activity.
Both kinds of measures, qualitative and quantitative are effective tools that help the management to identify threats during the enactment of processes. At risk definition time, the risk manager looks at the definition of activities and processes assigning to them risk monitoring rules that can be automatically managed by the WfMS during the workflow execution.
Even if the implementation of the top level model shown in fig. 1 for process focused risk management can contribute to reduce the cost of data collection and to the acquisition of precise data about workflow execution, the model brings its advantages especially in the

area of operational risks. A risk manager must be aware of this limitation considering the decision support system provided by the process focused risk management as an important part of a wider RMS that can take advantage also of traditional techniques in order to handle the four risk management areas discussed in the introduction.

8. References

Ahmad R.; Yuquing F, Jian T. (2006). Workflow: an enabler to collaborative design process *Proceedings of the 5th WSEAS INT. Conf. on artificial intelligence, Knowledge engineering and data bases*, Madrid, Spain, February 15-17, 2006.

Aiello R.; Esposito A.; Nota G.(2002). A Hierarchical Measurement framework for the evaluation of automated business processes. *International Journal of Software Engineering and Knowledge Engineering*, vol. 12, n° 4, 2002.

Aiello R.; Nota G.; Grieco N., Coppola P. (2004). The Workflow Approach to the Measurement of Distributed Software Processes *Automated Software Engineering: Proceedings of the Workshops CSSE 2004* - Cooperative Support for Distributed Software Engineering Processes, Linz (Austria), 21 September 2004.

Aiello R; Nota G.; Faggini M. (2006). Continuous Process Measurement, Economics and Complexity, 2006, vol. 3, n. 1, ISSN: 1398-1706.

Aiello R.; Nota G., Di Gregorio M.P. (2008). Ontology Based Risk Management New Economic Windows 2008: Decision Theory and Choice: a complexity approach University of Salerno, Italy, 19-20-21 June 2008.

American Academy of Actuaries, Committee on risk Classification, Risk Classification, statement of principles.

Alberts C.J. (2006) Common Elements of risk *CMU/SEI-2006-TN-014,* Software Engineering Institute Carnagie Mellon University, Pittsburgh, PA, 2006

Alberts C.J.; Dorofee A.J. (2009) A framework for categorizing keydrivers of risk *Technical report CMU/SEI-2009-TR-007,ESC-TR-2009-007,* Software Engineering Institute Carnagie Mellon University, Pittsburgh, PA, April 2009.

Alles M.G.; Kogan A.; Vasarhelyi M.A. (2008). Audit automation for implementing continuous auditing : principles and problems, *Ninth International Research Symposium on Accounting Information Systems,* Paris, France, December 13 2008

Basel Committee (2001) on Banking Supervision Consultative document "Operational Risk" January 2001

Basili V.R. (1985). Quantitative evaluation of software engineering methodology , *Proceedings of the First Pan Pacific computer conference ,* Melbourne, Australia, September 1985

Basili V.R.; Caldiera G.; Rombach H.D.(1994). The goal question metric approach, In : *Enciclopedia of software engineering* , John Wiley &sons, Inc., New York , 528-532.

Basili V.R; Melo W.L. (1996). A validation of object-oriented design metrics as quality indicators, *IEEE transactions on software engineering*, vol. 22, NO. 10, October 1996

Basili V.R. (2002). Software modeling and measurement: The Goal/Question/Metric paradigm, *Technical Report CS-TR-2956*, Department of Computer Science of Maryland.

Berarder P.; Jönsoon P.(2006) A Goal question metric based approach for efficient measurement framework definition *ISESE'06*, September 21-22,2006, Rio de Janeiro, Brasil

Cooper D.F.; Grey S.; Raymond G.; Walker P. (2008).*Project Risk management guidelines managing risk in large projects and complex procurements* ,John Wiley & Sons, ISBN 0-470-02281-7

COSO (2004).Enterprise Risk management – Integrated framework. Executive Summary, *Committee of Sponsoring Organizations of the Treadway Commission*, 2004 internal control systems

COSO (2009) Internal control – Integrated framework guidance on monitoring internal control systems

Degl'Innocenti M; Ferrari G.L.; Pacini G., Turini, F. (1990) RSF: A formalism for executable requirement specifications. *IEEE Trans. Softw. Eng. Vol. 16*, no. 11 (1990) pp. 1235–1246

Financial Service Authority (FSA, 2002) *Consultation paper 142,* July 2002

Hillson, David - Earned valued management and risk management: a practical synergy PMI 2004 Global Congress Proceedings – Anaheim, California, USA

Huang S.; Yen D.; Hung Y.; Zhou Y.; Hua J.(2209) A business process gap detecting mechanism between information system process flow and internal control flow, *Decision Support Systems 47* (2009) 436–454

http://www.businessdictionary.com/

http://www.fsa.gov.uk

http://www.psmsc.com/

Kan S.H. (1995). *Metrics and Models in Software Quality Engineering*, Addison Wesley 1995

Leymann F.; Roller D. (2000) *Production Workflow,* Prentice Hall ISBN 0-13-021753-0

McGarry J.; Card D.; Jones C.; Layman B.; Clark E.; Dean J.; Hall F.(2001) *Practical Software Measurement* , Addison Wesley ISBN 0-201-71516-3

Mees W. (2007).Risk management in coalition networks, *Proceedings of the Third International Symposium on Information Assurance and Security, IAS 2007*, August 29-31, 2007, Manchester, United Kingdom, pp. 329–336 (2007)

Mendoça M.G.; Basili V.R. (2000). Validation of an approach for improving existing measurement frameworks, *IEEE transactions on software engineering* , vol. 26, no. 6, June 2000, pp. 484-499

Neef D.; Siesfeld A.G.; Cefola J. (1998) The economic impact of knowledge, Butterworth-Heinemann, ISBN 978-0-7506-70098

Nonaka I.; Nishiguchi T. (2001). Knowledge Emergence : Social Technical, and Evolutionary Dimensions of knowledge creation. Oxford : Oxford University Press 2001 ISBN 0-19-513063-4

Nonaka I. (2005). Knowledge management: critical perspectives on business and management printed by Routledge, 2005 ISBN 0-415-34030-6 vol 1.

Nota G.; Pacini G. (1992). Querying of Executable Software Specifications, *IEEE Transactions on Software Engineering*, vol. 18, n° 8 August 1992.

Nota G.; Aiello R.; Di Gregorio M.P. (2008). Ontology Based Risk Management, *Proceedings NEW2008 - Decision Theory and Choice: a Complexity Approach* – Dipartimento di Scienze Economiche e Statistiche dell'Università di Salerno, 19-20 June 2008.

Nota G.; Carvello R.; Di Gregorio M.P. (2009). Distributed Risk Management in a Virtual Enterprise Environment, submitted to *International Journal of Quality Management*.

Oracle (2002). Oracle workflow Guide, Volume 1, release 2.6.2, Oracle Corporation.

PMBOK (2004). A Guide to the Project Management, Body Of Knowledge (PMBOK Guides), Project Management Institute (2004) Third Edition

Sharmak W.; Scherer R.; Katranuschklov P. (2007). Configurable knowledge based risk management process model within the general construction project process model *Proceedings 24 th W78 Conference,* Maribor, 2007

Stankosky M.A. (2005) Creating the discipline of Knowledge Management *Elsevier Inc. ISBN :0-7506-7878-X*, 2005

Van der Aalst W.; Van Hee K.(2002). Workflow management : models, methods and systems, *Mass : Mit Press*, Cambridge, 2002, P3-27

Weinber G.M. (2001) *An introduction to general systems thinking* Dorset House publishing ISBN 0-932633-49-8

Workflow handbook (1997). Edited by Peter Lawrence John Wiley &_ sons published in association with Workflow management coalition, ISBN 0-471-96947-8

zur Muehlen M. (2004). Workflow-based Process Controlling. Foundation, Design, and Application of workflow-driven Process Information Systems. (Advances in Information Systems and Management Science, 6) (Paperback) Logos Verlag Berlin, 2004, P 99

zur Muehlen M.; Ting –Yi Ho D. (2005). Risk Management in the BPM lifecycle *Business Process Management workshops* Volume 3812/2006 Springer Berlin / Heidelberg