Operational risk analysis in business processes

A K Jallow, B Majeed, K Vergidis, A Tiwari and R Roy

The operational continuity of a business process is an important performance indicator that contributes to the perceived quality of service delivery, hence it is important to understand and monitor the underlying issues that can affect the performance of the process. These issues might have been foreseen at the beginning of the process design and deployment phase, or might have emerged during the execution of the process, and must be viewed as risk threats to the business process. In most cases risk is only considered from the project management angle or from financial, market, insurance and other general business perspective. Operational risk at service provision level receives little attention and thus there is a need to develop methodologies and tools to identify and analyse business operational risks. The authors concentrate on operational risk for business process management by introducing a novel way for applying risk assessment frameworks at the process activity level. The paper briefly reviews existing risk frameworks and selects the COSO framework as the most appropriate for business processes. This framework is modified in order to address and evaluate the main elements of business processes. It defines a statistical approach towards operational risk assessment by quantifying risk factors in each activity within a business process for service provision. A risk forecast is produced for each activity, and for the whole process, to model associated uncertainties and to contribute in identifying the risk factors that affect the business process objectives. To demonstrate the framework, it is applied to a hypothetical process involving setting up a network service. These results help to advise on which risk factors need higher attention in order to achieve successful process fulfilment.

1. Introduction

In today's modern business environment, organisations are pushed for fast delivery of quality services to customers in order to gain competitive advantage. This results in operational risk being distributed down the levels of the enterprise hierarchy towards the business process layer. The disruption of business operations due to the realisation of some of the process risks has become a serious threat to the organisation's operations affecting its strategic objectives. Financial and insurance institutions over the past decades have experienced losses in revenue as a result of operational failures/risks. Business success is largely dependent on reducing the operational risks thus improving operational efficiency. The consumers of services are more demanding and uncompromising in terms of expected quality and can lose confidence in the service provider if services are disrupted frequently. Service organisations need to support their operations continuously in order to avoid operational failure. This paper introduces a framework for capturing and forecasting the operational risks in service-related business processes.

2. Related Work

To begin with we briefly discuss the concept of risk, methods of risk analysis and we also provide an overview of existing risk frameworks. Risk is identified within the organisational processes that are either in the form of a project or a continuous operation. When the identified risk is actually realised, organisations are not able to successfully deliver projects and operations fail to complete. Archer [1] observes that the successful operation of any business depends on risk management. Therefore there is a need to manage risk in order to achieve the organisational aims and objectives effectively.

There have been many different definitions and approaches towards risk. Knight [2] distinguished between risk and uncertainty. He defined as risks those events for which the probability of occurrence can be calculated as opposed to uncertain events for which analysis is impossible because their occurrence does not follow an apparent pattern. According to Frost et al [3], risks are uncertain future events which could influence the achievement of the organisation's objectives, including strategies, operational, financial and compliance objectives. Most definitions treat risk as a threat to organisations as it can affect the manner in which business processes are carried out for both customer and stakeholder satisfaction in accordance with strategic objectives [4]. It is also important to mention that risk has two attributes attached to it. These are:

- impact, i.e. the consequence of the risk realisation related to the process,
- probability, i.e. the relative chance that the event will occur.

A challenge is for risk to be measured and quantified precisely. Risks can be calculated relatively using factors such as impact, probability and time frame, combined with other risk factors [5]. Link and Marxt [6] — similarly to Jaafari [7] — calculate risk mathematically, as the impact multiplied by the probability of occurrence. The main focus of this paper is operational risk that is different from the general risk. Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events [8]. Operational risk is crucial to the continuity and reliability of operations within an organisation because it destroys value for all shareholders [9].

2.1 Risk analysis

Risk identification is the process of establishing which risks are likely to erupt from the business operations. Some of these risks may be internally caused, but there are external drivers that could force risks into operations. The quality of information generated in risk identification determines how well the results or outcomes of the risk analysis will be. Risk analysis is the development of a quantitative estimate of risk based on engineering evaluation and mathematical techniques. In risk analysis there are tools, techniques and methodologies used to enhance and facilitate the process. It is important to note that answers to the questions asked in the risk assessment help risk analysts identify, measure, quantify and evaluate the risks and their impact [10].

There are two main risk analysis methods — qualitative and quantitative. Both these methods are facilitated by powerful software tools. Qualitative risk analysis methods according to Suh and Han (2003) determine loss based on the knowledge and judgement of a risk analyst rather than on precise monetary values. In most cases, the analysis of the probability and impact is carried out by the risk owners as they should be the people best able to analyse, plan and manage risk. Certain players should be involved in this type of analysis. These include relevant stakeholders, subject matter experts and the person who identified the risk. The analysis should measure the probability of the impact of identified risk in terms of time, cost, and performance. Quantitative risk assessment (QRA) measures the risk based on a monetary or discrete value. According to Kendrick [12], quantitative methods strive for greater precision, and they reveal more about each risk. Also there are many computer software models that support risk analysis quantifying risk by implementing statistical methods. Computer-aided risk assessment can greatly facilitate quantitative analysis in the treatment of uncertainty in several ways [13]. The most common of these software tools support Monte Carlo simulation by using a representation of a business operations system and simulating it iteratively to analyse its performance.

2.2 Risk frameworks

Risk management in modern organisations is growing at a fast pace though not a new concept. Over the past twenty years risk management has been significantly developed and formalised. The primary aim of risk management is to ensure that all project and operational threats to businesses are identified and controlled; it is currently regarded as one of the main topics of interest for researchers and practitioners working in the area of project management [14]. There are various risk management frameworks proposed in literature. Despite their different steps, they all aim at identifying, planning and controlling the risks that are expected in a project or operation. Risk analysis is an essential part of all risk management frameworks. A selection of the existing frameworks and the stages these involve is presented in Table 1.

Table 1 A selection of risk management frameworks.

Framwork name/source	Risk framework description (main steps)
PMI body of knowledge	Risk framework involving four stages: 1. Risk Identification, 2. Risk quantification, 3. Risk response development, 4. Risk response control.
The COSO framework [16]	Enterprise-wide framework with eight interrelated components: Internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, andmonitoring.
The Software Engineering Institute [17]	Framework consisting of five distinct phases: identification, analysis, response planning, tracking and control which are linked by an ongoing risk communication effort.
Fairly [18]	A framework consisting of seven steps: identify risk factors, assess risk probabilities and effects, develop strategies to mitigate identified risks, monitor risk factors, invoke a contingency plan, manage the crisis, and recover from the crisis.
Continuous risk management (CRM) framework [19]	NASA's risk framework has six phases and is a life cycle process: identify, analyse, plan, track, control and communicate risk.

Table 1 shows that these risk frameworks follow a similar approach towards risk in terms of sequence of steps. Their differences, however, lie in the sub-processes and how formalised and detailed they are [14]. What is missing from most of these frameworks is an activity-based approach to provide more accurate risk measures for the complete process. High-level risk analysis often proves unrealistic. Breaking down risk into the main elements of a process, thus analysing the impact for each activity, helps in acquiring more accurate risk estimations. The next section presents an activity-based risk analysis framework.

3. A framework for risk analysis in business processes

A comprehensive risk management framework should be able to support all the different stages of risk management from identification and quantification to mitigation and control mechanisms. Kliem [20] defines the three main action phases of a general risk management framework — identification, analysis and control. Our work focuses mostly on the first two aspects, i.e. risk identification and analysis within the business process context. According to Zhou and Chen [21], the typical evaluation criteria of business process performance are cost, time and output quality. Consequently, any business-process-related risk quantification and analysis approach should address these three elements. These are briefly discussed below in the risk framework context:

- Cost analysis

  Statistical cost analysis of risk factors can illustrate to business analysts how much impact on cost and budget an activity-level risk can generate to the business process. This enables the identification of the risk factors that are likely to significantly increase the cost of the activity and the potential to deal with them in order to reduce the estimated process cost.

- Time analysis

  The statistical time or schedule analysis of risk factors can illustrate how much impact on time/schedule a risk has from activity level within the process. Schedule risk analysis enables the prevention of time delays in the process by inspecting each activity individually.

- Performance/Quality Analysis

  The statistical analysis of the performance of activities with focus on risk factors can justify the potential impact of a risk on quality from activity level. Activity performance measurement can identify the risk factors that potentially can have a negative contribution towards the performance of the activity.

The risk assessment framework is built around these three dimensions. Statistical analysis is applied to each of them as it can provide accurate assessment of the probability and impact that risks have upon the operations of the business process. Process-based statistical risk analysis focuses on the unique activities involved in a business process and identifies which particular activities need greater attention, thus focusing more resources towards them. The framework uses a business process model broken down into the individual activities. For each activity the potential risks are identified, quantified and Monte Carlo simulation is used to produce different forecasts and scenarios. The proposed framework uses a combination of both qualitative and quantitative methodologies in order to identify and assess the different risk factors. It also follows the principles and the stages of the COSO Framework (see Table 1). The COSO risk framework is widely used within the ICT sector and is popular in other industries including financial and insurance companies. COSO has a comprehensive risk management process which looks at risk management from an enterprise-wide point of view. The framework presented in Fig 1, demonstrates our interpretation of the COSO framework in the business process context. The sequential steps below comprise our methodology that aims at carrying operational risk to business processes. To the authors' knowledge, it is the first approach of applying a risk framework to business processes.

- Step 1 — Model the activities of the business process

  The framework supports activity-based risk analysis. Instead of analysing the risks of a complete process, the framework uses as input a business process model that consists of unique process activities. Having a series of activities, there is a capability to analyse the risks for each activity and then for the complete process.

- Step 2 — Determine the objectives

  As mentioned previously, business processes are evaluated based on the three dimensions that this framework supports — cost, time and performance. Breaking down the business process into a series of interconnected activities, inevitably associates each activity with the same dimensions, i.e. each process activity has an expected duration (time), a cost of execution and an output (performance). The framework supports risk analysis for each of these dimensions of a business process but one at a time and not a combination of them which could be a future extension. Therefore, each time that the framework is considered, the objective of the risk analysis needs to be specified. Business process risk analysis can then focus on the risks of process completion either on time, or within the process budget or according to defined key performance indicators (KPIs).

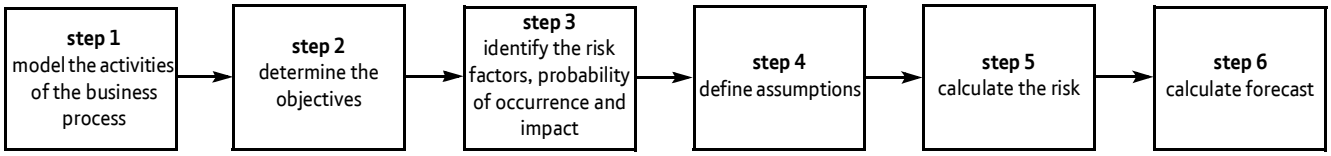

Fig 1 The risk-based proposed framework.

- Step 3 — Identify the risk factors, probability of occurrence and impact

  This stage identifies risk factors for each activity of a given operational business process. These factors could be driven internally as well as externally which means event identification should incorporate both these environments as supported by the COSO framework. The identification of events must differentiate those that would negatively affect the effectiveness of the operations (i.e. risks) from those with positive effects (i.e. opportunities). Once the risk factors of an activity are identified, their probability of occurrence (measured in percentage) needs to be calculated. Probability of occurrence measures the probability that the risk will actually occur. When a risk does occur in a business process an associated impact is suffered. Estimating the impact helps the business analysts to determine how risks affect the business process KPIs.

- Step 4 — Define assumptions (regarding the risk impact)

  When analysing risks it is important to incorporate the uncertainties that are associated with them. It can be very challenging to estimate accurately the exact impact of a risk. Providing a single value as risk impact may result in unrealistic analysis. To avoid this, assumptions should be defined to take into account the uncertainties associated with risk. A three-point estimate (low, most likely, maximum) and a triangular distribution are used to quantify the uncertainties of each risk factor in order to define the assumptions. Other distributions can be also used to define the assumptions of uncertainties depending on the nature of the assumption. Other distributions involve normal, uniform, binomial, lognormal, discrete uniform, etc.

- Step 5 — Calculate risk

  For each risk factor identified, a risk output is calculated. Each risk factor is calculated by multiplying the probability of its occurrence by the magnitude of its impact. The impact is not a discrete value but a series of values generated by the simulation based on the distribution; it results from random values selected within the range of the distribution.

- Step 6 — Calculate forecast

  The framework produces two different types of risk forecast, one for each individual process activity and one for the complete business process. The activity forecast takes into account the accumulative outcome of all the risk factors that were identified for a particular activity. The business process forecast is the sum of activity forecasts. Based on these forecasts, analysis of risk can occur by identifying the risk factors that can have a significant influence on the business process in terms of excess costs, overtime or poor performance.

The different steps of the risk framework are utilised in an assessment table for each of the process activities. Assessment tables can easily be implemented or incorporated into spreadsheets thus making the necessary calculations straightforward and enabling the application of Monte Carlo simulation. Abiding by the steps of the framework, an assessment table is created and a forecast is calculated for each activity which are then added together to produce the forecast for the complete business process. The application of the framework to a simple process example is described next to explain how these steps are carried out in practice.

4. Application to a business process

The risk assessment framework presented above is applied to a hypothetical business process. The business process is network provision by a small telecommunications operator and is discussed and broken down into its main activities as shown below. Then for each activity the risk assessment table is filled and the forecasts for the activities and the complete process are presented.

4.1 Business process description

The network provision process involves activities from inception to provision of the operations, and ensures that supply is functional. The process makes use of different resources, e.g. human, material and financial. These resources are used in all the activities of the process. The main activities involved in setting up the network are survey, analysis, and installation and supply. The process activities are shown in Fig 2 and discussed in more detail below.

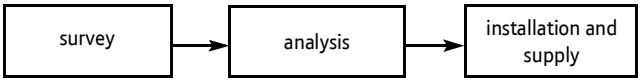

Fig 2 The network provision business process.

- Survey

  This activity surveys the current environment to establish that all information and resources required to proceed with the project are available and fit for purpose. Existing customer facilities are reviewed and staff readiness for such changes is also studied. The network design is also part of the survey. IT systems are looked at and their effect and contribution towards the business delivery of the client are reviewed.

- Analysis

  In this activity, a prototype network solution is set up and analysis is conducted to look into the efficiency of its services. Network traffic is studied and inspection of the internal and external activities is also conducted. Transfer and receipt of data are analysed as well as hardware capability for this purpose. Network access and security control as well as intrusion are also analysed. Analysis is also done with reference to the national IT programme's policy for IT implementation and usage.

- Installation and supply

  Having completed all the analyses, minor corrections are made on errors that are identified within the prototype network. The installation includes laying the cables, configuration of the server and other software. Firewalls and virus protection software are installed and trials are made. Routers and switches are also acquired and installed, based on the service requirements. Patch panels are erected where the switches and routers are kept. Following the installation, the network service starts operations and users are given the access to use the facilities. Network downtime is analysed when the service starts its operations as well as any unauthorised access. A network audit trail is also incorporated in the installation for administration purposes. User training and minor maintenance procedures are also provided to the IT teams of the client.

However, it is rarely the case that all these activities are conducted without any hitches. As stated earlier, there are sometimes particular tasks within activities that are not completed on the anticipated schedule and/or within the allocated budget. These can be threats to the successful completion of the activities that thus have a negative impact on the business process. To assess the impact of these threats risk assessment is carried out.

4.2 Risk assessment of the individual process activities

After having studied all the activities within the process of setting up the network, it is necessary to try to identify associated risk factors that can affect the accomplishment of the tasks. Risk assessment includes identification and quantification of the risk factors associated with each activity. The quality of risk information generated in this stage has a crucial effect on the risk quantification process. Risk analysts are asked to provide risk factors for the three activities of the business process using both historical data and brainstorming as risk identification methods. Risk factors are identified along with the probability of their occurrence and with their impact both on the activities and the process.

In this hypothetical example only cost risk analysis of the business process is demonstrated. The idea, however, is the same for the other objectives, time and performance, that are also supported by the proposed risk framework. In addition, we only present the detailed analysis of the survey activity as detailed below.

For the survey activity, it is assumed that the initial budget is £5000[1]. Three risk factors are identified by the experts — expertise (20%), access to site (10%) and IT equipment (5%). The numbers in brackets represent the corresponding probabilities for each risk factor, i.e. there is a 20% probability that enough expertise would not be available to perform the survey. If this — or any other — risk occurs there will be an impact on the activity and on the process.

Since we are dealing with cost risk analysis, the impact that we are interested in is expressed as the excess cost that will occur in both the activity and the whole process. This cost impact is usually uncertain and must be modelled or estimated using a probability density function to take the uncertainty into account. Depending on the available knowledge, a number of distribution functions can be used to model the impact.

In this example, we have elected to use the triangular probability density function to describe the cost impact of all risk factors. This triangular density function is both simple and widely used in modelling risk impact, especially in cases where there is not enough information to generate a more sophisticated function (e.g. a normal distribution). The triangular distribution has a lower limit l, mode m and upper limit u as shown in Fig 3. Notice that the total area under the curve is equal to unity and the highest probability is $2/(u-l)$.

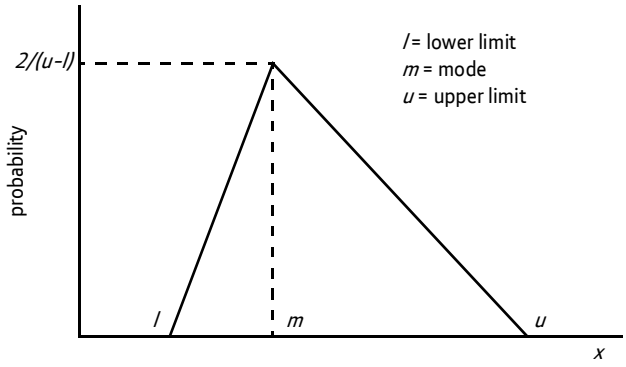

Fig 3 Probability density function — triangular distribution, l = lower limit, m = mode and u = upper limit.

For the survey activity we assume that the lack of expertise risk impact has a triangular distribution with a lower limit of £900, a mode of £1000 and an upper limit of £1200. A similar interpretation applies to all other risk factors associated with survey activity as shown in Table 2.

The nominal output column in Table 2 represents the increase in cost resulting from the mode of the triangular distribution. Later on we will discuss how the other values are used with the Monte Carlo simulation.

In a similar manner, the risk factors for the other two process activities are identified and the risk assessment is produced as shown in Tables 3 and 4.

[1] It must be emphasised that all cost figures in this example are for the purpose of demonstrating the techniques and thus have no connection to actual figures.

Table 2 Risk assessment of the survey activity.

Activity 1 — survey		Budget = £5000			
		Impact on cost (triangular distribution)			
Risk factors	Probability	Lower limit	Mode	Upper limit	Nominal output (prob × mode)
Expertise	20%	£900	£1000	£1200	£200
Access to site	10%	£3200	£5050	£7000	£505
IT equipment	5%	£25	£50	£75	£2.5
			Total impact on cost		£707.5
			Total budget		£5707.5

5. Monte Carlo simulation results

Having gathered the information needed on all the risk factors identified within each of the activities, a risk analysis model can be created. The model is built using the Microsoft Excel and add-on software, Crystal Ball™, which provides capabilities such as assumptions and forecasts definition plus Monte Carlo simulation. Each of the risk assessment tables discussed previously is incorporated into the model and is set to run a Monte Carlo simulation. Crystal Ball provides the capability to run two different types of simulation sampling methods — normal Monte Carlo sampling and Latin Hypercube sampling (LHS). These sampling methods are also used by other risk analysis programs that support Monte Carlo simulation. More details on these two sampling methods can be found in McKay et al [22] and Pebesma and Heuvelink [23]. However, only the results of the normal Monte Carlo simulation are discussed here, as it is not the purpose of the paper to compare the sampling methods, but to demonstrate the results of the risk framework application to business processes. The simulation generates two different sets of results in the form of charts.

- Forecast charts

  These show the range of different results for each forecast and the probability of achieving these results. These are calculated during the simulation based on the effects of the assumptions on the forecast for each activity as well as the whole process. By utilising the forecast charts, one is able to find out the probability of a forecast falling within a particular range.

- Sensitivity charts

  These communicate the influence of each of the model's assumptions on the forecast cells. In other words, the information generated from the sensitivity charts shows whether an assumption has a positive or negative correlation with the forecast. This results in identifying those risk factors with the largest negative effects and concentrating available resources to mitigate the effects where possible.

Figure 4 introduces the forecast and sensitivity charts for the first activity of the business process, i.e. survey. The forecast chart communicates that the most likely cost forecast for the survey activity, with all the risk and their uncertainties involved taken into account, lies around £5707. Note that the initial cost estimate was £5000. The sensitivity chart shows that the 'access to site' risk factor has a very high correlation to the forecast. This means that it is a really important risk factor within this activity and pre-

Table 3 Risk assessment of the analysis activity.

Activity 1 — analysis		Budget = £7500			
		Impact on cost (triangular distribution)			
Risk factors	Probability	Lower limit	Mode	Upper limit	Nominal output (prob × mode)
Expertise	10%	£1200	£3000	£4500	£300
Access to site	5%	£2500	£3050	£5000	£152.5
IT equipment	2%	£500	£2000	£3000	£40
			Total impact on cost		£492.5
			Total budget		£7992.5

Table 4 Risk assessment of the supply activity.

Activity 1 — supply		Budget = £6500			
		Impact on cost (triangular distribution)			
Risk factors	Probability	Lower limit	Mode	Upper limit	Nominal output (prob × mode)
Expertise	15%	£1000	£2500	£5000	£375
Access to site	2%	£500	£1000	£3200	£20
IT equipment	5%	£5000	£7500	£10 000	£375
			Total impact on cost		£770
			Total budget		£7270

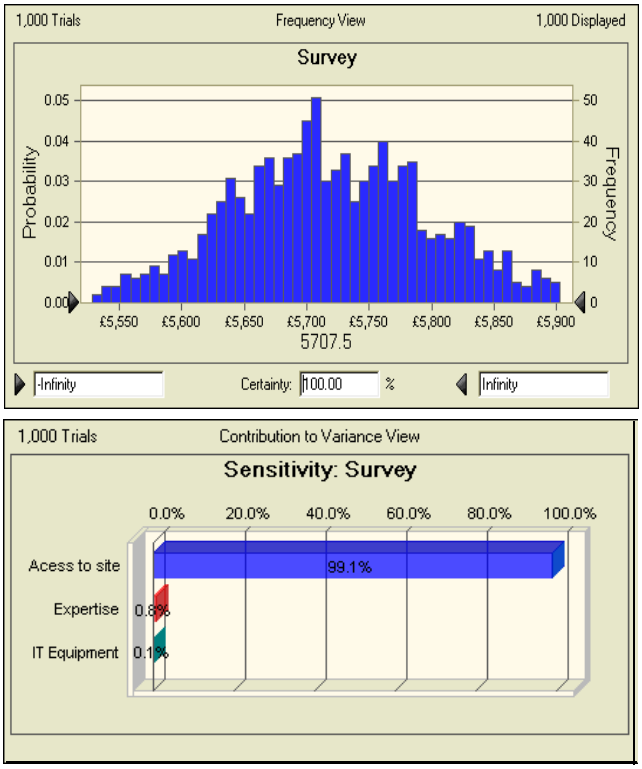

Fig 4 Forecast and sensitivity charts for activity 1 — survey.

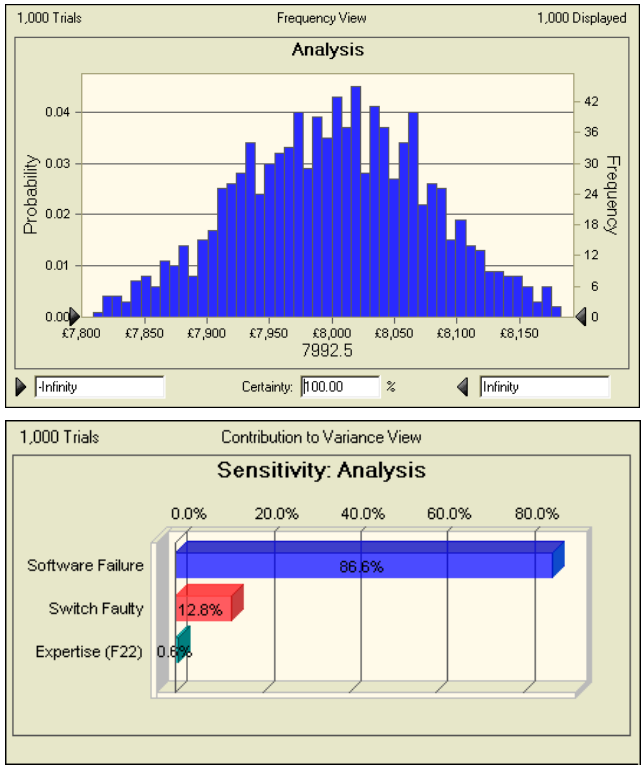

Fig 5 Forecast and sensitivity charts for activity 2 — analysis.

cautions need to be taken to ensure that it will not occur or else it will have a detrimental effect on the cost of survey as part of the network provision process. 'Expertise' and 'IT equipment' risk factors have very low effects such that 'IT equipment' may even be ignored or taken off the risk factor list for this activity.

Figure 5 demonstrates the simulation results for the second activity, i.e. analysis. It can be seen that there is a wide range of values with very close probabilities of occurrence bunched together in the central section of the forecast chart. These lie around the most likely value of around £7992.5 compared to the initial budget of £7500. In terms of unique risk factors, 'software failure' is considered as an important risk factor and cannot be ignored with 86.6% impact on the activity cost. 'Switches faulty' is second with a 12.8% impact and 'expertise' has an insignificant 0.6% impact. This risk factor is likely to be ignored as well.

The results of the last activity of the process, i.e. installation and supply, are presented in Fig 6. Again, around £7270 there is an accumulation of different simulation scenarios with very close outcomes. Note that the initial cost of this activity was £6500. In terms of risk factors, 'server down' is the most influential risk factor within the installation and supply activity of the network provision process with an 87.7% impact on the cost of the process. 'intruder' has 11.4% impact and 'electricity failure' just 1%.

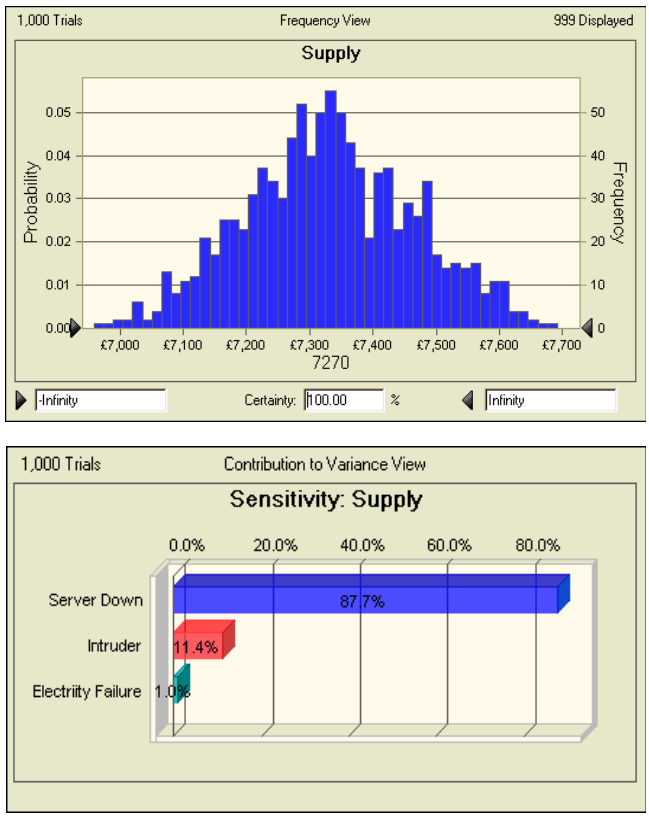

Fig 6 Forecast and sensitivity charts for activity 3 — installation and supply.

Perhaps the most interesting results are shown in Fig 7, which presents the simulation estimations for the complete business process involving all the activities and risk factors. It can be seen here that the forecast chart can be effectively approximated by a triangular function of the type defined earlier in section 4.2. The more likely outcomes are gathered around the estimated process cost of £20 970 compared to the £19 000 initial process budget. The sensitivity chart in Fig 7 contains all the risk factors identified in each activity and demonstrates the effect that each might have on the process cost. By far the most influential risk factor is 'server down' from the installation and supply activity. Influencing the process cost by more than 50%, this risk factor calls for attention and concentration of efforts so that the risk it represents is neutralised. The next three risk factors that can potentially increase significantly the process costs are 'access to site' with cost impact 20.2%, 'software failure' with 15.5% and 'intruder' having 10.3% impact. These also need special attention and care to prevent them from occurring. The remaining risk factors do not have significant contribution in terms of costing the process. However, they

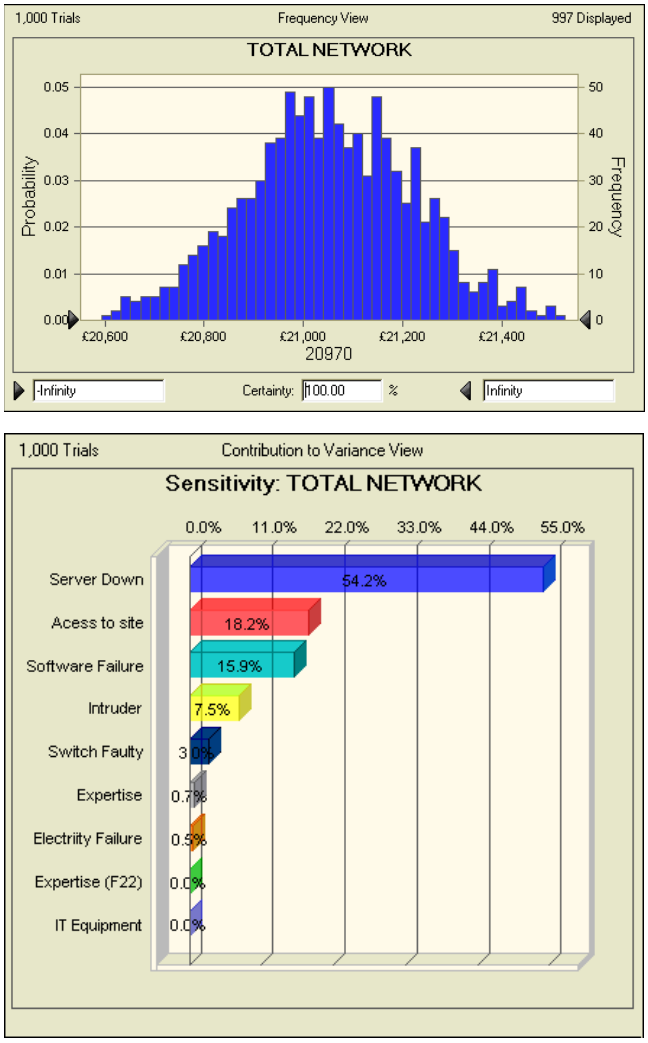

Fig 7 Forecast and sensitivity charts for the network provision process

are identified risk factors for the process activities and they might have a more significant effect on the other two dimensions of the process — either to affect the completion time or quality of output. In any case they also need to be dealt with.

6. Conclusions

This paper has presented a risk assessment framework oriented to business processes. The framework focused on three main factors — cost, time, and performance/quality — from an activity level, in order to quantify risk and acquire a more realistic picture of the complete process. The framework justified that a process needs to be broken down into the different activities that would be required to accomplish the process. Each activity is analysed individually having in mind that any shortcoming has a measurable effect on the complete process.

The framework identified the risk factors for each activity and estimated, based on historical data or expert knowledge, their probability of occurrence and impact, thus providing quantitative information to measure risk. Risk analysis is carried out either for cost, time or performance of the process at any given time. The forecasts generated for each activity and the process provide critical information about the estimated process budget based on different scenarios (i.e. different combinations of risk occurrences) and also identify which are the most influential risks in terms of excess costs.

Simulation of these scenarios helps the business analysts to locate any potential crisis and concentrate their efforts and resources in order to avoid it. The application of the framework is demonstrated using a simple process example of network provision. The activities and their risk factors are identified and analysed, and the results of the forecasts are presented demonstrating which risk factors are the most influential.

In terms of future challenges, more effort is required for analysing risks that are not directly linked to business process activities. Also independent and correlated risks between time, cost and performance need to be taken into account in the framework. The distribution used in the framework (in our case the triangular) needs to be carefully considered and validated by an expert for being the most appropriate in reflecting the risk in a given context.

Associating risk with business processes can prove a crucial advantage when it comes to implementations of Service-Oriented Architectures (SOAs). In such architectures, services are selected from among different implementations to perform certain processes.

Having the capability of selecting the most reliable service in terms of risk makes the SOA far more robust and

competitive than existing structures that evaluate services based on quantitative criteria only. The possibility of building specialised intelligent software for evaluating operational risk among alternative process implementations is a significant step in that direction.

References

1 Archer D: 'Creating a Risk Management Framework. CMA Management,' 76, No 1, pp 16—19 (2002).

2 Knight F H: 'Risk uncertainty and profit', Houghton Mifflin (1921).

3 Frost C, Allen D, Porter J and Bloodworth P: 'Operational risk and resilience: understanding and minimizing operational risk to secure shareholder value', Price Water House Coopers (2001).

4 Bell T, Marrs F, Solomon I and Thomas H: 'Auditing organizations through a strategic-systems lens: the KPMG Business Measurement Process', KPMG Peat Marwick, LLP (1997).

5 Gemmer A: 'Risk Management: Moving Beyond Process', Computer, 30, No 5, pp 33 — 43 (1997).

6 Link P and Marxt C: 'Integration of risk – and chance management in the co-operation process', International Journal of Production Economics, 90, pp 71—78 (2004).

7 Jaafari A: 'Management of Risks, Uncertainties and Opportunities on Projects: Time for a Fundamental Shift', International Journal of Project Management, 19, pp 89—101 (2001).

8 Basel Committee: 'Sound Practices for the Management and Supervision of Operational Risk', Bank for International Settlements, Basel, Switzerland (2003).

9 Crouhy M, Galai D and Mark R: 'Operational risk: Viewpoints of depositors and shareholders', Journal of Derivatives, 12, pp 51—55 (2004).

10 Haimes Y Y: 'Risk Analysis, Systems Analysis and Covey's even Habits', Society for Risk Analysis, 21, pp 217—224 (2001).

11 Suh B and Han I: 'The IS risk analysis based on a business model', Journal of Information and Management, 41, pp 149—158 (2003).

12 Kendrick T: 'Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project', Amacom (2003).

13 Henrion M and Morgan M G: 'A Computer Aid for Policy and Risk Analysis', Risk Analysis, 5, No 3, pp 195—208 (1985).

14 Raz T and Michael E: 'Benchmarking the Use of Project Risk Management Tools', Proceedings of the 30th Annual Project Management Institute, Seminars and Symposium (1999).

15 Duncan R A: 'Guide to the Project Management Body of Knowledge', Project Management Institute (1996).

16 COSO: 'Enterprise Risk Management — Integrated Framework. Executive Summary, 16', Committee of Sponsoring Organizations of the Threadway Commission (2004).

17 Dorofee A J, Walker A. J, Alberts C J, Higuera R P, Murphy R L and Ray C W: 'Continuous Risk Management Guidebook', Carnegie Mellon University, Pittsburgh (1996).

18 Fairly R: 'Risk Management for Software Projects', IEEE Software (1994).

19 NASA: 'Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners', Office of Safety and Mission Assurance, Version 1.1 (2002).

20 Kliem R L: 'Risk Management for Business Process Reengineering Projects', Information Systems Management, 17, pp 71—73 (2000).

21 Zhou Y and Chen Y: 'Project-Oriented Business Process Performance Optimization', in Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, 5, pp 4079—4084 (2003).

22 McKay M D, Backman R J and Conover W J: 'A Comparison of Three Methods for Selecting Values of Input Variables in the Analysis of Output from a Computer Code', Technometrics, 21, No 2, pp 239—245 (1979).

23 Pebesma E J and Heuvelink G B M: 'Latin Hypercube Sampling of Gaussian Random Fields. Technometrics', 41, No 4, pp 303—312 (1999).

Abdou Karim Jallow graduated with an MSc in IT for Product Engineering from the Decision Engineering Centre, School of Applied Sciences, Cranfield University (UK), in September 2006.

He also holds a BSc (Hons) in Information Systems Management from Cranfield University at the Defence College of Management and Technology in Shrivenham (UK). He has strong research interest in intelligent systems, business process modelling, risk analysis and information systems.

Dr Basim Majeed is a Principal Research Professional at the Intelligent Systems Research Centre within BT Research and Venturing at Adastral Park.

He holds a Masters degree (1987) and a PhD degree (1992) in Intelligent Control Systems from the University of Manchester.

He is part of a team working in the area of real-time business intelligence and business process management. He is a Member of the IET and IEEE, and a Chartered Engineer.

Kostas Vergidis is currently a Doctoral Researcher at Cranfield University in the area of Business Process Optimisation.

He holds a BSc in Applied Informatics from the University of Macedonia, Greece, and an MSc in IT for Product Realisation from Cranfield University (UK).

Dr Ashutosh Tiwari is a Lecturer in Decision Engineering at the Manufacturing Department, School of Applied Science, Cranfield University (UK).

He has a stong academic, research and industrial background in applied soft computing, process modelling and re-design, and multi-criteria decision making.

Professor Rajkumar Roy is the Head of the Decision Engineering Centre at Cranfield University (UK).

His major areas of research include applied soft computing and engineering design.

He is the Editor in Chief for Applied Soft Computing published by Elsevier, and is the Chairman of the World Federation on Soft Computing (WFSC) organisation.