

Integrating Risks in Business Process Models

Michael zur Muehlen
Michael Rosemann
Stevens Institute of Technology
Queensland University of Technology

Howe School of Technology Management
Stevens Institute of Technology
Hoboken, NJ, USA
Email: mzurmuehlen@stevens.edu

Faculty of Information Technology
Queensland University of Technology
Brisbane, Queensland
Email: m.rosemann@qut.edu.au

Abstract

In the context of process management, risk has been considered mainly from a project management perspective. But risk is an inherent property of every business process and techniques are needed to identify, represent and analyse business process risks. The absence of such techniques is a concern because both operational risk mitigation and legal compliance depend on the sufficient identification of corporate risk. This paper addresses the topic of risk management in the context of business process management. We present a taxonomy of process-related risks and discuss how this taxonomy can be applied in the analysis and documentation of business processes. We demonstrate how a contemporary process modelling method can be extended to document process-related risks and their relationships with goals, other risks and processes. A critical administrative process in an university is used as an example.

Keywords

Business Process Management, Risk Modelling, Process Modelling, Risk-aware Process Design

MOTIVATION

In June 2005, the payroll process of a large educational institution failed. More than 4,000 employees were not paid on schedule, but on the following day instead. This unanticipated delay resulted in bounced checks, rejected automatic bill payments and declined check card purchases by staff and faculty, who did not receive information about this delay in time. A hastily installed mediation procedure allowed employees to receive their compensation as a cash disbursement, which was then deducted from their following month's paycheck, depleting cash reserves of the university.

An investigation of the problem revealed that the cause for the delay was a typographical mistake made by a staff member who entered the wrong payroll date in one step of the payroll process. Two administrators signed off on the scheduled payroll run and did not notice the wrong date. The payroll run order was transmitted to the university's bank for processing and when the error was discovered it was too late to re-schedule the payroll run.

What went wrong? The payroll process was clearly designed with mitigation activities in place to ensure its success, and the double sign-off required on the payroll run document should have caught any error. But since for the past decade payroll processing had experienced little, if any, problems, the sign-off had become routine and the date offset by one day did not raise any red flags. The fact that a single data entry activity by an administrator could jeopardize the success of the payroll process was not accurately reflected in the process documentation. As a consequence, the organisation was not sufficiently aware of the impact of this risk. This brief example shows the tight relationship between processes and risks. On the one side, risk management can be seen as a business process, i.e. the different stages of the risk lifecycle form a business process, which requires management. On the other side, risk is an important business phenomenon, which increasingly has to be considered in the (re-)design of business processes (Figure 1). Though there is such a close link, the process and risk management communities are rather separate groups with different research agendas and methodologies.

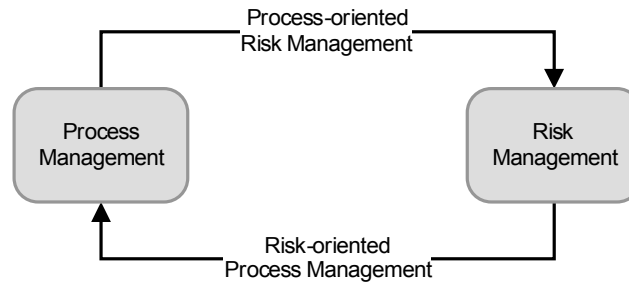


Figure 1: Relationship between Process and Risk Management

Identifying process risks such as data entry errors is of paramount importance to ensure the continuity of business operations and to satisfy compliance requirements generated by legislation such as Sarbanes-Oxley or the Health Insurance Portability and Accountability Act (HIPAA). While compliance to legal standards addresses mainly the protection of personal or financial data, compliance cannot be guaranteed without an analysis of the business processes in which this information is generated, read or changed.

This paper addresses the topic of risk-oriented process management. It reports on the outcomes of the first step of a comprehensive research project, in which we aim for the development of a risk-aware process management methodology. The focus of the current stage is on the development of risk-aware process modelling techniques, which substantially increase the capabilities of existing approaches in terms of risk modelling. The outcomes of our research are of significance for vendors of process modelling solutions, consultants, and public and private organisations.

BACKGROUND

Decision making theory defines risk as “reflecting variation in the distribution of possible outcomes, their likelihoods, and their subjective values” (March et al. 1987). Risk can be expressed mathematically as “the probability of occurrence of loss/gain multiplied by its respective magnitude.” (Jaafari 2001). Since risks are commonly associated with negative outcomes (March et al. 1987), the distinction between risks and problems often remains unclear. Risk is not necessarily a problem, but a “potential problem” that may result from making a particular decision (Charette 1990).

In the context of process management, risk has mainly been addressed as a factor in the management of process-related projects. A notable exception is the case study of the Little Rock Music and Arts Festival by Ballou et al. (2000). The authors discuss risk at the business process level, but their study of the processes remains at a high level of abstraction (e.g., they treat sponsorship arrangements as a discrete business process) and risk is only dealt with from a financial and general business risk perspective, while operational risk at the task level is not addressed. Our approach aims at providing a taxonomy and modelling techniques to include risks in business process models both at the overall process level and at the activity level.

Suh and Han (2003) propose the use of functional decomposition and the Analytic Hierarchy Process to identify business related risks in the IS infrastructure of an organisation. They use a functional model of business operations as a guideline to evaluate the criticality of individual IS components. This traditional view of the organisation does not account for cross-functional components that may support multiple business functions and does not support a process-oriented view of business operations. In this paper we focus on the inclusion of risk in process-centric operations and thus take a different perspective on risk than what Suh and Han (2003) propose.

Yu et al. (1999) discuss different models to assess possible failure modes, effects and their criticality. They list the risk priority number method and the expected cost method as suitable to determine process-related risks. Based on manual operating procedures the authors then present a human error criticality analysis technique that allows for the valuation of possible human error in a given process. This analysis technique leads to an error tree with probabilities, but does not integrate with other conceptual modelling techniques. The purpose of this paper is to provide process modellers with techniques that allow them to capture process-related risks within the scope of established process modelling languages.

Garrett and Apostolakis study the inclusion of system context in the risk assessment phase of software applications (Garrett et al. 1999). They introduce the notion of an “error-forcing context” that will cause a software bug to lead to sometimes catastrophic consequences. They point out that while malfunctions of complex systems are difficult to avoid, they do not always lead to damaging consequences. We include the notion of context in our process analysis by studying the organisational and process goals that might affect the weighting of risk factors.

A TAXONOMY FOR BUSINESS PROCESSES

In order to discuss risk in the context of processes a sound understanding of the notion of a ‘business process’ is required. A business process is widely defined as a structured flow of activities, which supports business goals and is facilitated by data and resources (Harmon 2003; Sharp and McDermott 2001). It requires business objects as input (*e.g.* raw material, an incoming invoice) and transforms them within the process to outputs (*e.g.* a final product, a paid invoice). The core of a process is its control flow, *i.e.* the temporal and semantic relationships between the activities of a process. Various transition conditions can be used to specify this control flow. The following meta model (Figure 2) captures these and a few more elements and relationships in detail. This model is based on the model developed by zur Muehlen (2004) and the separation of entity clusters is inspired by the perspectives proposed by Bussler and Jablonski (1996) in the *Mobile* framework.

In the context of this paper and its focus on risks, two facets are of importance. First, the close relationship between a process and goals shows that processes can have different objectives, and these objectives are supported by the activities within a process. As risks are obviously linked to activities, they also have to be interpreted as being goal-sensitive. A risk which could lead to a potential delay of one day for the entire process is relevant in a process, which aims for a short processing time, but it can be irrelevant in a more quality-focused process. Second, a process consists of much more than just a flow of activities. Thus, there are also many more sources where risks can become potentially relevant. Risks can be related to the incoming business objects (*e.g.* raw material with low quality), data (*e.g.* a vendor master record with outdated conditions), resources (*e.g.* an employee is sick) or information technology (*e.g.* a network transmission fails).

Besides risks that can be associated with the five clusters goal, structure, information technology, data and organisation, the links between these clusters are potential sources for risk as well. For instance, the link between the organisation and activities relates to the correct and efficient allocation of work (*i.e.*, activities) to available employees. The link between the organisation and data relates to access rights of individuals to business objects, and the link between information technology and the organisation relates to the availability of applications to individual employees.

For business processes two lifecycle phases are generally distinguished: Build-time, when the layout and input/output requirements of a process are designed, and run-time, when instances of the designed process are executed. While the clusters goal and structure are of concern during build-time, the clusters organisation, information technology and data gain in significance during run-time.

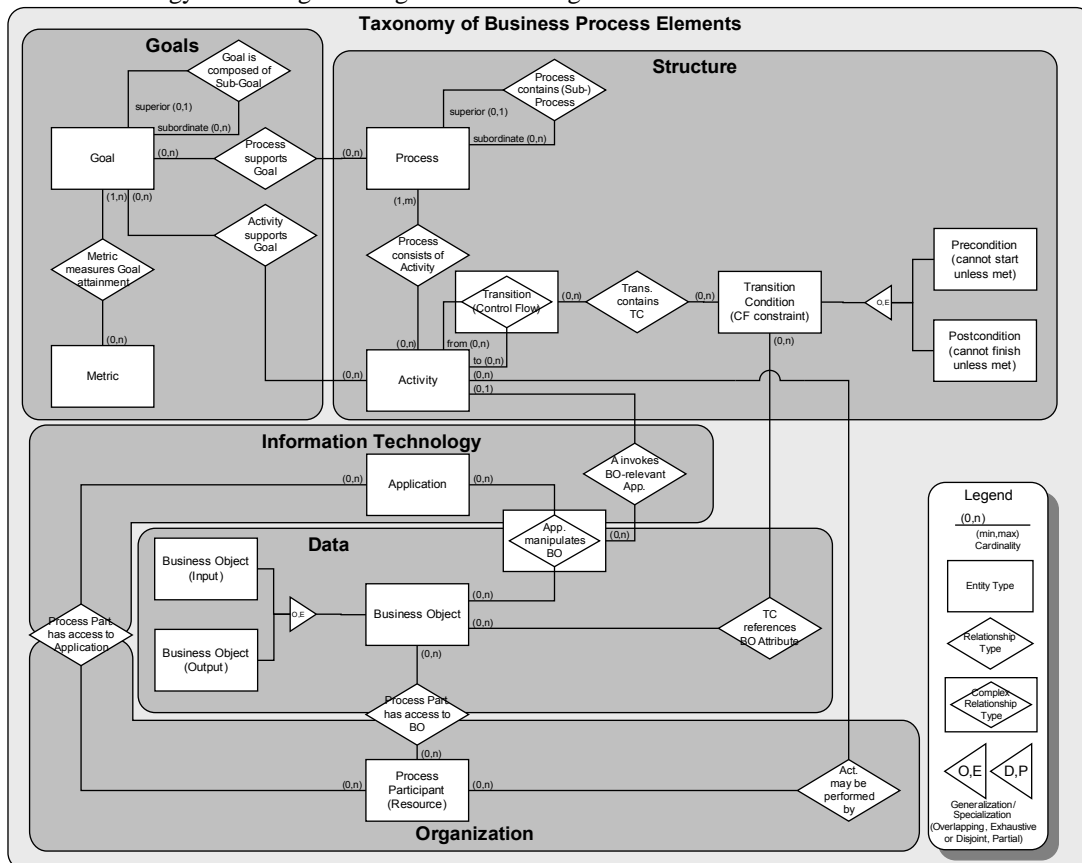


Figure 2: Business Process Taxonomy

A TAXONOMY FOR RISKS

The notion of risk in enterprise projects has been dealt with extensively in the academic literature. The most popular taxonomy of risks in enterprises looks at the risk context. Typically, a business entity is always threatened by natural risks, human risks and environmental risks (Peltier 2004). Similarly, in the area of business process management projects, risks are often categorized into the three groups: people risks, management risks and technical risk (Kliem 2000). Nevertheless, Davenport points to organisational/human resources and information technologies as two major enablers of process innovation (Davenport 1993). This implies that the enablers of process innovation can produce negative impacts on businesses if they are not managed properly.

In their model of risk factors in Enterprise Systems implementations, Scott and Vessey add external business context to the risk factors identified above (Scott *et al.* 2000). They also identify the interrelationships in their risk model which basically suggests that risks can produce positive impacts to businesses if they are well managed within the organisation and if the organisation is able to react outside changes. In Sumner's research, the general risk contexts are broken down into smaller groups: skill mix, management structure and strategy, software system design, user involvement and training, technology planning, project management and social commitment (Sumner 2000).

Figure 3 shows a risk taxonomy in form of an Entity-Relationship model. In our interpretation, risk describes the probability with which an error will lead to an (unwanted) consequence. Since an error type may have multiple consequences, and consequences can be caused by a variety of errors, risk functions as the measuring entity that is connected to the individual error occurrence. Both errors and risks can be classified using the process taxonomy described in the previous section. Goal risks are those that threaten the achievement of process and activity objectives, structural risks threaten the integrity of the process design. These risks are mostly considered during the design of a process, and are difficult to manage once the process is executed. For this reason we call them *build-time risks*.

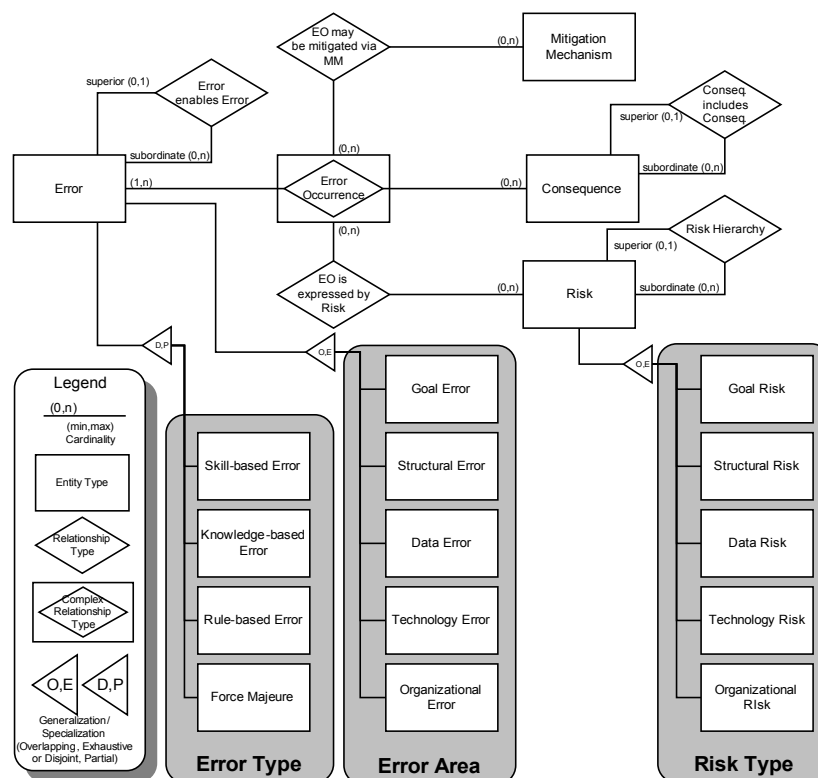


Figure 3: Risk Taxonomy

Structural risks refer to wrong choices made during the design of a process, which may make the process unsuitable to achieve the desired goals. Data, information technology and organisational risks refer to errors that may jeopardize the execution of a given process by undermining data integrity, system availability or employee performance, among others. These risks are typically considered at build-time through the introduction of mitigating activities (such as separation of duty practices, backup systems or data consistency checks). However, many of these risks cannot be eliminated completely because they are caused by the process context, *i.e.*, factors that lie outside the structural and logical design of the business process. This aspect is illustrated in Figure 4 through the notion of error types. Skill-based errors occur, if a resource does not possess the requisite skills to

carry out an activity. Knowledge-based errors occur if a resource misjudges the appropriate actions within an activity and rule-based errors occur if either the design of the process does not allow for the right actions (which would be a build-time risk), or if the right behavioural rules are applied in the wrong context (*i.e.*, if an employee skips a security check because s/he mistakenly believes a customer is entitled to preferential treatment). We therefore call these risks *run-time risks*.

The purpose of risk management is to “reduce or neutralize potential [risks], and simultaneously offer opportunities for positive improvement in performance.” (Ward, 1994, p. 23). A general risk management framework is composed of three main action phases: identification, analysis and control (Kliem 2000). Risks are caused by various uncertainties. Hence it is not easy to frame risks in a precise fashion. One way to do so is to have risks characterised using properties such as impact, probability, time frame and coupling with other risks (Gemmer 1997).

Four risk-handling strategies are suggested in the literature: mitigation (Adler *et al.* 1999), avoidance, transfer and acceptance/assumption (Peltier 2004). Table 1 summarizes these strategies in detail. Not all risk-handling strategies can be applied to all types of risk. For instance, risk transfer and avoidance are typically employed when a risk can be identified at build-time, while risk assumption and mitigation strategies require mechanisms at run-time to deal with the resulting error occurrences. While risk avoidance and mitigation typically aim at reducing the probability of a given error, risk transfer and assumption consider more the magnitude of the error consequences.

Risk Management Strategy	Definition	Examples
Mitigation	To reduce the probability of a risk and/or the impact that an occurrence of the risk may bear. Risk limitation aims at the implementation of controls that dampen the effects of risk occurrences, while not completely alleviating them.	<ul style="list-style-type: none"> • Standardized process routing • Formalized exception handling • Complete kit processing • Collaboration, checks & balances
Avoidance	To eliminate the probability of a specific risk before its occurrence. This strategy is normally realized by trading the risk for other risks that are less threatening or easier to deal with.	<ul style="list-style-type: none"> • Process redesign • Task allocation strategies
Transfer	To shift risk or the consequences caused by the risk from one party to another. Also called “risk sharing”.	<ul style="list-style-type: none"> • Process Outsourcing • Insurance Policies
Acceptance/ Assumption	To adapt to the risk when it becomes a problem. The enactment of a risk contingency plan is required in this strategy.	<ul style="list-style-type: none"> • Adaptation to regulatory requirements

Table 1: Risk Management Strategies

RECOMMENDATIONS FOR A RISK-AWARE PROCESS MODELLING TECHNIQUE

The previous sections demonstrated the complex nature of processes and risks. Conceptual modelling is an established approach to comprehend different types of complexities, *e.g.* complexity related to data, processes, organisational structures, etc. (Gupta and Sykes 2001). However, at this stage classical IS modelling techniques such as ER, UML, Petri Nets or IDEF do not explicitly capture risk-related information. We propose to utilise conceptual risk modelling in order to be able to consider risk as part of process management projects.

In detail, we propose four interrelated model types in order to appropriately capture risk in the context of business processes. We will use the widely accepted Architecture of Integrated Information Systems (ARIS) and extensions of the embedded Event-driven Process Chain Notation (EPCs) in order to visualise our ideas (Scheer, 2000). The assumption is that a widely used methodology such as ARIS will be beneficial for the dissemination of our suggestions. However, our proposal can be easily applied to different process modelling techniques (*e.g.* UML, BPMN). Two of the models related to structural and behavioural properties of risks, while the other serve as integration models that relate risks to process goals and to the overall process structure respectively.

The four proposed model types are:

- Risk Structure model
- Risk Goal model
- Risk State model

- EPCs extended with risks

Risk Structure Model

A risk structure model provides insights into the hierarchical relationships between risks. This model type supports the two basic semantic relationships composition (*i.e.*, is-part-of) and generalisation/specialisation (*i.e.*, is-a). Modelling *composed risks* is helpful to understand what risks have to occur together so that one risk can occur. In our payroll process, for example, the risk that the administrators do not realize that the date of the payroll is incorrect consists of two sub-risks, *i.e.* two administrators check the date and any of these two can potentially identify the wrong date. Modelling *specialised risks* helps to elaborate on the details of risks. For example, the risk of a wrong data entry can be specialised into ‘Wrong date for payroll run is entered’, ‘Wrong employee number is entered’, ‘Wrong bank details are entered’, etc. As such, capturing more generalised risks helps to classify different types of risks. Figure 4 shows two examples for such risk structure models. The composition is shown on the left, and the specialisation can be seen on the right of this figure. Such risk structure models can already be designed with the ARIS Toolset 6.2.

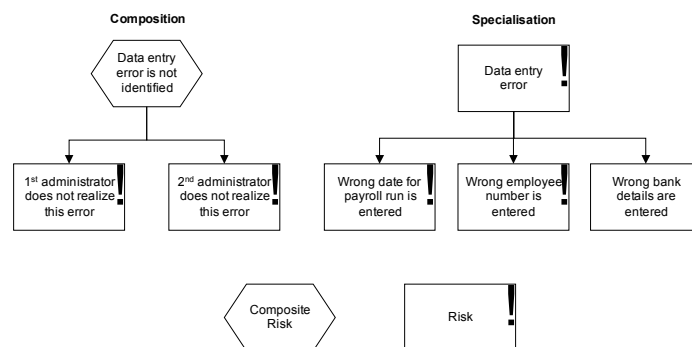


Figure 4: Examples for Risk Structure Models

Risk Goal Model

Risks have been defined as possible occurrences which could lead to the situation that a pre-defined goal is not achieved. As such, different risks have impact on different goals. The risk goal model is a matrix with risks forming the rows and goals placed in the columns. Thus, it supports two viewpoints. First, it can be studied what impact a risk can have on different goals. If goals are weighted with scores to reflect their importance, such a model can support the identification of important risks. Second, the risk goal model shows the risks that a goal is exposed to. This information is helpful to uncover goals that are unlikely to be reached or that require extra protection through risk mitigation mechanisms or similar.

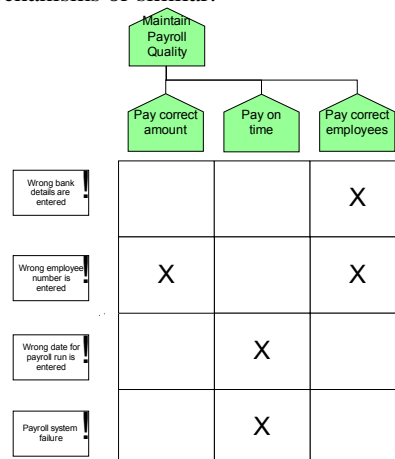


Figure 5: Example for a Risk Goal Model

The risk goal model can potentially be complemented by a goal stakeholder model, which can be used to capture the relevance of a goal for different stakeholder groups (*e.g.* customer, employee). In combination with the risk goal model it can be used to highlight and calculate the risks from the view of different stakeholders. As part of this paper, we do not further elaborate on the goal stakeholder model as it has in principle the same matrix-based design principle like the risk goal model, and as it does not focus on risks.

Figure 5 shows an example for a risk goal model. In this matrix the risk “Wrong employee number is entered” affects both the goal “Pay correct amount” and “Pay correct employees”. The first goal is at risk because associating a wrong employee number with a particular payroll run detail may lead to an employee being paid the salary of another employee. The second goal is at risk because the entering of an employee number that does not refer to an existing employee may lead to a cancellation of the payment and the intended recipient may not be paid during that particular payroll run.

Risk State Model

The previous two model types support the description of static risks characteristics. However, further model types are required to capture the dynamic aspects of risks. We propose to capture dynamic characteristics of risks in two different model types. First, we will elaborate on the risk state model. A risk state model is a new model type consisting of the object types risk, consequence and the control flow connectors exclusive OR (XOR) and AND. The purpose of a risk state model is to depict non-hierarchical interrelationships between risks and the causal relationships between risks and consequences. In its simplest form a risk state model consists of one risk leading to one consequence. The probability of the risk corresponds in this case with the probability that the (unwanted) consequence occurs. However, in many cases only a number of risks together lead to a certain consequence. These consequences are depicted in the risk structure model as composite relationships.

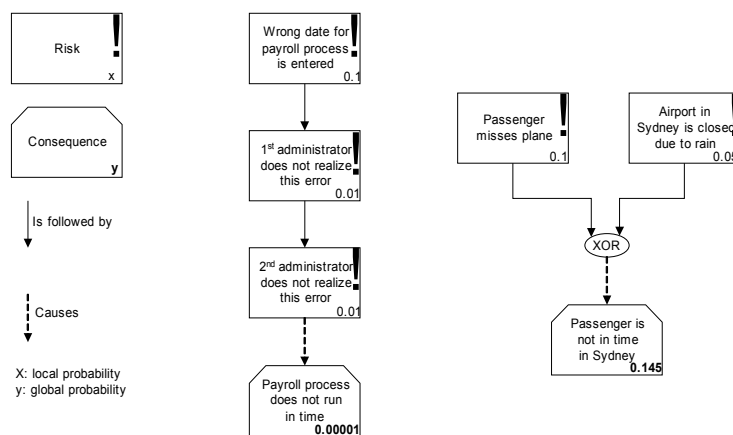


Figure 6: Examples for Risk State Models

An example related to the payroll process is the fact that one person enters the wrong date AND two administrators subsequently do not realize this error leads to the consequence that the payroll process does not run in time. In this case the three risks (wrong data entry, first administrator does not realize error, second administrator does not realize error) are in a sequential relationship. The local probability for one risk (e.g., wrong data entry) is different to the probability that the consequence occurs. Instead all probabilities along this sequence have to be multiplied in order to calculate the probability that the unwanted consequence occurs. Such sequential risk state models typically describe risk mitigation procedures in place. Risks in a risk state model do not have to be in a sequential relationship. An example related to the unwanted consequence ‘not being in time for a meeting in Sydney coming with the plane from Brisbane’ would be that the person either misses the plane in Brisbane, or in rains in Sydney and consequently all planes to Sydney are late. A risk structure model would not indicate any relationship between these two risks. In this case the occurrence of only one risk is sufficient to lead to the consequence. Thus, the probability that the consequence occurs is calculated as: $1 - (1 - \text{probability for risk A}) \times (1 - \text{probability for risk B})$. As a risk state model captures important relationships between risks and consequences, it is a valuable data source for calculating the total probability for a consequence. Figure 6 provides two examples for such risk state models.

EPCs Extended with Risks

The culmination of linking risks and processes is to highlight relevant risks in an actual business process model. While the risk state model is focused only on the risk as a model element, the proposed extended risk-aware Event-driven Process Chain (EPC) can be used to assign risks to the individual steps of a business process. In these cases a relationship between the functions of an EPC and risks indicates steps in the process which are exposed to risk. The consideration of the probability and magnitude of the assigned risks can then be used to quickly identify the most critical functions (i.e., activities) in a process model. An example for such a risk-extended EPC can be found in Figure 7. This diagram shows the events (hexagons), functions (soft rectangles), the control flow (arrows between events and functions), the control flow logic (here an exclusive OR represented

as an XOR), the involved application (payroll system), the input and output data (on the left), the organisational responsibilities (on the right) and the assigned risks.

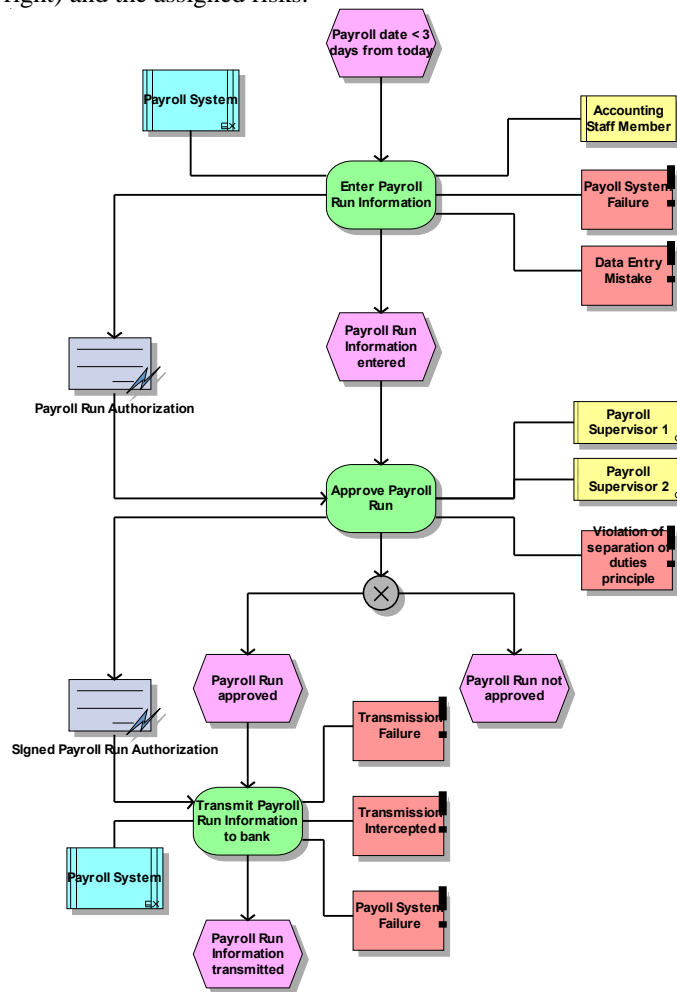


Figure 7: eEPC of the Payroll Process with Common Risks Attached to Functions

However, this notation is not able to capture *all* types of process-related risks as discussed in the taxonomy of business processes (see Figure 2). In particular, it is not possible to capture risks related to process elements other than functions. For the purpose of a more comprehensive model, which captures different types of risks in the context of a process model, we propose a column-based notation (see Figure 8). In this model each risk type (see Figure 3) is captured in a separate column next to the process model.

CONCLUSION

Process management and risk management are both topics of increasing popularity. However, at this stage there are no consolidated approaches, which either apply the process paradigm to the risk management discipline, or consider risks as part of business processes. Our paper makes a first step towards a more risk-aware process modelling technique. After presenting taxonomies for business processes and risks, we propose four interrelated model types, which together can accommodate risk-related requirements. The models have been explained using the payroll process as an ongoing example. These proposed model types, especially the risk goal model, the risk state model and the EPC in column display, extend the widely used ARIS approach towards capturing risk. As such, they are potentially significant for organisations with interest or pressure to model risk in the context of business processes. The results are also of importance for modelling tool vendors who are pressed to deliver conceptual solutions for risk modelling.

This paper has a few *limitations*. First, we are still in the ‘Generate design alternatives’ phase of Simon’s Generate/Test Cycle (Simon 1996; Hevner *et al.* 2004). Consequently, we are still searching for a satisfying solution. Our current evaluation method is very much a descriptive informed argument, in which we try to provide a convincing case by elaborating on the insufficiencies of existing techniques. However, we believe that our proposal has reached the level of maturity that we can enter the stage of empirical testing. We already contacted a number of organisations in Australia and in the USA with interest in process modelling in the context

of Sarbanes-Oxley. Second, our proposal is centred on extensions of ARIS-based modelling techniques. However, we do not see main challenges in transferring these conceptual ideas to other modelling techniques.

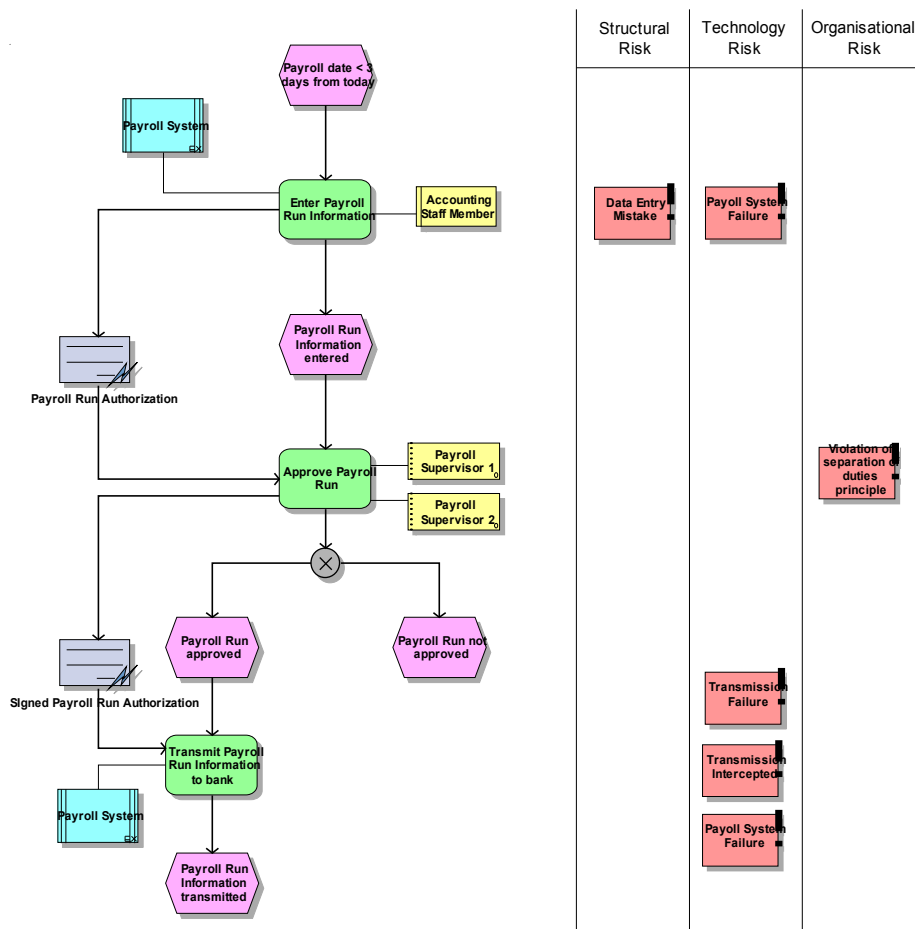


Figure 8: Extended EPC in Column Notation

In our *future work*, we will empirically test our proposed solutions for capturing risks against realistic requirements. We will conduct observational evaluations by applying our extended methods with existing ARIS users in Australia and USA. Thus, we aim for action research with the aim to iteratively improve the proposed techniques. Second, we want to finetune our proposed techniques for specific risk management purposes. A focus will be most likely on the requirements of Sarbanes-Oxley. Third, we will include risk mitigation in our proposed extensions of ARIS. As a consequence, we will develop extended meta models and new model types, which can be used to capture control activities and the risk management strategies as outlined in Table 1.

REFERENCES

- Adler, T. R., Leonard, J. G. and Nordgren, R. K. (1999) Improving Risk Management: Moving from Risk Elimination to Risk Avoidance, *Information and Software Technology*, 41, 29-34.
- Ballou, B., Godwin, N. H. and Tilbury, V. (2000) Riverfest: Managing Risk and Measuring Performance at Little Rock's Annual Music and Arts Festival, *Issues in Accounting Education*, 15, 483-512.
- Charette, R. (1990) *Applications Strategies for Risk Management*, McGraw-Hill, New York.
- Clemons, E. K., Thatcher, M. E. and Row, M. C. (1995) Identifying Sources of Reengineering Failures: A Study of the Behavioral Factors Contributing to Reengineering Risks, *Journal of Management Information Systems*, 12, 9 - 36.
- COSO. (2004) *Enterprise Risk Management - Integrated Framework. Executive Summary*, 16: Committee of Sponsoring Organizations of the Threadway Commission.
- Davenport, T. H. (1993) *Process Innovation*, Harvard Business School Press, Boston, Massachusetts.
- Evans, A. (2004) Operational Risk Management, *Risk Management Magazine*, 51, 50.

- Garrett, C. and Apostolakis, G. (1999) Context in the Risk Assessment of Digital Systems, *Risk Analysis*, 19, 23-32.
- Gemmer, A. (1997) Risk Management: Moving Beyond Process, In *Computer*. Vol. 30, 33 - 43.
- Guimaraes, T. (1997) Empirically Testing the Antecedents of Bpr Success, *International Journal of Production Economics*, 50, 199-210.
- Gupta, P., Sykes, J. A. (2001) Conceptual Modeling Process and the Notion of a Concept. In: *Information Modeling in the New Millennium*. IDEA Group Publishing, Hershey 2001, pp. 53-69.
- Harmon, P. 2003: *Business Process Change*. Morgan Kaufman Publishers. San Francisco.
- Hevner, A. R., March, S. T., Park, J. (2004). Design Science in Information Systems Research. *MIS Quarterly*, Vol. 28, No. 1, pp. 75-105.
- IT Governance Institute. (2004) IT Control Objectives for Sarbanes-Oxley. The Importance of It in the Design, Implementation and Sustainability of Internal Control over Disclosure and Financial Reporting, 84. Rolling Meadows, IL.
- Jaafari, A. (2001) Management of Risks, Uncertainties and Opportunities on Projects: Time for a Fundamental Shift, *International Journal of Project Management*, 19, 89-101.
- Jablonski, S., Bussler, C. (1996) *Workflow Management. Modeling Concepts, Architecture and Implementation* International Thomson Computer Press, London et al.
- Kliem, R. L. (2000) Risk Management for Business Process Reengineering Projects, *Information Systems Management*, 17, 71-73.
- March, J. G. and Shapira, Z. (1987) Managerial Perspectives on Risk and Risk Taking, *Management Science*, 33, 1404-1418.
- Peltier, T. R. (2004) Risk Analysis and Risk Management, *The EDP Audit, Control, and Security Newsletter*, 32.
- Remenyi, D. and Heatfield, A. (1996) Business Process Re-Engineering: Some Aspects of How to Evaluate and Manage the Risk Exposure, *International Journal of Project Management*, 14, 349-357.
- Scheer, A.-W. (2000). *ARIS – Business Process Frameworks*. Springer-Verlag: Berlin et al.
- Scott, J. E. and Vessey, I. (2000) Managing Risks in Enterprise Systems Implementations, *Communications of the ACM*, 45, 74-81.
- Sharp, A., McDermott, P. 2001: *Workflow Modeling*. Artech House. Boston, London.
- Simon, H. A. (1996). *The Sciences of the Artificial*. 3rd ed., MIT Press: Cambridge, MA.
- Suh, B. and Han, I. (2003) The Is Risk Analysis Based on a Business Model, *Information & Management*, 41, 149-158.
- Sumner, M. (2000) Risk Factors in Enterprise-Wide/Erp Projects, *Journal of Information Technology*, 15, 317-327.
- Ward, S. and Chapman, C. (1994) Transforming Project Risk Management into Project Uncertainty Management, *International Journal of Project Management*, 21, 97-105.
- Wieggers, K. (1998) Knowing Your Enemy: Software Risk Management, *Software Development*, 6.
- Yu, F.-J., Hwang, S.-L. and Huang, Y.-H. (1999) Task Analysis for Industrial Work Process from Aspects of Human Reliability and System Safety, *Risk Analysis*, 19, 401-415.
- zur Muehlen, M. (2004) *Workflow-based Process Controlling. Foundation, Design, and Application of workflow-driven Process Information Systems*. Logos, Berlin, 315.

COPYRIGHT

Michael zur Muehlen, Michael Rosemann © 2005. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.