Journal of the Operational Research Society (2012) 63, 431–444

www.palgrave-journals.com/jors/

A Bayesian network structure for operational risk modelling in structured finance operations

AD Sanford* and IA Moosa

Monash University, Victoria, Australia

This paper is concerned with the design of a Bayesian network structure that is suitable for operational risk modelling. The model's structure is designed specifically from the perspective of a business unit operational risk manager whose role is to measure, record, predict, communicate, analyse and control operational risk within their unit. The problem domain modelled is a functioning structured finance operations unit within a major Australian bank. The network model design incorporates a number of existing human factor frameworks to account for human error and operational risk events within the domain. The design also supports a modular structure, allowing for the inclusion of many operational loss event types, making it adaptable to different operational risk environments.

Journal of the Operational Research Society (2012) **63,** 431–444. doi:10.1057/jors.2011.7
Published online 11 May 2011

Keywords: banking; Bayesian networks; operational risk; cognitive mapping; artificial intelligence

Introduction

Banks and non-bank financial institutions have become increasingly complex in terms of size and scope, global reach, and product and technological complexity. In addition to their more traditional focus on credit and market risk, these factors have driven the need for financial institutions to become more aware of the operational risks they face. Although severe operational loss events are very rare, such events have demonstrated their potential to bankrupt an organization.

Operational risk is defined by the Basel Committee on Banking Supervision (BCBS) as 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events' (BCBS, 2001). This definition covers legal risk (the risk associated with legal action) but it does not include reputational risk (the risk of loss due to a decline in a firm's reputation) and strategic risk (the risk of loss associated with an improper strategic decision). The BCBS identifies seven types of operational loss events: external fraud; internal fraud; damage to physical assets; clients, products and business practices; business disruption and system failure; execution, delivery and process management; and employment practices and workplace safety. The type of operational risk modelled in this case study falls under 'execution, delivery and process management'.

The use of Bayesian networks in operational risk analysis has been recommended by Alexander (2000, 2003), Mittnik and Starobinskaya (2007) and Moosa (2008), as a tool for measuring and managing operational risk in financial institutions. The inherent heterogeneity and limited availability of operational loss event data makes the modelling of operational risk more problematic than that of credit risk and market risk. Both of these risk categories are more amenable to statistical analysis because of the availability of large sets of comparatively homogenous historical data. Operational risk modelling, on the other hand, requires the augmentation of the sparse historical data with human judgement and expert opinion. Similarly, human judgement and expert opinion plays a critical role in the design and verification of the network structure developed in this study.

Literature review

Although new to the banking and finance industry, it could be argued that modelling operational risk using probabilistic network models, such as Bayesian networks, has been around for quite some time. Similar models have been developed in other industrial settings, often under the label 'probabilistic risk analysis' (PRA) (Bedford and Cooke, 2001). This form of analysis, which has evolved out of engineering-based practice, has until recently been more commonly applied to industrial situations in nuclear energy, aerospace and chemical processing, rather than to

*Correspondence: AD Sanford, Faculty of Business and Economics, Department of Accounting and Finance, Monash University, Clayton, Victoria 3800, Australia.
E-mail: Andrew.Sanford@Buseco.monash.edu.au

commercial situations. Paté-Cornell and Dillon (2006) define PRA as a 'combination of systems analysis and probabilistic elicitations tools'. The typical common tools used in PRA for causal analysis are fault and event trees, which provide causal descriptions of operational loss events. Although Bayesian network tools have been applied to PRA analysis in industry, it is our view that the methodology is particularly well suited to operational risk modelling in financial institutions and markets. While the logic-based fault and event trees models are more suited to modelling the 'hard' physical and technical environments found in industry, Bayesian networks can be used to model the 'conceptual' and 'subjective' environments found within the softer commercial context.

Modern financial and commercial activities are highly dependent on human and systems reliability, as well as human-to-human and human-to-computer interfaces. Bayesian networks are particularly suited to modelling these areas, since they make it possible to fuse disparate and diverse historical and subjective data. For this reason, Bayesian networks may prove to be a better modelling tool for the commercial environment than the more logic-based fault and event trees. A number of authors have demonstrated that Bayesian networks actually subsume fault and event tree models, making the Bayesian network, an extension of these popular analytical tools (see Bobbio *et al*, 2001; Marquez *et al*, 2010).

The technology that makes Bayesian network tools possible has been available for 20 years (Pearl, 1988; Neapolitan, 1990). A rather diverse range of literature exists that describes the application of Bayesian networks to a multitude of domains. A short, but by no means exhaustive, list of published applications covers transportation (Trucco *et al*, 2008), systems dependability (Sigurdsson *et al*, 2001; Neil *et al*, 2008), infrastructure (Willems *et al*, 2005), medical and health-care provision (van der Gaag *et al*, 2002; Cornalba, 2009), environmental modelling (Bromley *et al*, 2005; Uusitalo, 2007), legal/evidential reasoning (Kadane and Schum, 1996), forensic science (Taroni *et al*, 2006), venture capital decision making (Kemmerer *et al*, 2001), project management (Khodakarami *et al*, 2007), customer service delivery (Anderson *et al*, 2004), new product development (Cooper, 2000), traffic accident modelling (Davis, 2003), and national security and terrorist threats (Paté-Cornell and Guikema, 2002). A common underlying theme of many of these studies is the development of models to facilitate reasoning and decision making under uncertainty.

Papers addressing the issue of operational risk modelling within the finance industry using Bayesian networks are limited, with a relatively short history. These include Neil *et al* (2005), Mittnik and Starobinskaya (2007), Adusei-Poku *et al* (2007), Cowell *et al* (2007), and Neil *et al* (2009). None of these papers, with the exception of Adusei-Poku *et al* (2007), base their models on real-world banking environments.

Neil *et al* (2005) describe the use of a Bayesian network to model statistical loss distributions for operational risk in financial institutions. Their emphasis is on what they describe as the core problem of predicting losses. They describe Bayesian networks as providing further support for self-assessment oriented scorecards. Bayesian networks, as suggested by Neil *et al* (2005), provide (i) the ability to combine proactive loss indicators with reactive outcome measures, including loss and near-miss events; (ii) the means to incorporate expert judgment and qualitative estimates; (iii) graphical representation, documentation and inference over incomplete observations; and (iv) predictive and verifiable outputs. They produce a model using the loss distribution approach (LDA), whereby total operational losses are modelled by combining event frequencies and severities. From the total loss distribution, expected and unexpected losses, as defined under Basel II, can be determined. They also introduce, as parent nodes of frequency and severity, a process effectiveness node, which also has parents that represent operational quality, technological fidelity and staff quality. The introduction of these risk drivers represents a movement away from using these models just for the purpose of capital allocation, to the management of the causes of operational risk.

Adusei-Poku *et al* (2007) develop a Bayesian network model of operational risk in an operational foreign exchange transactions (FX) settlement domain. With a similar objective to our own, Adusei-Poku *et al* are concerned with developing an operational risk management tool rather than a model for determining economic capital allocation. They begin by describing the process of FX settlement and identifying the entailed sub-processes. They define each operational loss event in the FX settlement process, which include delayed payments, incorrect payments, misdirected payments, non-payments and duplicate payments. The model they develop is based also on the approach to operational risk whereby the frequency of operational loss events is modelled separately from the severity of events (as previously described in Neil *et al*, 2005). The final operational loss distribution is generated as a convolution of the two. The entire parameterization of the model is based on domain expert elicitations, carried out using formal methods. Despite the availability of historical data, it appears that Adusei-Poku *et al* (2007) took no opportunity to use any model learning features of the Bayesian network tool. Although the FX settlement environment appears similar to the one examined in this paper, it differs in that it involves a more homogenous set of transaction types and processes, which allows more of these processes to be automated. This results in less reliance on '*ad hoc*' human processing arrangements and the subsequent exposure to human

error. Having said this however, the types of causal errors sound remarkably similar to the analysis in our own research. Adusei-Poku *et al* (2007) identify causes of settlement failures to be the quality of settlement information and payment input method, which although not identical, have similar features to the cause we identify, such as data integrity and transaction implementation errors.

Cowell *et al* (2007) provide a comprehensive discussion of two fictional applications of Bayesian networks. The first application involves modelling operational loss events that are associated with computer system failures of an e-business, while the second application deals with fraudulent claims in the insurance business. Cowell *et al* (2007) demonstrate how Bayesian networks can be used to (i) form posterior probabilities of events, given observations on other states of the domain; (ii) simulate different scenarios for each business line; (iii) adapt or learn new probabilities for events; and (iv) quantify the predictive performance of each model. Cowell *et al* (2007) note that a drawback of Bayesian networks as a modelling tool is that they may require considerable initial resources to set up. They also note that although a strength of Bayesian networks is its subjective nature, this attribute is also a weakness that curbs the tendency of prudential supervisors to accept them for the purpose of measuring risk capital allocations. We particularly agree with the second view, and this is why our model is centred on the need for institutions to manage their operational risk profile internally.

Mittnik and Starobinskaya (2007) consider Bayesian networks as a solution for the advanced measurement approach of Basel II. Their concern is that the standard methods of modelling stochastic dependencies are insufficient for assessing operational risk. In conventional models, correlations and copulas are used to measure relations between business lines and risk events, but they do not include measures of causal relations between these entities. Mittnik and Starobinskaya (2007) also follow the LDA specified under Basel II, modelling the frequency and severity of operational loss events separately. They argue that ignoring topological aspects of the domain, as regards the interconnection of work-processes and information flows, means that standard models do not account adequately for multiple, simultaneous failures. Applying Monte Carlo simulation, they demonstrate that at different degrees of dependency, the topological interconnections between business lines result in an avalanche-like effect, or clustering of events.

Neil *et al* (2009) develop a hybrid dynamic Bayesian network for the modelling of operational losses faced by financial institutions for the purposes of economic capital allocation. They claim that applications of Bayesian networks have failed to address three fundamental problems: (i) applications deal only with small fragments of a much more complex banking environment; (ii) models do not incorporate the time dynamics of operational loss events; and (iii) implementation of continuous variables. As in Neil *et al* (2005), they create a model involving three layers, one representing operational loss events, another for operational risk impact and a third for the aggregation of losses. It is a hybrid model, containing both discrete and continuous nodes. Interactions between failure modes and controls are modelled to generate an approximate continuous loss distribution using an algorithm that they call 'dynamic discretization'. This algorithm determines the discretization of continuous nodes automatically, a procedure that has the benefit of avoiding the trial-and-error approach that modellers follow to select manually the appropriate discretization ranges, which may change as distributions in the environment change.

Bayesian networks

A detailed presentation of the Bayesian network technology seems unnecessary, given the large number of very good references currently available (for example, Korb and Nicholson, 2004; Neapolitan, 2004; Jensen and Nielsen, 2007; Koller and Friedman, 2009).[1] Therefore, we provide only a brief description of the technology as a background for the remainder of the paper. For a more comprehensive discussion of Bayesian networks, as they relate to operational risk modelling, refer to Cowell *et al* (2007).

A Bayesian network consists of nodes and directional arcs or arrows. In earlier forms of the Bayesian network technology, in order to use efficient inferential algorithms, each node was restricted to being either discrete, having at least two states, or continuous, having a Gaussian distribution over the real line. To work around such restriction, Bayesian network developers have had to use static discretized nodes over the ranges of non-Gaussian distributed nodes. Alternatively, to avoid these distributional restrictions, slower, less efficient inferential algorithms, such as simulation-based methods, have been used. Such distributional constraints have until recently restricted the application of Bayesian networks in modelling real-world environments. Fortunately, techniques for creating efficient hybrid Bayesian networks, consisting of both discrete and continuous nodes have now been developed. Inferential efficiency in hybrid Bayesian networks has been achieved by the development of dynamic discretization techniques, which allow the inclusion of a wide variety of continuous distributions as discrete form approximations. Approximating continuous nodes in this manner, using dynamic discretization means that the fast

[1]The Bayesian network technology has been in existence for 20 years, and so a large number of tools, in both a commercial and research-based form, are now available for research, development and applications. The tool used for this research was Hugin Researcher version 7.0.

and efficient inferential algorithms can still be employed for probability propagation. A description of hybrid Bayesian networks and the dynamic discretization technique can be found in Neil *et al* (2007).

Within the Bayesian network, each node represents some variable of interest within the domain to be modelled. Behind each node is a function that represents the probability distribution of the states of that node. That function is often represented as a table, which is called the conditional probability table (CPT) or node probability table. Given the semantics of the nodes and states, we see that in modelling an environment, the modeller must decide on what variables are of interest to the user or decision maker. They must also decide on what measures are used to determine the state of these variables and what state descriptors provide the most value to the user or decision maker. In determining the number of states for a discrete node, the modeller should be aware that increasing the states improves the granularity of the measure, but makes probability elicitation potentially more complex. Therefore, a trade-off between the number of states and the additional complexity needs to be considered when developing the network.

More contentious is the meaning of the directed arcs within a Bayesian network model. It is usually the case, however, that the arrows and their direction encode a concept of 'influence' or 'cause' within the domain. An arrow extending from node X to node Y indicates that a change in, or manipulation of, the state of node X will cause changes in the state of node Y. In this paper, we take the firm view that the arrow directions are causal.

Architecturally, although Bayesian networks can take on an arbitrary level of complexity, all models consist of three basic structures. These are the serial, convergent or divergent structures, as illustrated in Figure 1. Although networks can be constructed in such a way as to show that all nodes are connected to each other, Bayesian networks are more suitable as a modelling tool in situations where connections between nodes are sparse rather than saturated.

Once the nodes and causal relations are identified, and the Bayesian network constructed, the state probabilities can be elicited and incorporated into each node's CPT.

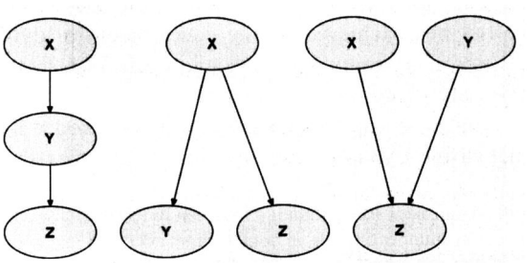

Figure 1 Serial, divergent and convergent network structures.

These state probabilities can be elicited from human experts, statistical analysis of historical data or, in some situations, learned directly by the Bayesian network.

After state probabilities have been included, the network can be queried by the user. In querying the network, information or evidence on the state of the domain is usually entered. This evidence is propagated throughout the network, allowing the marginal distributions of unobserved states within the environment to be determined, based on the assumptions encoded in the model. Before any evidence is entered, a node X displays its *a priori* marginal distribution, $Pr(X)$. After evidence ε has been entered into the network, the unobserved nodes such as X, will display their *a posteriori* distribution, $Pr(X|\varepsilon)$.

The process of propagating evidence through the network in order to evaluate the prior marginal and posterior distributions of nodes is referred to as inference. Inference can be readily performed by generating the joint probability distribution encoded within the network, and then summing out all nodes other than the node of interest. The problem with this approach is that it leads to an exponential growth in the inference task. It has long been recognized, that under worst-case conditions, inference in Bayesian networks is *NP-Hard,* for both exact and approximate inference. Despite this being the case, a large number of algorithms have been developed that, by taking advantage of the probability structures encoded within the network, achieve efficient probability propagations. The following discussion relates to one of the more popular exact propagation methods, known as Junction Tree propagation.

The Junction Tree propagation method involves the manipulation of functions, referred to as potentials. In the case of Bayesian networks, these potentials represent the CPTs associated with each of the nodes. It is through manipulating these potentials that the marginal probability for each node in the network is calculated. In the Junction Tree method, marginal probabilities are calculated by the process of variable elimination, where probabilities are summed over the domains of the nodes using the information stored in the CPTs. Inferential efficiency is achieved by the identification of an optimal elimination sequence that eliminates variables in the most memory-efficient manner and delays the multiplication of potentials until absolutely required. This optimal schedule is achieved by manipulating the original Bayesian network into a Junction Tree structure. The Junction Tree is a tree data structure consisting of clusters that comprise sets of node potentials from the original Bayesian network. Each cluster within the Junction Tree has only a single parent cluster, and is joined to its adjacent clusters by an undirected link. The set intersection between each adjacent cluster is a non-empty set, known as the sepset, which contains slots known as mailboxes, used for message passing up and down the tree. These messages represent the summed potentials from

adjacent clusters. The propagation calculations take place over the generated Junction Tree, allowing efficient summing and product calculations to generate the marginal probabilities. For a more detailed discussion of the Junction Tree propagation method, and other exact and approximate propagation algorithms, refer to Koller and Friedman (2009).

An advantage of using Bayesian networks as a modelling tool is that they can provide answers for both predictive and diagnostic queries. For example, a predictive query would be 'what is the probability of a payment failure, given that a loan is being processed?', while a diagnostic query would be 'what is the most probable transaction type processed given that a payment failure occurred?' Having observed the state of an effect node, such as a payment failure, inference can be carried out to show the probable states of the causal nodes within the network.

Structured finance operations (SFOs)

The institution that participated in this research is one of Australia's largest banks. Included within the group is the bank's wholesale banking division, which itself also includes two business units: the Structured Finance and the Corporate Finance units. It is the responsibility of these two units to develop and market structured finance products to the bank's wholesale corporate customers. Structured products are created by bundling individual transaction products together to provide a tailored financial solution to meet an individual client's needs. The different individual products that may be included within a structured product can range from simple vanilla loans and deposits, to the more complex risk management tools such as over-the-counter options and credit derivatives. These structured products may have overall terms lasting as little as 2 weeks to as long as 5 years. They may be comprised of only a few individual cash flows involving only a single currency, or a large number of flows involving different currencies, values and timings. These structured products may also involve the establishment of alternative legal structures, or special purpose vehicles (SPVs), which are necessary to make the transactions tax-effective. To manage these complex transactions during the life of each structured product, a separate business unit has been established within the wholesale banking division. This unit, known as SFO, is responsible for the successful implementation of each structured product.

The management and staffing of SFO consists of a single director, who has overall responsibility for the leadership of SFO, its budget, workflow and personnel. A number of associate directors, reporting directly to the director, are responsible for the day-to-day management of SFO deal teams. They also have direct responsibility for individual deals of a highly complex nature. Below them are the associates, or line managers, who take responsibility for a number of outstanding individual deals and direct the analysts, who are junior staff within the deal team. It is the analysts who perform most of the activities related to individual transactions. Given the diversity of transaction types within the domain, SFO operators tend to be generalists rather than specialists. For this reason, it may be difficult to replace staff once they move on to other areas of the bank. This creates further potential risks brought about by staff turnover, inadequacy of training and the level of task instruction necessary.

Given the heterogeneity of the different transaction types making up a structured product, it is difficult to develop a process-based model to manage them. Instead, the SFO implements a 'deal team' or jobbing arrangement. Such a structure provides the flexibility to implement the actions necessary to support these products. This flexibility is not costless however, with the potential for more frequent operational loss events resulting from human error. Furthermore, much of the bank's existing automated legacy systems lack the specific functionality needed to support these unique products. Therefore, greater reliance on both manual and spreadsheet-based solutions has resulted, more so than in a homogenous transaction environment.

In the process of creating a new structured product for a client, the Structured Finance and Corporate Finance units produce a physical document known as the 'deal document'. Within this document, all details (such as transaction types, cash flows, timings, currencies and legal structures) are specified and described. The deal document is the 'blue print' that specifies the structured product from the initial setup to termination. It is the deal document that is passed on to SFO, and it is the deal document on which the SFO staff relies to guide them through each transaction. Given the potential complexities and risks involved in structured products, considerable due diligence is carried out in the authoring of this document. To ensure that errors are removed, the document passes through a large number of oversight hurdles prior to its release to SFO.

From an operational risk perspective, and as defined under Basel II, SFO exposes the bank to 'execution, delivery and process management' risk. SFO has identified its major operational risks as:

- Payments made to incorrect beneficiaries, and/or for an incorrect amount, and/or for an incorrect value date.
- Regulatory breach such as regulatory reporting or account segregation.
- Failure to enforce its rights or meet its obligations to counterparties over the life of a deal.
- Exposure capture. This is the risk that the terms of a transaction or details of a counterparty/security are not recorded accurately in the Bank's systems, resulting in a misunderstanding of the risk profile.

Other risks identified by SFO include: (i) approval compliance (the risk that transactions are undertaken without the necessary internal approval process); (ii) documentation (the risk that documentation does not adequately protect the Bank's rights because of incorrect execution or incorrect drafting); and (iii) theft (the risk that the Bank's or customers' funds or property are misappropriated).

As part of the existing operational risk oversight and assessment of SFO, business environment scorecards are prepared regularly to identify generic key risk drivers (KRDs) common to all units within the wholesale banking division and score individual units against each dimension. Generic risk drivers include: (i) whether the unit is large and distributed or small and centralized (scale measure); (ii) whether transactions processed within the unit are of a large wholesale dollar amounts, or low retail dollar values (transaction measure); (iii) whether the products are complex and large in volume or simple and low in volume (product measure); (iv) whether the operational processes within the unit are complex, manual and outsourced, or simple, automated and carried out in-house (process measure); (v) whether the units operational and systems technology is legacy, disparate and with multiple interfaces, or is modern, integrated and with fewer interfaces (technology measure); (vi) whether unit staff are incentive driven, with high turnover, or wage and salary remunerated with low turnover (staff measure); (vii) whether the unit is undergoing rapid, large scale and complex change, or slow, small scale and simple change (change measure); (viii) whether the unit is experiencing new aggressive and competitive entrants, or competition is benign and stable (competition measure); (ix) whether the unit operates in a tight regulatory environment, with multiple legal entities and global reach, or a loose regulatory environment, with few legal entities and a local or national focus (regulatory/legal/geographic measures). For each unit, the operational risk drivers are assigned a number ranging from 1 (highest risk) to 9 (lowest risk). Although scorecards are a popular and valuable tool, they—unlike Bayesian networks—do not make explicit the causal relations between various risk drivers.

The SFO senior management views the Bayesian network model as offering a number of practical features. First, risk communications within and across business units can be improved, as the model makes explicit the risk drivers and their causal relations. Furthermore, auditable justifications for risk decisions can be made explicit and accessible to external parties. For example, the model could be used to support the bank's internal audit team in assessing the risk profile of SFO. The model also provides supporting evidence for management decisions on reducing and mitigating potential operational risks within the business unit. Although the model presented in this paper does not incorporate decision nodes, the Bayesian network technology allows for the inclusion of decision and utility nodes, which may be added in future versions of the model.

Methodology

While efficient algorithms for inference in Bayesian networks have been available for some time, construction and development of these networks is still as much an art as it is a science. In modelling a problem domain, the developer must use their judgement in determining what level of detail is appropriate, which nodes should be included, and what causal relations may exist. Supporting these choices is the ultimate purpose of the model. As a simple modelling rule, the choices made have been informed by our desire to provide potential users with gainful insights of the domain, while at the same time avoiding the creation of a model whose complexity makes future use cumbersome, and is difficult to maintain and improve. Pragmatically, the rule is 'simple enough to be used and complex enough to be useful'. The development approach is taken from the knowledge elicitation methodology discussed in Korb and Nicholson (2004). This methodology emphasizes the use of domain experts in the construction and elicitation phases, with iterative feedback and re-modelling being an important feature.

Reliance on human expert judgement in the construction and elicitation phases presents a number of difficulties. These include such situations in which the available domain experts do not have sufficient knowledge scope to cover all facets of the domain, or where domain experts have difficulty specifying the correct causal ordering of events, or where problems associated with the combination of probabilities provided by all of the individual experts arise. A potential remedy for such difficulties is the use of automated machine learning techniques, which have been an active area of Bayesian network research, motivated particularly by the desire to overcome the bottleneck associated with using expert judgement. Many Bayesian network tools incorporate such machine learning algorithms, including the tool used in this paper. Given the lack of available hard observational data, the use of domain expert input appears unavoidable here. More generally, this may always be somewhat true, given the very nature of operational risk. Despite these difficulties, it is our view that, with respect to operational risk management, the involvement of domain expert judgement is highly desirable. Incorporation of expert knowledge is therefore a strength of Bayesian network modelling, but it is also a weakness because of the difficulties expert elicitation presents.

The Bayesian network construction process is iterative, proceeding in steps and cycles. The following

development steps are taken from Korb and Nicholson (2004):

1. *Structural development and evaluation*: initial development proceeds by identifying all of the relevant risk driver events, their causal relations, and the query, hypothesis or operational loss event variables. This produces a causal network without any elicited or learned probability parameters. Evaluating the network at this step requires an analysis of the dependencies of nodes, as encoded within the network design, to ensure that such dependencies conform to the judgements of the domain experts. A cross-validation or clarity test can also be performed to ensure that the variables included within the design are deemed to be comprehensive, relevant and unambiguous, by domain experts not previously involved with the network design.
2. *Probability elicitation and parameter estimation*: this step involves defining the probability distributions of the nodes and setting their parameter values. Parameter values must be set such that they reflect the marginal and conditional probabilities observed in the domain. These marginal and conditional distributions can be determined by reference to domain-based experimental results, passive observation of events, learning from historical data or access to domain experts. For our purposes, the last source dominates.
3. *Model validation*: this step is probably the most problematic component of Bayesian network construction, especially when historical data is sparse. How does one validate a model constructed largely through the subjective opinion of experts? Korb and Nicholson (2004) suggest a number of validations approaches, including (i) an elicitation review; (ii) sensitivity analysis; and (iii) case evaluation. We use the first two approaches for the validation of the model.

In this paper, we are only concerned with the first stage of the development cycle, structural development and evaluation. Sanford and Moosa (2009) discuss stages two and three.

Structure development

In the process of constructing the network model, we sought to answer the following broad-based questions:

1. What operational risk queries should the model be able to answer?
2. What operational risk categories and events should be included in the model?
3. What are the main risk drivers in SFO for operational risk events?
4. What are the causal relations between risk drivers and risk events?
5. What are the key performance indicators (KPIs) for the SFO domain?

Acquiring answers to these questions initially proceeded through a review of SFO's internal documentation to gain an appreciation of the business and operational environment. The existing operational risk documents pertaining to SFO, provided by senior operational risk staff, were of particular value. Included within this material were the most recent business environment score ratings for SFO. These scorecard assessments proved invaluable in providing an overview of the unit's operational risk profile. SFO's ratings were: scale (8), transactions (2), product (2), process (2), technology (4), people (8), change (4), competition (8), and regulatory/legal/geography (7). Obviously, transactions, products and processes, as well as technology and change, present the greatest challenges to SFO. It has low transaction volumes but with relatively high dollar values. Its products are relatively complex while its processes rely on human performance and manual intervention. It also faces a business environment that is dynamic and changing due to business growth. Existing internal documentation also revealed that the KPI used by SFO senior management was the number of transactions process per month.

Following on from the document reviews, a number of face-to-face unstructured and semi-structured interviews were carried out with the Director of Quality Assurance for SFO. For future reference, we refer to this domain expert as the 'risk manager' who has over 20 years of banking experience, and was responsible for the monitoring of SFO's operational risk events. For this reason, they had considerable interest in the project and the development of the Bayesian network tool, as it directly impacts their own responsibilities. The risk manager has considerable detailed knowledge of the SFO domain and was very familiar with the operational processes involved, potential loss events and their drivers. They do not, however, have any experience in Bayesian networks as a decision support or risk management tool.

Taking a user's perspective, the risk manager saw the model as providing probability outputs for various operational loss events, conditional on the underlying characteristics of each type of transaction performed within SFO. It was the risk manager's view that SFO management required a more formal method of assigning operational risk capital allocations for each transaction. The current methods for doing this are somewhat *ad hoc*, opaque and reliant on the judgement of senior management. By introducing the Bayesian model, a more formal and transparent decision-making approach would be available, based on hard evidence, as well as professional judgement. The model would, at the very least, make the cognitive causal models used implicitly by SFO staff

accessible to internal and external parties. The network model would also be useful as a baseline negotiating position in discussions between SFO and any of the other transaction originating business units.

During these interviews, several candidates were discussed as potential output categories. The most important risk events to be included in the model, referred to as the key risk indicators (KRI), were identified as payment failures, exposure management failures and regulatory/legal/tax failures. Payment failures include any event related to a failed payment such as a payment delay caused by an incorrect counterparty, incorrect value date, or incorrect payment amount. Exposure management failures refer to situations in which the bank's financial positions or risk exposures are incorrectly recorded. Regulatory/legal/tax failures are related to errors that result in the bank failing to meet its regulatory, legal or tax requirements as they impact on prudential supervision, legal requirements from both the bank's and the clients' perspectives, or with respect to the tax effectiveness of transactions such as account segregation.

To manage and control operational risk, an understanding of the causal antecedents is a key first step. In the operational risk literature, these causes are often referred to as KRDs. The KRDs identified during the initial and subsequent interviews include (i) the transaction type; (ii) the data capture mode or mechanism (whether manual/spreadsheet or bank legacy system) for recording transaction information; (iii) existence of SPVs; (iv) the actively managed transaction volume currently handled by SFO's staff; (v) the skills (or quality) of existing SFO staff; (vi) the availability of SFO staff; (vii) the accuracy of transaction information capture; (viii) the correctness of transaction implementation; and (ix) the existing oversight controls currently performed by SFO staff. Subsequent interviews led to the addition as risk drivers of (x) the failure or downtime of computer systems; and (xi) the work environment. Validation of the initial network design was carried out using a structured walk-through by a senior operational risk analyst. During the model walk-through, the operational risk analyst was able to confirm the existing nodes and the proposed causal relations, while making a number of valuable suggestions as to the inclusion of other nodes. These additional inclusions emphasized legal and taxation issues. The proposed additions were later discussed, confirmed and approved by the risk manager for inclusion in the model.

The transaction type driver includes not only the transaction type itself, but more broadly the implicit transaction processing involved in actioning that transaction type. Transaction types processed by SFO include loans (LN), deposits (DEP), foreign exchange transactions (FX), interest rate swaps (IRS), cross-currency interest rate swaps (XCS), exchange-traded derivatives (ETD), over-the-counter options (OOP), over-the-counter credit derivatives (OCD), listed equities (EQL), unlisted equities (EQU), preference shares (EQP), financial leases (FNL), and operating leases (OPL). Each of these represents a separate transaction type within the model. Each instrument may consist of one or more separate payment flows between counterparties, an acquisition or removal of a financial position, or the creation or closure of an SPV. Each may be denominated in a number of different currencies, involving a variety of actions, which may be common to many or unique to only a few. The idea of transaction type being a driver of risk represents an attempt to capture the different operational risks inherent in each transaction process or the task variation.

The data capture mode driver refers to the manner in which transaction information is captured and stored, which has implications for the risk profile of any one transaction. This driver is closely associated with the existence, or otherwise, of an SPV that pertains to the transaction being processed. Transactions processed with an associated SPV are more likely to have their data capture performed using manual and spreadsheet-based solutions (than via the bank's existing information system infrastructure) with its attendant automated features, error and reconciliation controls. This is because the use of SPVs can make a transaction more complex, requiring processing that is unique for that transaction.

Furthermore, transaction-based characteristic risk drivers also include the transaction size or principal value, and the payment or cash flow sizes associated with that transaction. These characteristics have particular influence on the impact of an operational loss event, as potential losses can be closely linked to these variables. Taken together, transaction type, data capture mode, SPV, transaction size and payment size constitute what we broadly categorize as the transaction characteristics that drive operational risk events.

The next set of drivers, actively managed transaction volumes, and quality and quantity of operational staff, which we broadly classify as 'skills and experience', are meant to capture the important states of SFO's working environment. Actively managed transaction volumes provide a proxy measure to the KPI used in SFO, the number of transactions processed. By including the actively managed transaction volumes within the model, we also gain some measure of the demands of the working environment on operational staff. It is the interaction of external factors, as found in the social-working environment and the technical environment, which drives the internal psychological states of the SFO operators. We consider the internal and external states of the operational staff to be of particular importance in driving operational loss events, because of SFO's reliance on the human factor.

In an attempt to capture the internal states of the operational staff, as they interact with their contextual working and technical task environments, we include

within the model a number of nodes that represent three important internal states of the working operational staff. These categories (stress load, mental effort load and time load) are taken directly from the Subjective Workload Assessment Technique (SWAT), originally developed by Reid and Nygren (1988). We do not utilize the SWAT in its entirety, but rather borrow its operator load categories only. This framework introduces the measures, each of which has discrete, three-tiered states. Each state is provided with a description, which assists the operator in determining the level of time, mental effort and stress load they experience, while performing a given task. The SWAT is a particularly popular framework, providing good face validity for an operator's internal state. By implication, it is the combination of these three individual states that induce an overall workload state. For our purposes, the workload state is determined by a simple summation of the individual states.

Further to SFO's reliance on human factors, we include into the network model another set of nodes for the purpose of capturing, under a more formal categorization, the different types of human errors that may generate or potentially generate operational loss events. These nodes, and the human error categories they represent, are taken from Reason's (1990) generic framework for human error categories. These categories are mistakes, slips, lapses and mode errors. All human errors can be placed under one of these categories. Our reasoning for including these categories is to support SFO's efforts to learn more about their working and operational environment over time. Using a formal categorization of human errors may assist SFO to develop a greater awareness of what type of errors occur and how, particularly as staff interact with the task environment. Categorizing errors helps raise awareness of the different forms and their attributes, improving communications and situation awareness. These categories are quite generic, but specific SFO categories, or other human error categories, could also be developed. For example, a more detailed framework related to spreadsheet error taxonomies, which is described in Powell *et al* (2008, 2009), could be incorporated into the network, with the human error categories divided between spreadsheet-based and non-spreadsheet-based errors. Furthermore, other error categories could be included, such as the commonly used 'errors of commission', which constitute errors occurring due to actions that should not have been taken, and 'errors of omission', which involve errors arising from not performing actions that should be performed.

Although the incorporation of Reason's generic framework and the SWAT frameworks improves the analytical features of the network model, it does come at some small cost. It makes expert elicitation more difficult, as it is unlikely that local experts within SFO have ever given any consideration to these types of categories or view their environment in these terms. They are likely to be unfamiliar with these human error categories or operator loadings, even though they will be called upon to provide *a priori* probabilities. In introducing these node categories, it is important that the local experts are given sufficient instructions to understand them and support in deriving prior probabilities for them.

To provide further categorization to error outcomes, we have also introduced 'error types' that are more specific to SFO, but which could also be relevant in other back office and operational environments. These errors types are: (i) system errors; (ii) data integrity errors; (iii) transaction implementation errors; and (iv) oversight control errors. At this point, we make a distinction between these categories of errors, as they impact on SFO and its operational loss profile. Error types that are considered to be under the control of SFO, and which have their origins within SFO, are considered to be endogenous errors. Alternatively, those error types that are not under the control of SFO, and have their origin in some business unit or entity external to SFO, are considered to be exogenous errors. The only one of these four error types that we consider to be exogenous is system errors, which are associated with the failure of the information and communications technology (ICT) infrastructure on which SFO rely. These system errors may be due to loss of power, software or hardware failure, a malicious computer virus or denial of service attack, to name just a few. Control of such risks is the responsibility of the bank's IT department. We consider system errors as defined here to be beyond SFOs control, but are still included as they have the potential to cause operational loss events that impact on SFO operations. Because of the exogenous nature of this risk, it has no KRDs associated with it as parent nodes. It is included, however, to cover those operational loss events that may originate from an ICT system failure. Although it is not included in our existing model, deal document errors form another exogenous error type, similar to systems error.

The causal relations between the generic human error nodes and error type nodes was originally designed as direct causes, as described in the left-most diagram of Figure 2. Such a structure places considerable cognitive

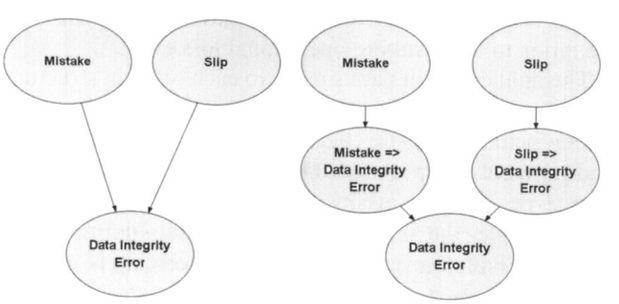

Figure 2 Divorcing parent nodes from child nodes.

load on the local experts who must provide the prior probabilities. How does one distinguish the probability of a data integrity error given a [Mistake = *true*, Slip = *false*, Lapse = *true*, and Mode error = *false*] *versus* [Mistake = *false*, Slip = *true*, Lapse = *false* and Mode error = *true*]? To alleviate this problem, the technique known as 'divorcing' is used to reduce the complexity of probability elicitation or the learning (estimation) of probabilities. Divorcing involves separating a large number of parent nodes from their child nodes by introducing intermediate nodes. Divorcing is carried out to assist domain experts in their elicitations and improve the estimation or adaption of parameters through direct learning of observed data. The human error categories are divorced from the error type nodes by introducing intermediate causal nodes, as shown in the right-most diagram of Figure 2. The error type node 'Data Integrity Error' is evaluated deterministically by an 'OR' function. Provided that any of the intermediate nodes are true, the error type node 'Data Integrity Error' will also be true, otherwise it will be false. By introducing the intermediate causal nodes such as Mistake => Data Integrity Error (the symbol => implies causation), the elicitation for domain experts is made somewhat easier. Domain experts may now only consider the situations in which a mistake results in a data integrity error. Divorcing also aids parameter estimation by adaption, as the data set is more likely to contain sufficient counts of parent node configurations to allow learning.

An observer of Figure 2 may take issue with how it purports to represent the relationships between the various human error events. One may argue that each of these human error events are mutually exclusive, and therefore human error events could be represented as a single node, having the five states of 'Mistake', 'Slip', 'Lapse', 'Mode error' or 'No Human error'. This would be true if we were interested in capturing the existing states of the environmental, staff and task variables each time a particular human error state was observed. As the model stands, however, the real concern is to capture the states for the environmental, staff and task variables when an operational loss or near miss event occurs. As such it is quite possible that in investigating an operational loss event, the operational risk manager identifies several different human error events taking place, at different stages in the transaction leg, prior to the resulting operational loss event.

The final categories are similar to each other in structure and represent the categories of operational loss events. These include regulatory/legal/tax, exposure management and payment failure events. Divorcing is also used between error types and loss events, producing intermediate nodes (for example, the transaction implementation Error => Exposure Failure event). Once again, divorcing is used to ease complexity and aid, at a later stage of development, expert elicitation and probability adaption.

One driver that is not included in the mix of KRDs is the quality of the deal document presented to SFO. Any errors in the deal document could be manifested within the SFO environment as an operational loss event. To demarcate between units, we have assumed that the deal document received by SFO is completely correct. This assumption, however, is not realistic, and is only used for the purpose of drawing a boundary around SFO. The problem with this approach is that it removes the opportunity for the bank to use the model for the purpose of measuring correlations between operational loss events occurring in various units. Absence of this deal document KRD is inconsistent with the current inclusion of the system failure KRD, whose causal antecedents would likely be located in the wholesale banking division's information technology and systems management unit. Criticizing current operational risk models, Mittnik and Starobinskaya (2007) suggested that Bayesian networks represented superior modelling tools because they could incorporate the linkages between units more easily.

Other operational loss events previously identified by SFO, such as approval compliance and documentation, are not explicitly included in the final network model, although they may be included within regulatory/legal/tax failure, at the discretion of the risk manager. However, the subsequent modular design of the final network would make their inclusion relatively straightforward. The remaining category, theft, is considered to be more problematic and requires its own separate causal model.

The structure of the final model is partitioned into the following broad categories: (i) work environment/skills and experience; (ii) transaction characteristics; (iii) human error categories; (iv) error types, and the more familiar operational loss events; (v) regulatory/legal/tax failure events; (vi) exposure management failure events; and (vii) payment failure events. Figure 3 and Table 1 describe graphically the final Bayesian Network structure.[2]

The resulting network generates a Junction Tree with 45 cluster nodes of which the maximal cluster size is a joint distribution table containing 15876 joint probabilities. These sizes are easily handled by the propagation algorithm, producing very efficient inference throughout the network.

Using the Bayesian network, SFO management can generate the unit's Operational Value-at-Risk (Op-VaR) measure, via simulation. An Op-VaR for a given time period can be estimated by using forward estimates of transaction volumes for SFO over the time period of interest. By simulating events for the specified volume of transaction activity, operational loss events can be counted, and the total loss amounts calculated. By generating an arbitrarily large number of possible event histories, over the time

[2]A document containing a detailed description of each node can also be obtained via e-mail by contacting the corresponding author.

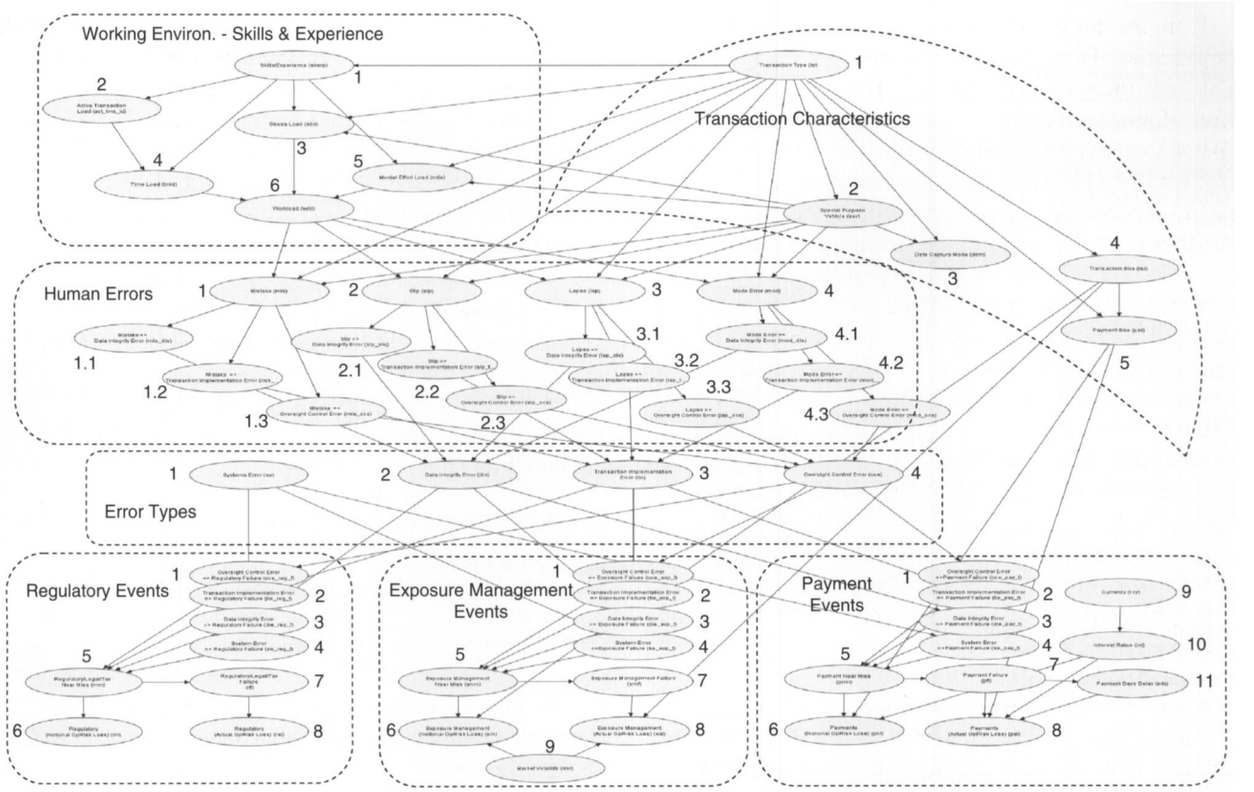

Figure 3 SFO Operational Risk Network Model.

period and associated transaction volume, a distribution of operational losses can be generated and the Op-VaR dollar amount estimated for any specified confidence level.

Structure evaluation

Two approaches to structure evaluation are used during and at the end of the construction phase. The first approach involves revisions, walkthroughs and feedback from operational risk and SFO staff who are not involved in model construction. This is a somewhat informal approach, involving familiarity with the model, questioning and suggesting alternatives. The second is a more formal approach, based on the fact that a Bayesian network encodes, via its directed-acyclic graph, assumptions regarding the conditional dependence and independence relations between nodes or variables within the environment. Independence between nodes is referred to in the Bayesian network literature as d-separation.[3] Two nodes or two groups of nodes are said to be d-separated, if they are independent or conditionally independent of each other. For example, nodes in group Y are said to be d-separated from nodes in group X, given evidence, ε, instantiated on the remaining nodes Z when the following is true:

$$P(Y|X, Z = \varepsilon) = P(Y|Z = \varepsilon) \quad (1)$$

The probability of event Y, given event X and the evidence $Z = \varepsilon$, is equal to the probability of event Y, given evidence $Z = \varepsilon$. A condition-independence relation is sometimes written using the notational form:

$$(Y \perp X|Z = \varepsilon) \quad (2)$$

This reads as follows: X and Y are independent, given evidence of $Z = \varepsilon$. The d-separation properties between nodes is also symmetrical, thus if X is independent of Y, given $Z = \varepsilon$, then Y is independent of X, given $Z = \varepsilon$. Furthermore, it is possible for a node or a group of nodes that were previously d-separated to become d-connected when evidence is added to the network.[4]

What does d-separation mean from a network modeller's perspective? If two nodes or groups of nodes are d-separated, then information about the first node or groups of nodes will not provide any further information on the state or states of the second node or group of nodes. Therefore, in constructing a network model, the modeller should ensure that the network structure contains no

[3]The term 'd-separation' is short for 'directed acyclic graph separation'. Nodes are said to be d-connected if their states are dependent.

[4]If the state of a child node (effect) is observed, and this child node has multiple parent nodes (causes), then information about the state of one of the parent nodes can alter beliefs regarding the state of one of the other parent nodes. This is referred to as 'explaining-away'.

Table 1 SFO Operational Network*

Work environment—skills and experience	*Human errors*	*Regulatory events*
1 Skills/Experience [3] {26}	1 Mistake [2] {78}	1 Oversight Control Error = > Regulatory Event [2] {1}
2 Active Transaction Load [6] {15}	1.1 Mistake = > Data Integrity Error [2] {2}	2 Transact. Implement. Error = > Regulatory Event [2] {1}
3 Stress Load [3] {156}	1.2 Mistake = > Transact. Implement. Error [2] {2}	3 Data integrity error = > Regulatory event [2] {1}
4 Time Load [3] {36}	1.3 Mistake = > Oversight Control Error [2] {2}	4 System Error = > Regulatory Event [2] {1}
5 Mental Effort Load [3] {156}	2 Slip [2] {78}	5 Regulatory Near Miss [2] {0}
6 Work Load [3] {0}	2.1 Slip = > Data Integrity Error [2] {2}	6 Regulatory (Notional OpRisk Loss) [4] {2}
Transaction characteristics	2.2 Slip = > Transact. Implement. Error [2] {2}	7 Regulatory/Legal/Tax Failure [2] {1}
1 Transaction type [13] {12}	2.3 Slip = > Oversight Control Error [2] {2}	8 Regulatory (Actual OpRisk Loss) [4] {2}
2 Special purpose vehicle [2] {13}	3 Lapse [2] {78}	
3 Data capture mode [2] {26}	3.1 Lapse = > Data integrity error [2] {2}	*Payment events*
4 Transaction size [7] {78}	3.2 Lapse = > Transact. Implement. Error [2] {2}	1 Oversight Control Error = > Payment Failure [2] {1}
5 Payment size [7] {546}	3.3 Lapse = > Oversight Control Error [2] {2}	2 Transact. Implement. Error = > Payment Failure [2] {1}
Exposure management events	4 Mode Error [2] {78}	3 Data Integrity Error = > Payment Failure [2] {1}
1 Oversight control error = > Exposure failure [2] {1}	4.1 Mode Error = > Data Integrity Error [2] {2}	4 System Error = > Payment Failure [2] {1}
2 Transact. Implement. Error = > Exposure Failure [2] {1}	4.2 Mode Error = > Transact. Implement. Error [2] {2}	5 Payment Near Miss [2] {0}
3 Data Integrity Error = > Exposure Failure [2] {1}	4.3 Mode Error = > Oversight Control Error [2] {2}	6 Payments (Notional OpRisk Loss) [21] {0}
4 System Error = > Exposure Failure [2] {1}	*Error types*	7 Payment Failure [2] {1}
5 Exposure Failure Near Miss [2] {0}	1 System Error [2] {1}	8 Payments (Actual OpRisk Loss) [21] {0}
6 Exposure Management (Notional OpRisk Loss) [11] {0}	2 Data Integrity Error [2] {0}	9 Currency [9] {8}
7 Exposure Management Failure [2] {1}	3 Transact. Implement. Error [2] {0}	10 Interest Rates [9] {72}
8 Exposure Management (Actual OpRisk Loss) [11] {0}	4 Oversight Control Error [2] {0}	11 Payment Days Delay [6] {4}
9 Market Volatility [8] {7}		

Note: node labels—[Number of node states] {Number of probabilities requiring elicitation (0 indicates that an expression is used)}.

d-separated nodes, to which a domain expert would consider to contain information about each other.

Analysing the d-separation properties of the network is important as it allows the domain expert to check the network against their own understanding of the environment conditional independencies. The network model should represent a cognitive causal mapping of the working environment, as understood by the domain expert. By doing the d-separation analysis, the causal pathways and/or information relevancies of nodes can be validated against the internal model of the domain expert, which is the risk manager. The Bayesian network tool used here comes with functionality that makes the d-separation analysis relatively straightforward (for a more expansive discussion of d-separation, refer to Jensen and Nielsen, 2007).

In developing the network model, a major design concern is to ensure that the transaction type node remains d-connected to the operational loss event nodes. One of the most important outputs required of the model, from the risk manager's perspective, is to provide predictive probabilities of operational loss events, conditional on the different types of transactions processed and the working conditions within the SFO environment. The transaction type node represents a considerable amount of implicit information. Contained within that node is an implicit representation of the process detail, and how that transaction type process interacts with the working conditions and operator loadings. It would undermine the model's performance if this information was not available to the operational loss event nodes. It is not necessary to have a direct causal link between the transaction type and the operational loss events nodes, so long as at least one pathway is available. It might be argued, however, that the extra directed causal link from transaction type to operational loss event nodes would represent all other causes that are not related to human errors, or system error events, etc. This point is really moot, as ultimately the transaction type node is d-connected to all operational loss event nodes, provided that not all of the human error type nodes are instantiated, and they would not be instantiated when using the model for operational risk predictions.

All nodes are d-connected to the transaction type node, except those nodes related to system error, currency, interest rates and market volatility. Nodes related to system error, which are not d-connected to the transaction type, include system error = > regulatory/legal/tax event, system error = > exposure management event, and system error = > payment failure event. This result is consistent with the risk manager's own conceptualization of the domain (it is expected that the transaction types, and the processes they represent, within the domain would influence the state of all other nodes, except those exogenous variables located outside of SFO).

Likewise, the other important nodes related to operational loss events are those that model the working environment, and the internal state of operators within SFO. These nodes include skills and experience, active transaction load, time load, mental effort load and stress load. They may well be instantiated with evidence, as part of the process of predicting operational loss events. Once again, the transaction type node remains d-connected to the operational loss event nodes with all of the working environment and internal operator state nodes instantiated.

The process of verifying the independencies of variables in the modelled domain can place a heavy cognitive demand on the domain experts. This level of effort can in part be mitigated with the help of software tools that automatically identify and display the dependencies and independencies between the network nodes. Another approach that may also reduce the design and verification demands on domain experts is the use of 'idioms', first suggested by Neil *et al* (2000) as a means to support the design of large complex Bayesian networks. An idiom represents a smaller sub-network component of the overall domain. Their conceptual foundation is similar to that of the reusable object found in object-oriented software development. By combining smaller, less complex and reusable software components together, more complex software solutions can be created that are easier to verify and test. Idioms not only support a reduction in the demands of network design, they also allow the reuse of sub-network components. Although idioms were not used in the design of our network, the opportunity to use them in future research will be explored. A more recent example of the use of idioms can be found in Fenton *et al* (2007).

Conclusions and future research

We have developed a network structure for the modelling of operational risk based on a functioning SFO unit within a major Australian bank. The dominant perspective used in developing this model structure is that of human error and its role in contributing to operational losses. Within the unit under investigation, human action plays a dominant role in the transaction processes, which makes it logical to emphasize human error. The model is designed to generate probabilities of operational loss events by consideration of interaction between the working environment, transaction processes and their effect on the generation of human errors. A valuable feature of our model is its modularity, which provides the opportunity to add other types of operational loss events as necessary.

Future development of the model involves the elicitation of prior probabilities for each of the states for each node and their parent node configurations. This will allow *a priori* event probabilities to be generated and evaluated against the actual probabilities experienced within the unit. Further research will also consider how the model will adapt, as new information arises in the unit. The Bayesian network technology allows for the learning of model structure and parameters directly from observed data. We see this model adaption functionality as an important future development, making the model responsive to changes within the environment. We also see this adaption feature as being a valuable addition for the purposes of organizational learning. Operational staff will have the facility to compare their *a priori* assumptions and beliefs against the adapting model, as new risk events unfold.

Operational risk involves the failure of people, processes and systems. Although the 'people' component is well covered by the model, we would like to include more features that cover processes and systems as well. This, we feel, will give the model a greater range of applications in banking. An important further addition will be to introduce more nodes that help to identify control failures, particularly as they relate to internal and external fraud.

Although we focused on human errors in our model, it is worth reminding ourselves that it is people, and people alone, who possess the only source of agency within an organization. Although processes and systems may fail, whether due to poor design or function, it is ultimately people who must take responsibility. It is for this reason that, by focusing on human errors, the model provides a good foundation for future development.

Acknowledgements—The authors acknowledge the financial support provided through two research grants awarded by the Department of Accounting and Finance, Monash University, and the Melbourne Centre for Financial Studies. The second author is also supported by an ARC Discovery grant for which he is grateful.

References

Adusei-Poku K, Van den Brink GJ and Zucchini W (2007). Implementing a Bayesian network for foreign exchange settlement: A case study in operational risk management. *Journal of Operational Risk* **2**(2): 101–107.

Alexander C (2000). *Bayesian methods for measuring operational risk*. Discussion Papers in Finance No 2000-02. University of Reading.

Alexander C (2003). Managing operational risks with Bayesian networks. In: Alexander C (ed). *Operational Risk: Regulation, Analysis and Management*. Financial Times Prentice-Hall: London, pp 285–295.

Anderson R, Mackoy R, Thompson V and Harrell G (2004). A Bayesian network estimation of the service-profit chain for transport service satisfaction. *Decision Sci* **35**: 665–689.

Basel Committee on Banking Supervision (BCBS) (2004). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. Bank for International Settlements: Basel.

Bedford T and Cooke R (2001). *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press: Cambridge.

Bobbio A, Portinale L, Minichino M and Ciancamerla E (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliab Eng Syst Safe* **71**(3): 249–260.

Bromley J, Jackson NA, Clymer OJ, Giacomello AM and Jensen FV (2005). The use of Hugin® to develop Bayesian networks as an aid to integrated water resource planning. *Environ Model Softw* **20**: 231–242.

Cooper RG (2000). Strategic marketing planning for radically new products. *J Marketing* **64**: 1–16.

Cornalba C (2009). Clinical and operational risk: A Bayesian approach. *Methodol Comput Appl* **11**: 47–63.

Cowell RG, Verrall RJ and Yoon YK (2007). Modeling operational risk with Bayesian networks. *J Risk Insur* **74**: 795–827.

Davis GA (2003). Bayesian reconstruction of traffic accidents. *Law, Probability and Risk* **2**: 69–89.

Fenton N, Neil M and Caballero JG (2007). Using ranked nodes to model qualitative judgements in Bayesian networks. *IEEE T Knowl Data En* **19**(10): 1420–1432.

van der Gaag LC, Renooij S, Witteman CLM, Aleman BMP and Taal BG (2002). Probabilities for a probabilistic network: A case study in oesophageal cancer. *Artif Intell Med* **25**: 123–148.

Jensen FV and Nielsen TD (2007). *Bayesian Networks and Decision Graphs*. Springer Science + Business Media, LLC: New York.

Kadane JB and Schum DA (1996). *A Probabilistic Analysis of the Sacco and Vanzetti Evidence*. Wiley: New York.

Kemmerer B, Mishra S and Shenoy PP (2001). *Bayesian causal maps as decision aids in venture capital decision making: Methods and applications*. Working Paper. University of Kansas.

Khodakarami V, Fenton N and Neil M (2007). Project scheduling: Improved approach to incorporate uncertainty using Bayesian networks. *Proj Mngt J* **38**: 39–49.

Koller D and Friedman N (2009). *Probabilistic Graphical Models: Principles and Techniques*. MIT Press: Cambridge, MA.

Korb KB and Nicholson AE (2004). *Bayesian Artificial Intelligence*. Chapman & Hall/CRC: Boca Raton, FL.

Marquez D, Neil M and Fenton N (2010). Improved reliability modeling using Bayesian networks and dynamic discretization. *Reliab Eng Syst Safe* **95**(4): 412–425.

Mittnik S and Starobinskaya I (2007). Modeling dependencies in operational risk with hybrid Bayesian networks. *Methodol Comput Appl* **12**: 379–390.

Moosa IA (2008). *Quantification of Operational Risk under Basel II: The Good, Bad and Ugly*. Palgrave MacMillan: London.

Neapolitan RE (1990). *Probabilistic Reasoning in Expert Systems: Theory and Algorithms*. Wiley: New York.

Neapolitan RE (2004). *Learning Bayesian Networks*. Prentice Hall: Harlow.

Neil M, Fenton N and Nielsen L (2000). Building large-scale Bayesian networks. *Knowl Eng Rev* **15**(3): 257–284.

Neil M, Fenton N and Tailor M (2005). Using Bayesian networks to model expected and unexpected operational losses. *Risk Anal* **25**: 963–972.

Neil M, Tailor M and Marquez D (2007). Inference in hybrid Bayesian networks using dynamic discretization. *Stat Comput* **17**: 219–233.

Neil M, Tailor M, Marquez D, Fenton N and Hearty P (2008). Modelling dependable systems using hybrid Bayesian networks. *Reliab Eng Syst Safe* **93**: 933–939.

Neil M, Häger D and Andersen LB (2009). Modeling operational risk in financial institutions using hybrid dynamic Bayesian networks. *J Opl Risk* **4**: 3–33.

Paté-Cornell ME and Dillon RL (2006). The respective roles of risk and decision analyses in decision support. *Decision Anal* **3**: 220–232.

Paté-Cornell ME and Guikema S (2002). Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. *Mil Oper Res* **7**: 5–20.

Pearl J (1988). *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann: San Mateo, CA.

Powell SG, Baker KR and Lawson B (2008). A critical review of the literature on spreadsheet errors. *Decis Support Syst* **46**: 128–138.

Powell SG, Baker KR and Lawson B (2009). Impact of errors in operational spreadsheets. *Decis Support Syst* **47**: 126–132.

Reason J (1990). *Human Error*. Cambridge University Press: Cambridge.

Reid GB and Nygren TE (1988). The subjective workload assessment technique: A scaling procedure for measuring mental workload. In: Hancock PA and Meshkati N (eds). *Human Mental Workload*. North-Holland: Amsterdam, pp 185–218.

Sanford AD and Moosa IA (2009). *Operational risk modelling and organizational learning in structured finance operations: A Bayesian network approach*. Working Paper. Department of Accounting and Finance, Monash University.

Sigurdsson JH, Walls IA and Quigley JL (2001). Bayesian belief nets for managing expert judgement and modelling reliability. *Qual Reliab Eng Int* **17**: 181–190.

Taroni F, Aitken C, Garbolino P and Biedermann A (2006). *Bayesian Networks and Probabilistic Inference in Forensic Science*. Wiley: New York.

Trucco P, Cagno E, Ruggeri F and Grande O (2008). A Bayesian belief network modelling of organisational factors in risk analysis: A case study in maritime transportation. *Reliab Eng Syst Safe* **93**: 823–834.

Uusitalo L (2007). Advantages and challenges of Bayesian networks in environmental modelling. *Ecol Model* **203**: 312–318.

Willems A, Janssen M, Verstegen C and Bedford T (2005). Expert quantification of uncertainties in a risk analysis for an infrastructure project. *J Risk Res* **8**: 3–17.

Received April 2010;
accepted November 2010