The International Journal of Business Management and Technology, Volume 4 Issue 6 November–December 2020
ISSN: 2581-3889

Research Article Open Access

Managing Operational Risk using Bayesian Networks: A practical approach for the risk manager

Dr. Martin Leo, Dr. Suneel Sharma, Dr. K Maddulety
SP Jain School of Global Management

Abstract: This paper provides a practical approach to construct and learn a Bayesian network model that will enable an operational risk manager communicate actionable operational risk information for informed decision making by senior managers. Bayesian networks and their application in operational risk management has been widely studied; however, literature and research has predominantly focused on their application in modeling and measuring operational risk for capital calculation purposes. We detail the approach to construct and learn a BN model, from an incident database, using the machine learning capabilities in the R package bnlearn. The modeling and the inference capabilities of the Bayesian Networks can be applied to business-as-usual risk management techniques such as loss analysis, scenario analysis, risk assessment, development of key risk indicators, and risk reporting.

Keywords: Bayesian networks, Probabilistic Graphical Models, machine learning, operational risk management, banking

I. INTRODUCTION

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" and is a "fundamental element of risk management" at banks [1]. In a review of Bank annual reports, operational risk was varyingly presented and included several sub risks and could be referred to more as a non-financial risk. It included, among many others, fraud risk, cybersecurity, clients, products, and business practices, information and resiliency risk, money laundering and financial crime risks, vendor and outsourcing risks, technology risk, business disruption risks [2].

Risk measurement is a key tool in the capture and controlling of risks. Main reasons for which Banks typically measure operational risks are a) capital allocation b) performance management by linking capital allocation changes with the performance as regards risk management c) establishing criteria of objectivity and comparability in prioritizing risk control to improve the internal control environment d) evaluation of risk transfer decisions. Methods applied for measuring operational risk can either be statistical – similar to market and credit risk, based on historical data on the frequency of loss occurrence, size of the loss, or scenario analysis, based on scenarios – low frequency and high severity – referring to external data. Operational risk has, for a large part, been managed through qualitative risk management practices (e.g., checklist, operations manuals), which, while relatively easy to implement, have various limitations [3]. Approaches typically followed in operational risk modeling are either top-down – based on macro data or bottom-up based on the identification of individual events or loss causes [4].

Managers have varied objectives and the need for them to manage the inherent uncertainty around these objectives. Managers' decision making can be more effective when they are aware and can consider identified and measured risks that can be communicated through improved risk reporting methodologies, thus furthering the organization's ability to succeed. This, therefore, creates different requirements for risk information and should be factored into risk reporting approaches [5].

Probabilistic graphical models (PGM) have become the method of choice for representing uncertainty. They are used in many research areas such as computer vision, speech processing, time-series, and sequential data modeling,

cognitive science, bioinformatics, probabilistic robotics, signal processing, communications, and error-correcting coding theory, and the area of artificial intelligence. A PGM consists of a graph and a set of random variables. It represents a joint probability distribution (JPD) where the graph captures the conditional independence relationships among the random variables. PGMs are considered to be one of the best approaches for modeling uncertainty in many domains [6].

We see that BNs have been widely explored for operational risk capital calculation and related risk exposure reporting and disclosures [4,7,8]. They have also been explored to analyze better and understand the operational risk related to specific process areas or sub risk areas [9,10]. In this paper, we extend the research done, exploring the use of BNs in the modeling of operational risk to enable risk managers and business managers better manage operational risk on a day to day basis, i.e., "business-as-usual" operational risk management (ORM).

There is a rise in interest and the popularity of powerful and analytical solutions such as machine learning and artificial intelligence within financial institutions. This rise is a consequence of the desire to enhance analytical capabilities for managing and mining the increased volumes and variety of data [11]. It would be beneficial to study how machine learning can be applied in the enhancement of risk measurement, risk reporting, risk assessment, and aggregation of risk as banks seek to enhance their analytical capabilities and also mature their enterprise risk management [2].

We describe how Bayesian networks can be efficiently machine learned, from an operational risk incident database, enabling a risk manager to measure and report operational risk effectively. This BN can enhance risk reporting to various stakeholders in a bank, giving them the ability to manage risk better and to make risk-informed decisions. We created a risk incident database and applied the learning capabilities of the R package bnlearn to build the network structure, learn the parameters. We have then, through the application of the modeling and inference capabilities, evaluated the model for various ORM use cases. We evaluate the use of the R package bnlearn in the modeling of the BN for the management of operational risk. As the focus of this paper is not capital modeling, we have avoided references to distribution (e.g., loss distributions) and focused more on the risk impact as a discrete value.

We provide a review of BNs in the area of operational risk management in section 2. In section 3, we provide the approach to building the BN model by applying the R package bnlearn on an operational risk incident database. In section 4, we evaluate the use of the BN model in managing operational risk.

II. BAYESIAN NETWORKS AND OPERATIONAL RISK MANAGEMENT

2. 1 Definition

A graphical model is a probabilistic database – whose pieces are built using probability theory, ensuring a consistent overall interpretation - a machine that can answer "queries" regarding the values of sets of random variables [12]. PGMs use a graph-based representation as the basis for compactly encoding a complex distribution allowing for a compact representation of a set of independencies and also defining a skeleton for representing a high-dimensional distribution. There are two families of graphical representations of distributions – BNs, uses a directed graph, and the second a Markov networks use an undirected graph [13].

BNs, also known as "belief networks" (or "Bayes nets" for short), belong to the family of PGM, also corresponding to a structure known as a directed acyclic graph (DAG) that is popular in statistics, machine learning, and artificial intelligence. BNs, deriving their name from the Bayesian rule of probabilistic inference, are graphic models of events and processes, is based on probability and graph theories. They allow the representation of knowledge about an uncertain domain. They are considered mathematically robust and intuitively understandable. The concept of modularity (decomposing a complex system into simple elements) is central to constructing a graphic model. The probability theory is used for combining the elements into a system, providing consistency of the whole model, integrating the graphic models and distributions. The structure is ideal for combining prior knowledge and can be applied in the representation of both causal and probabilistic semantics. They can be further extended in the case of missing data to learn causal relationships, gaining insight into the problem domains, and in the prediction of future events. They can be a convenient tool for describing complex processes and events having structural and statistical

uncertainties and are a promising approach to simulate processes having uncertainties. They can be applied to both static and dynamic processes [14,15].

A graphical model can be defined as consisting of variables (nodes) K = {1, 2,…k} with a set E of dependencies (edges) between the variables and a set of P of probability distribution functions for each variable. BNs are graphical models, more specifically a DAG with all of the edges in the graph pointing in a particular direction – directed – with non-cyclic.

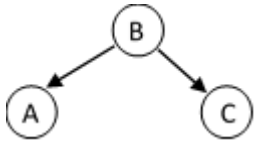

Fig 1 Bayesian Network.

Fig 1 is an illustration of a BN having a set of edges E= {(B, A), (B, C)}. The edges, encode a particular factorization of the JPD and are directed with no cycles. A and C are conditionally independent of each other with P(A | B, C) = P(A | B), meaning that for the factorization represented by this BN, the probability of A is conditioned only on B with the value of C irrelevant.

Friedman et al. (2004) describe a BN, B = (G; P), as a representation of a JPD. G is a DAG that consists of vertices (V), and edges (E), G = (V:E). The vertices, also called chance nodes, denote a domain of random variables $X_1 \ldots X_n$ and may assume a value x_i from the finite domain Val(X_i). When an edge goes from a node X_i to a node Xj, X_i is said to be a causal parent of Xj, showing causal dependencies between the nodes. P of the network B, describes a conditional probability distribution (CPD) for each chance node, P(X_i), given the set of its causal parents Pa(X_i) in G. The JPD of the domain $X_1 \ldots X_n$ can be written using the chain rule of probability, in the product form:

$$P(X_1, \ldots, X_n) = \prod_{i=1}^{n} P\,(X_i | Pa(X_i))\ SEQ\ Equation \setminus *\ ARABIC\ 1$$

Margaritis (2003), in his thesis, highlights the reasons for choosing BNs for modeling are that they are capable of displaying relationships clearly and intuitively, and being directional can represent cause-effect relationships. They can handle uncertainty and can do so through the established theory of probability. Their signature characteristic is the ability to encode directional relations that can represent cause-effect relationships. They are capable of representing many of the independencies in a domain through their structure, which is a DAG.

Svensson (2015) explains that Bayesian inference uses Bayes' theorem to draw statistical inference about observed data. It differs from the basic frequentist inference in the use of a prior hypothesis about data and the use of acquired data to update the probability. Bayes' theorem is in its simplest form is expressed as:

$$P(H|E) = \frac{P(E|H)P(H)}{P(E)}\ SEQ\ Equation \setminus *\ ARABIC\ 2$$

2.2 Bayesian networks in Operational Risk Management

Methods applied for measuring operational risk can either be statistical – similar to market and credit risk, based on historical data on the frequency of loss occurrence, size of loss; or scenario analysis, based on scenarios – low frequency and high severity – referring to external data [3]. Approaches typically followed in operational risk modeling are either top-down – based on macro data or bottom-up based on the identification of individual events or loss causes. Lack of data can cause difficulties in the measurement of operational risk [4].

Operational risk is hard to quantify, given the presence of heavy-tailed loss distributions. Extreme value distributions used in this context are very sensitive to data – and this is a problem when loss data is rare. Some events may be rare in frequency and unlikely to be observed but could be potentially more dangerous in terms of impact. In general, the objective is to arrive at the distribution of losses for the next period based on available data to obtain the predictive distributions for the frequency and severity [7]. The major challenge banks face in modeling operational risk scenarios is lack of relevant data, given the rarity of incidents with significant losses owing to operational failures

[4,17,18]. Therefore, the traditional data-driven approaches to model-building with parametric loss models are of limited use at well managed banks. BNs allow overcoming these hurdles as they combine qualitative data from experts and relevant quantitative data. Among other challenges in ORM are the complex dependence structures of the associated variables [18]. Also challenging, in ORM, is the modeling of dependence between different risk cells and factors given the need to model the correlations. Limited data does not allow for reliable estimates of correlations and are supplemented with estimates using expert opinion [19]

The development of operational risk models through a systems-oriented approach allows the models to be extended to operational risk control beyond risk capital allocation. Such a model requires a deeper understanding of causation in operational risk events incorporating antecedent events and causal pathways of operational losses. In a continually changing environment, the estimation of operational risk frequency and severity distributions cannot be done solely using historical data, given their limitations in predicting future losses. Scenario analysis is included to identify risks, analyze past events – internal or external – including near misses, and considering current and planned controls. Experts are surveyed through workshops and/or questionnaires. Additionally, external loss data is included in the modeling as an essential source of information [9].

Any model that incorporates subjective prior beliefs is a form of the Bayesian model. Operational risk modelling uses observable, and therefore 'objective' data and subjective choice, or 'prior belief' parameters and is, therefore, more suited for BN modelling. BNs enable reasoning under uncertainty, combining the advantages of an intuitive visual representation coupled with the sound mathematical base in Bayesian probability. BNs allow us to articulate dependencies between different variables and to consistently propagate the impact of evidence on the probabilities of uncertain outcomes. Another advantage is that they enable us to combine any statistical data available with qualitative data mirroring the causal structure of the underlying process easing the communication with the users and their understanding [20]. BNs improve transparency for efficient risk management, being based on causal flows in an operational process [21].

In the area of operational risk, BN methodologies can be applied to combining different sources of data (internal data, external data, and expert opinion). They can be used in modelling various risk factors of operational risk, learning correlation structures, and allowing for update of parameters to incorporate a dynamic flow of information. BNs can be used for scenario analysis. [4,7,19,21–24]. BNs have an advantage in that they enable us to combine any statistical data that is available with qualitative data, mirroring the causal structure underlying the process itself, making it easy to understand and communicate to business users. BNs can successfully model dependencies between events and processes in complex systems. The causes and effects of unexpected loss events, such as related to an IT infrastructure in a financial institution, can be modeled using a BN [20].

A Bayesian approach is a viable option for the managing of operational risk in an environment of uncertainty and scarce information. While the application of BN to operational risk management has been explored, much of the focus has been around their application to risk measurement for capital calculation or regulatory disclosures, such as calculation of the Value at Risk (VaR) or loss distribution analysis [9,25–27]. Several papers have extensively explored process and loss event analysis using BN modelling oriented more towards the better analysis and understanding of operational risk related to specific process areas or sub risk areas [9,10]. We see that further research is required to elaborate on how the BN models, can be constructed and learned, and then be applied in the effective management of operational risk at a bank or unit level. How can these models be used in the day to day risk management and not just for regulatory reporting or risk calculation purposes. Also, how the models can allow for risk management to be viewed at a bank-wide or bank unit wide level and not just specific to a process or sub-risk type.

III. MATERIALS AND METHODS

In this section, we detail the approach taken for building and applying a BN machine learning algorithm for the management of ORM.

Machine learning, lying at the intersection of computer science, engineering, and statistics, has been highlighted as a tool that can be applied to various problems. This is especially so in fields that require data to be interpreted and acted upon [28]. Machine learning has become a popular tool when faced with the requirement of extracting meaningful information from data, and to study the resulting complexity of patterns. Machine learning programs are endowed to learn and improve and can be applied when faced with the dual challenge of complexity and the need for adaptability [29].

In machine learning datasets are typically divided into two sets – a training set and a test set. The algorithm is first applied to the training set for it to learn whatever representation is most appropriate for the problem – in this case learning the causal structure (dag of a BN) or learning the parameters for the structure (CPT). Once this representation has been learned, it can then be applied in predicting the values of target variables. Testing the model on the same dataset can lead to overfitting; hence, the test set, separate from a training set, can be used solely for testing after the learning task is completed.

3.1. Algorithms

Model selection and estimation are collectively known as learning in the field of BNs and is usually performed as a two-step process.

1. Structure learning, learning the structure of the DAG
2. Parameter learning, learning the local distributions implied by the structure of the DAG learned in the structure learning step

These steps can be either performed as unsupervised learning, using information provided by a data set, or as a supervised learning, via knowledge elicited from experts in the field. It is not uncommon to combine both approaches [30].

bnlearn is an R package that includes several algorithms for learning the structure of BNs with either discrete or continuous variables. It provides a free implementation of some BN structure learning algorithms. It is designed to provide the versatility that is required when handling experimental data analysis and can handle both discrete and continuous data. By providing a single object class (bn) for all the algorithms and a set of utility functions for performing descriptive statistics and basic inference procedures, it simplifies the analysis of learned networks [31,32]. bnlearn and its dependencies (the utils package, which is bundled with R) are available from CRAN.

3.2. Building the BN

For purposes of this paper and the model development – we will cover the phases as below using the relevant R packages.

Network structure learning

The network structure of the BN associated with the data set can be learned with the grow-shrink algorithm or hill-climbing algorithm. Both algorithms are known to learn a different network structure. While it may be more common and efficient to learn the structure automatically in many domains, the necessity to incorporate expert/domain knowledge can be addressed with the network structure being manually defined. This manual definition of structure may be more appropriate and fit for purpose in many domains. Visual examination of the graph structure can further provide insights into the properties of the network. graph and Rgraphviz are packages for which interfaces are available in bnlearn and can be used for visually presenting the structures.

Parameter learning

Once we know the structure of the network, we estimate the parameters of the distributions. Only one estimator is implemented – either a maximum likelihood estimator (mle) or a Bayesian one – and this can be specified. In bnlearn, this can be computed taking the network structure and the data as parameters. Alternately, we can also estimate the same conditional probabilities in a Bayesian setting, using their posterior distributions

Inference

Inference is required for validation, testing, and during the business application of the model. Inference queries can be answered in two ways using either exact inference or approximate inference. Bnlearn or gRain can be applied for inference, with the latter applied for exact inference.

An alternative approach to inference is to use Monte Carlo simulations to randomly generate observations from the BN and use these to compute approximate estimates of the conditional probabilities of the variables of interest through cpquery and cpdist. cpquery returns the probability of a specific event given some evidence.

Validation

Cross-validation is a standard way to obtain unbiased estimates of a model's goodness of fit. Estimates computed from different learning strategies can be compared to choose an optimal structure for the data at hand.

bnlearn implements three cross-validation methods in the bn.cv() function. (i) k-fold cross-validation (the default): In this method, the data are randomly partitioned into k subsets. Each subset is then used in turns to validate the model that is fitted on the remaining k - 1 subset. (ii) Custom folds cross-validation: In this method, the data is manually partitioned by the user into subsets. These are then used as in k-fold cross-validation. There is no constraint for the subset to have the same size. (iii) Hold-out cross-validation: In this method, the data are repeatedly (randomly) partitioned into training and test data subsets of given size m and n – m. The observations are assigned randomly to each subset at each repetition. Each test subset is then used to validate the model that is fitted on the corresponding training subset.

The goodness of fit of different network structures, suggested by experts, can also be compared using bn.cv().

3.3. Data

In the absence of access to an operational risk database, we have created a synthetic risk incident database of 2002 records. We have created our database to be an extensive operational risk incident database similar to that likely to be found at a Bank. T**able 1** below shows the description of the table we created for our research. We have created the database with the fields, as explained in T**able 1**. A column "Risk.Type," referring to the Basel operational risk event type, has been included to capture a classification of the different risk types that a Bank and is based on the "Cause." The mapping between Cause and Risk.Type is shown in T**able 2**. Risk incidents have a consequential impact, and Banks capture this in their incident database. We have, therefore, created a discrete field called risk impact type and assigned a random risk rating (High, Medium, Low). The database has been created solely for modeling and to exhibit their application to use cases. It will not be used for any empirical analysis. Given the synthetic creation of the database, causal relationships are only illustrative, only a few Basel Operational Risk Event Types have been considered, and we have used discrete values for risk impact.

Table 1 The fields of the incident database, and their description, created for the research.

Incident Database		
Column Name	**Description**	**Values**
Control	Controls marked IT1 to IT12 refers to the internal controls. The failure of a control, in the presence of a Cause, would result in a Risk.Event. Control is a random variable.	IT1, IT2, IT3, IT4, IT5, IT6, IT7, IT8, IT9, IT10, IT11, IT12
Cause	Cause of the risk events. These refer to the causes the risk events (incidents) are attributed to. Cause is a random variable.	DF, HD, HL, HW, MSM, ND, Out, PD, SW, Telecom, UOD
Risk.Event	Risk events refer to the loss events that have occurred. These have been manually created to capture the risk event. They have been defined to capture the type of loss from the event. The events have been manually grouped to specific types of risk events as mentioned in the below table 2	AL, SD, TD, PE
Risk.Type	All incidents/risks, i.e. risk events, are grouped into specific risk types - or the Basel operational risk event types. The mapping is based on the cause of the incident and the risk event. Refers to the type of risk the risk event is classified into.	EF, BDSF, EDPM
Risk.Impact	A set of risk impact ratings were randomly generated to enrich the database with the impact of the incident. The values this variable can take are H (High risk), M (Medium risk), L (Low risk)	H, M, L

Table 2 Mapping of the Cause to the Risk Type (Basel Operational Risk Event Type). The linkage between Cause, Risk Event, and Risk Type can be seen in the table.

Cause	Risk Event	Risk Type
Hacking Damage (HD)	Asset Loss (AL)	External Fraud (EF)
External sources losses (HL)	Asset Loss (AL)	External Fraud (EF)
Natural Disaster (ND)	Asset Loss (AL)	Business disruption and systems failures (BDSF)
Delivery Failure (DF)	Service Disruption (SD)	Business disruption and systems failures (BDSF)
Hardware Failure (HW)	Technology Disruption (TD)	Business disruption and systems failures (BDSF)
Telecommunications (Telecom)	Technology Disruption (TD)	Business disruption and systems failures (BDSF)
Utility Outage/Disruption (UOD)	Technology Disruption (TD)	Business disruption and systems failures (BDSF)
Model System Misoperation (MSM)	Processing Error (PE)	Execution, delivery, & process management (EDPM)
Outsourcing (Out)	Service Disruption (SD)	Business disruption and systems failures (BDSF)
Product Defects (PD)	Processing Error (PE)	Execution, delivery, & process management (EDPM)
Software (SW)	Processing Error (PE)	Execution, delivery, & process management (EDPM)

The structure can be replicated for other loss events or incidents also. Per Basel requirements, the bank would be maintaining a database of all their loss events. This can be extended to record event external loss incidents that could be used for risk analysis. It is also assumed that a control failure that did not cause a loss (near-miss) would be captured in the database for recording and analysis purposes giving the bank a better visibility into potential risk and impacts.

3.4. Building and Evaluation

Design flow

We will set up a BN structure from beginning to end using bnlearn. Fig 2 shows the design for the process followed in the building and analysis of the BN. We start with the incident database created for this research. For validation purposes, we divide the data into separate training and test data sets. R's sample.int is used to randomly sample and create a 90% and 10% split. The training dataset will be used for structure learning and parameter learning. Once the parameters have been learned, we will be validating the parameters inferred from the training learning dataset with values queried from the test dataset. The BN learned from the training dataset will then be used in application to the Operational risk use cases and evaluated accordingly.

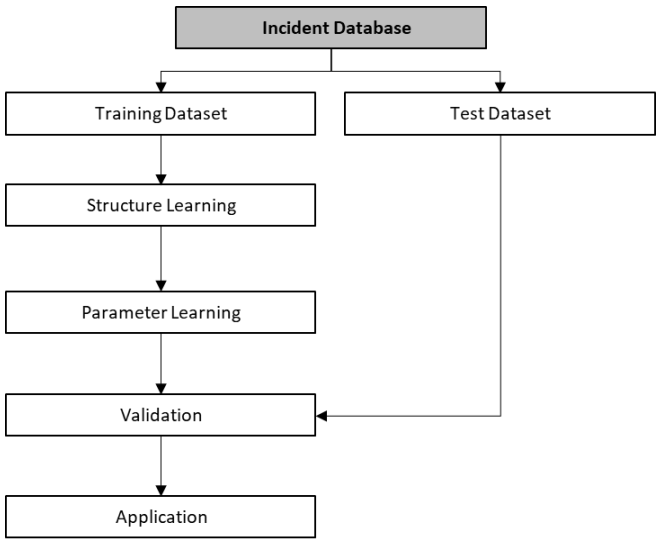

Fig 2 Design for the process followed in the building and analysis of the BN for this research

Evaluation

For evaluating and exhibiting the practical value of the model for managing operational risk, we will assess the following use cases:

1. Loss Analysis – use for analysis of causal factors and control deficiencies
    a. Causes and Controls that have the highest probability of resulting in risk events
    b. Causes and Controls that have the highest probability when there have been high risk impact events
2. Key Risk Indicators – Does the model allow for the design of useful and meaningful KRIs
    a. Related to specific risks in a clear and consistent way
    b. Development of KRIs for high risks identified
3. Scenario Analysis – Does the model allow the risk manager to assess the impact of new information received, e.g., new incidents (internal, external)
4. Risk assessment – Can the risk manager and other operational managers get information that could be used in an RCSA
    a. Assessing the probability of a given risk event given the failure of control and the presence of a causal factor
    b. Assessing the probability of a risk type
    c. Assessment of control effectiveness
5. Does the model allow for risk information to be communicated in a manner catering to different senior managers and risk managers?
    a. Allow senior managers to prioritize their risk remediation efforts
    b. Be aware of the risk types and the probability of the risk impact per impact type

Structure Learning

The structure can be modeled using expert advice. In this case, we use the risk event model explained through the causal view of risk [33]. We have modified the model, ignoring the mitigating variable, while renaming the consequence to risk impact. Additionally, to bring in the risk type, we have to add a path between the trigger to the risk impact. The risk type here refers to the Basel operational risk event type, and the trigger/threat would be the basis for determining the risk event type. Fig **3** below shows (a) the Fenton and Neil Model (b) a modified version of the Fenton and Neil model, where we add in the risk type and replace trigger with cause (c) the modified model with variables shown as an example (d) the BN model that has been manually constructed using bnlearn.

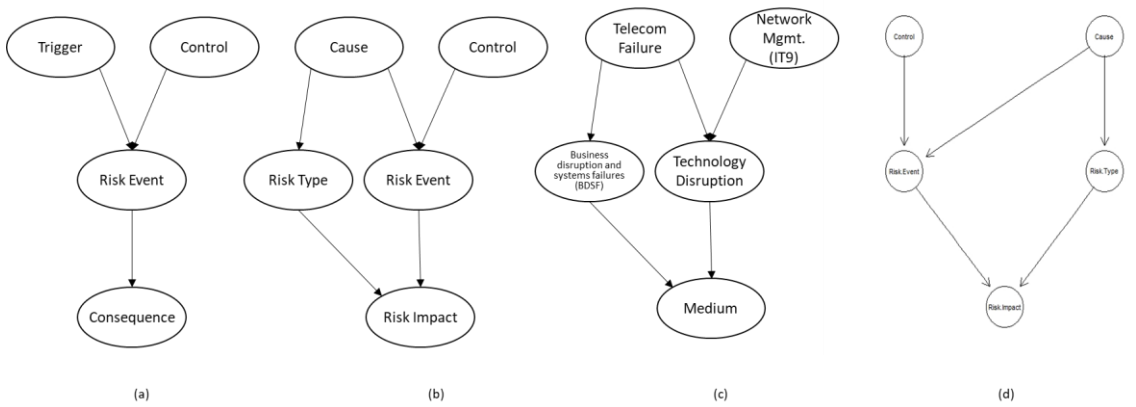

Fig 3 Bayesian network model (a) Fenton and Neil model (b) Fenton and Neil model modified adding in risk type (c) the modified model with example variables (d) structure of the BN model manually constructed using bnlearn.

Parameter Learning

As we know the structure of the network, now the parameters, in this case, conditional probabilities in the local distributions, can be estimated (or learned) from the database through the bn.fit function. We use the maximum likelihood estimation method in this case.

The conditional probabilities can be plotted for better visualization. This can provide beneficial insights for diagnostic and exploratory purposes. Fig **4** below shows the conditional probabilities can be presented for the risk type, given the risk event (e.g. BDSF given risk event DF).

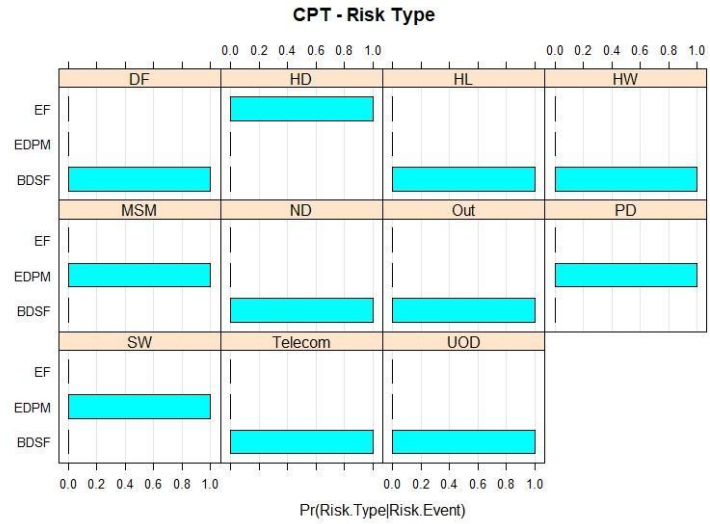

Fig 4 Chart from the BN showing the conditional probabilities for a risk type, given the risk event. Pr(Risk Type | Risk Event)

Similarly, **Fig** 5 goes further to show the risk impact conditional on risk event and risk type. A risk manager can see from such a chart that given a risk event (AL) and risk type (EF), a high risk impact incident is more likely.

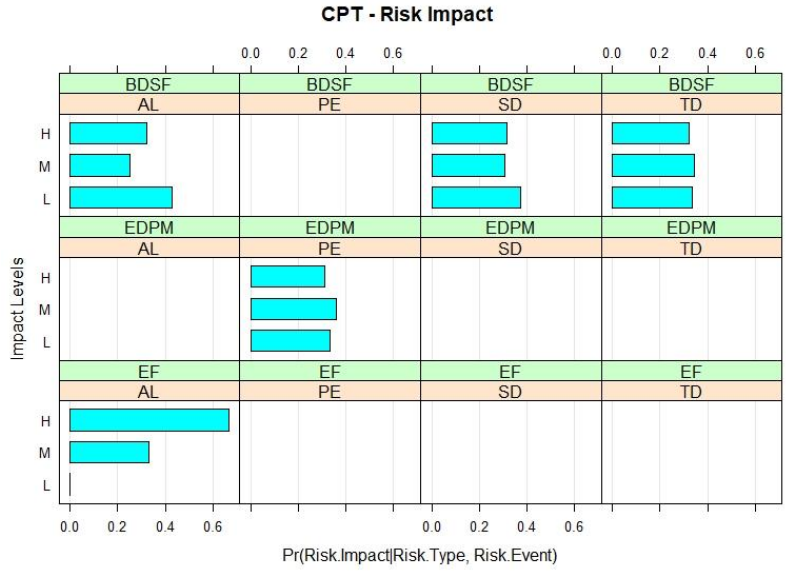

Fig 5 Chart from the BN, showing the probability of risk impact given a risk event and risk type. Pr(Risk Impact | Risk Event, Risk Type)

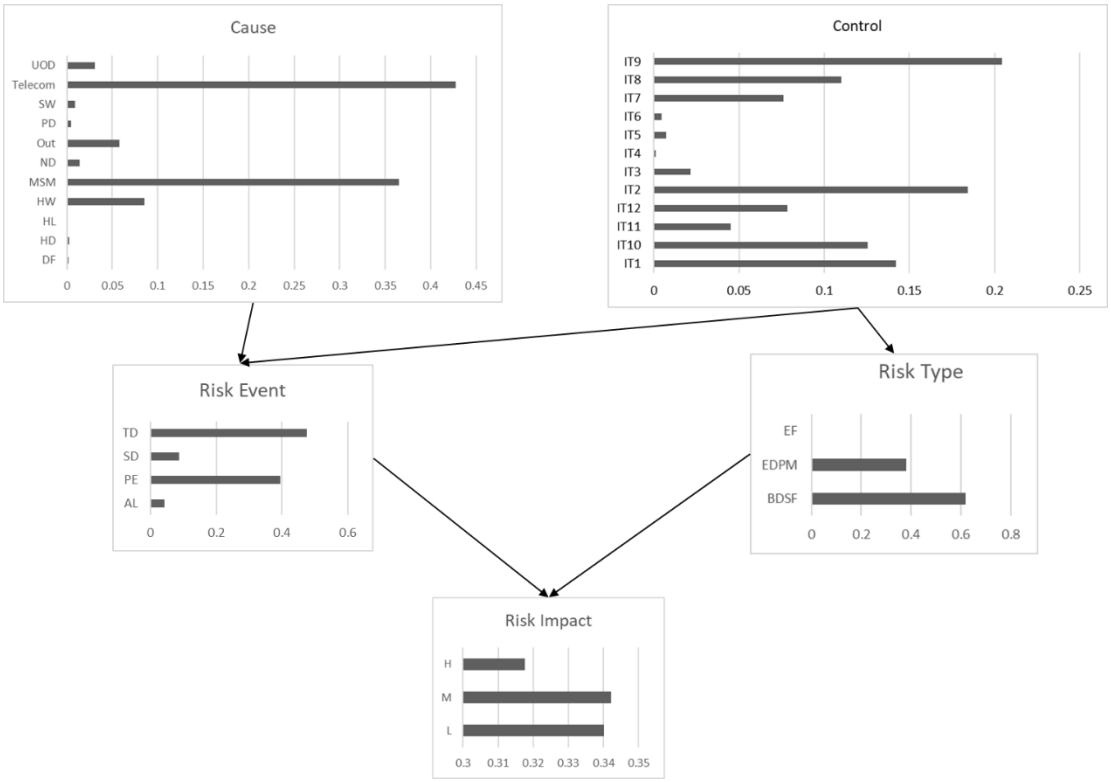

Fig 6 Bayesian Network with probabilities for each node of the BN for which parameters were learned from the incident data.

Validation - Compare a training and test database

We were able to calculate the probabilities from the BN for a few variables and given criteria, and used this to compute the expected values (number of rows meeting the same criteria) in the test data set. The estimate was then compared with the actual number of rows meeting the same criteria in the test. A risk manager can use this validation as an additional check to understand and evaluate the predictive ability of the BN. With adequate data,empirical validation of this output would be possible.

IV. DISCUSSION

In this section, we evaluate the application of the BN for the management of operational risk

4.1Loss Analysis

We can use the BN to analyze and understand the incident loss database such as the probabilities of the risk events and risk types. We can analyze the controls and causes that have a higher probability of causing a risk event. We can estimate the probability of occurrence of a high impact risk event or a medium risk impact event. The charts have been drawn using data computed through gRain and bnlearn inference queries.

a. Top risk event causes and controls – A risk manager by plotting a chart as in ***Fig*** *7* and ***Fig*** *8* can quickly understand the causes and controls that have the highest probabilities of resulting in a risk event.

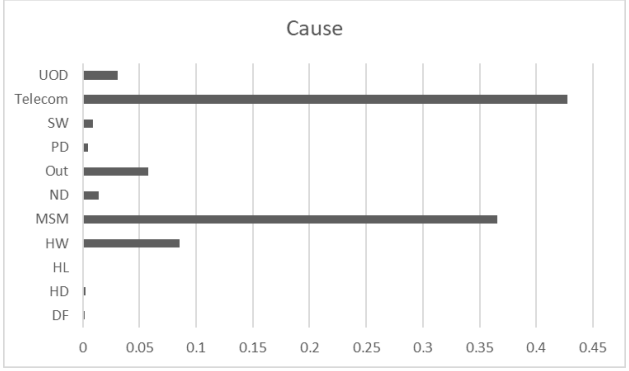

Fig 7 A chart to present the probabilities of each variable of the node Cause to easily view the cause having the highest probability of occurrence leading to an incident

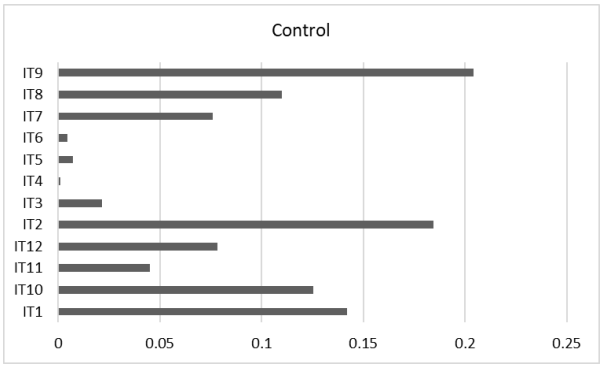

Fig 8 A chart to present the probabilities of each variable of the node Control to easily view the control having the highest probability of failure resulting in an incident

c. Cause and control failures of high impact risk events – A risk manager can evaluate the scenarios for High risk impact incidents. The node risk impact can be conditioned setting the state to High impact and the probabilities of the variables for each parent node – cause, control, risk events - can be then evaluated. ***Fig*** *9* shows the probabilities of the nodes when we set the evidence as risk impact = High allowing a quick understanding of the causes and controls that have the highest probabilities of resulting in high risk impact events.

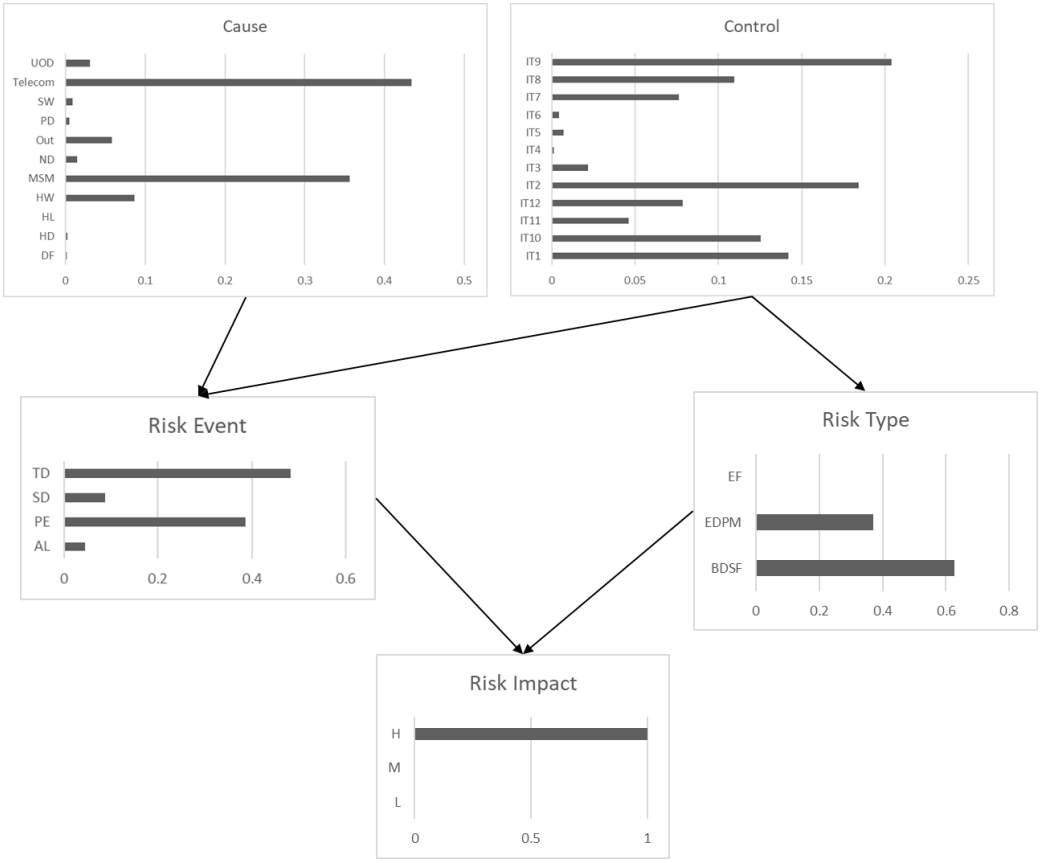

Fig 9 Network node probabilities after the BN is conditioned on the evidence "Risk Impact = H (High Risk)."

4.2. Scenario Analysis

We evaluated whether the model allows the risk manager to incorporate and assess the impact of new information arriving, e.g., new incidents (internal, external) so to add value in the process of scenario analysis.

We simulated a situation of two hacking damage related incidents being reported (internally or externally) by adding two incidents with the relevant cause and control to the incident database (training database). The number of rows in the training database increases after the addition of the 2 incidents.

We then learned the network structure and parameters of this updated data set. We were able to see that the marginal probabilities of the controls and the cause nodes changed, with the relevant cause and control probabilities, showing a slight increase from the original training database.

We ran a few inference queries to study the changes in the probabilities after adding the 2 incidents.
Fig 10 and **Fig** 11 below shows how changes in the related probabilities for the scenario we were simulating.

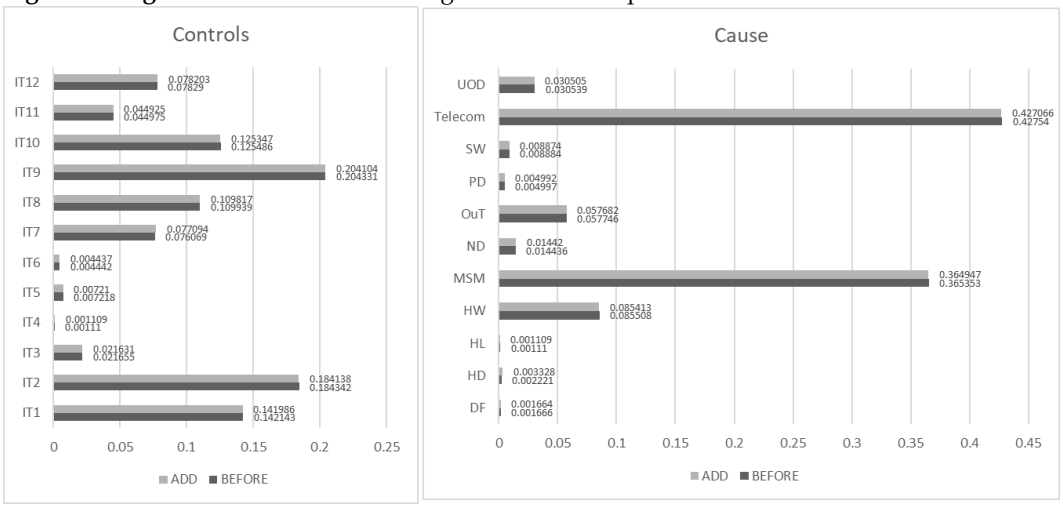

Fig 10 The change in probabilities of the variables for the nodes Controls and Cause – from the original training database (before) and post the addition of 2 rows to simulate the occurrence of 2 hacking events (add) can be presented for quick viewing by the risk managers

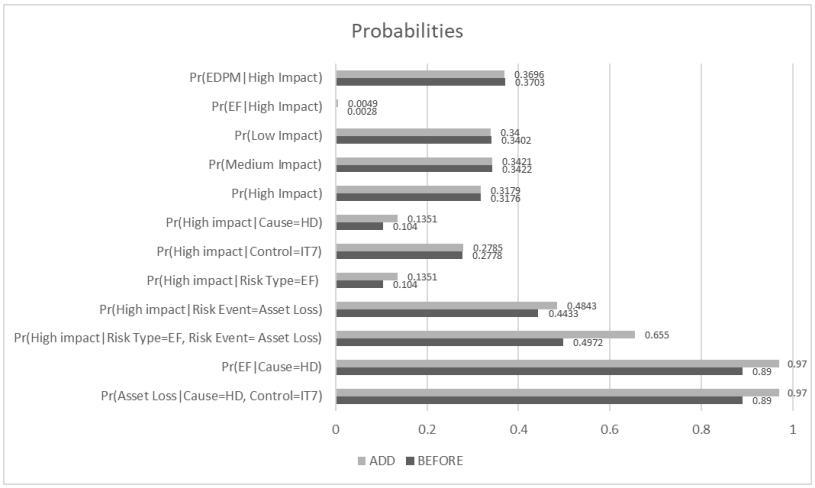

Fig 11 Changes in probabilities of inferences made from the original training database (before) and post the addition of 2 incident rows to simulate the scenario of 2 hacking events (add). This can be presented to senior business managers for an easy understanding of the impact of the scenario.

The change in probabilities resulting from the scenario that was input shows that a risk manager can use the BN modeling for operational risk to evaluate the impact of different incidents or simulate various scenarios to assess the risk implications. The risk manager can discuss the assessment results with senior managers, process owners, and control owners who can allocate resources efficiently by prioritizing mitigation efforts towards causes and controls that have a higher probability of resulting in a high risk impact incident.

4.3. Key Risk Indicator (KRI) development

a. Related to specific risks in a clear and consistent way: As seen in the loss analysis and impact/scenario analysis sections earlier, a risk manager can analyze and identify the key causes and controls to monitor. The structure of the network allows for a clear understanding of the specific risks that could materialize from the causes and controls, allowing for the identification of controls and causes to be monitored via KRIs. By charting the node Controls, as in **Fig** 8, the risk manager can visualize and identify Controls that have a high probability of causing a risk event and therefore require to be monitored. These controls can be identified as candidates for which KRIs should be designed for monitoring purposes. The scenario analysis also allows for defining KRIs. As we added 2 incidents to simulate HD (hacking damage), both high risk incidents, inference has shown the change in the probabilities of a High impact risk caused by HD or by the risk type EF. A risk manager using such simulation and scenario analysis can assess the implications of control weakness and include the specific control for KRI monitoring.

b. For high risks identified - develop KRIs: With the evidence set to evaluate the probabilities only for risk impact = High, the risk manager can get better insight into the causes and controls that require monitoring. They can, therefore,

develop KRIs that allow for the effective monitoring of indicators that have a high probability of resulting in a high risk event. When plotted, as shown in ***Fig** 12*, the risk manager can see the relation between high impact risk events, the controls associated with them, and the probabilities. A risk manager looking at the charts in ***Fig** 12* (a) can see that the risk event TD, in risk type BDSF, has a higher probability of resulting in a high impact risk event. Further, the risk manager can relate this with ***Fig** 12* (b) and understand the controls related to TD, that have a higher probability of failing (IT9, IT2). These controls can be then considered for the definition of KRIs.

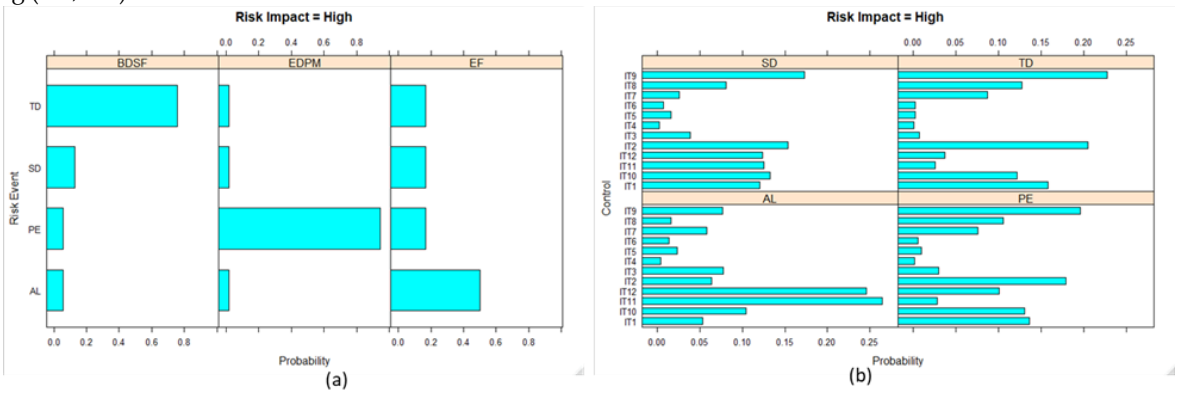

Fig 12 Probabilities for the BN when the evidence is set to risk impact = High (a) Probability of Risk Event conditional Risk Type (b) Probabilities of the controls when the risk impact is high

4.4Risk assessment

Can the risk manager and other operational managers get information that could be used in RCSA?

a. Assessing the probability of a given risk event given the failure of control and presence of a causal factor: The ability of a risk manager to query the BN, providing some criteria, allows for the assessment of probabilities for use in the RCSA process. A risk manager looking to answer the question of 'what is the probability of an asset loss risk event, given that there was a given causal factor and failure of relevant the control, would be able to query the BN providing these criteria and determine the conditional probability. They could further determine the probability of a High impact risk happening given an asset loss risk event occurring.

b. Assessing the probability of a risk type: The risk manager can also further query the BN to determine the probability of the various risk events happening.

c. Assessment of control effectiveness: The risk manager can determine the control effectiveness from the control node providing information on the probabilities of the controls failing and causing a risk event. This information can be an input for the RCSA process. The BN allows for further assessment of the implications of the control being ineffective. We can assess the impact of a failed control– through the propagation to the nodes risk event, risk type, and risk type.

4.5. Risk Reporting

Does the model allow for risk information to be communicated in a manner that would cater to different senior managers and risk managers?

a) Allow senior managers to prioritize their risk remediation efforts

b) Be aware of the risk types and the probability of the risk impact per impact type

For purposes of this paper, we have not explored or extensively used the various visualization capabilities available currently, given the focus is on how the BN structure and the probabilities learned can be used for ORM. The analysis earlier shows how the structure and the parameter learned can give us much insight into the key controls, causes, risk event types, and the impact. These allow us to measure the operational risk exposure and also present them either as KRIs or an overview of the probabilities of the risk events and risk types occurring. This information caters to different groups of senior managers. Operational or line managers can view the risk events that have the highest probability of occurring. They are then in a position to work with the risk manager to understand better the specific control and causal factors related to their area, those on which they need to prioritize their remediation efforts. Process owners are also able to better manage their process by gaining visibility into the controls that have a higher probability of causing a risk event and then prioritize their remediation efforts there. KRI focused on these areas will help them efficiently manage this risk while understanding the alignment with the risk event and the risk type. ***Fig** 13* shows a set of sample charts to illustrate how information elicited from the BN can be used for risk reporting purposes - (a) shows the risk impact conditional on the risk event and the risk type –managers through a visualization of the information can quickly know what they should be focusing on; (b) is a plot of the risk type against risk impact (y-axis) and frequency/likelihood (x-axis) – aggregated risk information can be presented in reporting to senior managers. Senior managers, who typically require aggregated risk information, can look at the charts focusing on the high-frequency area of the chart and learn the risk areas to prioritize the bank's remediation efforts.

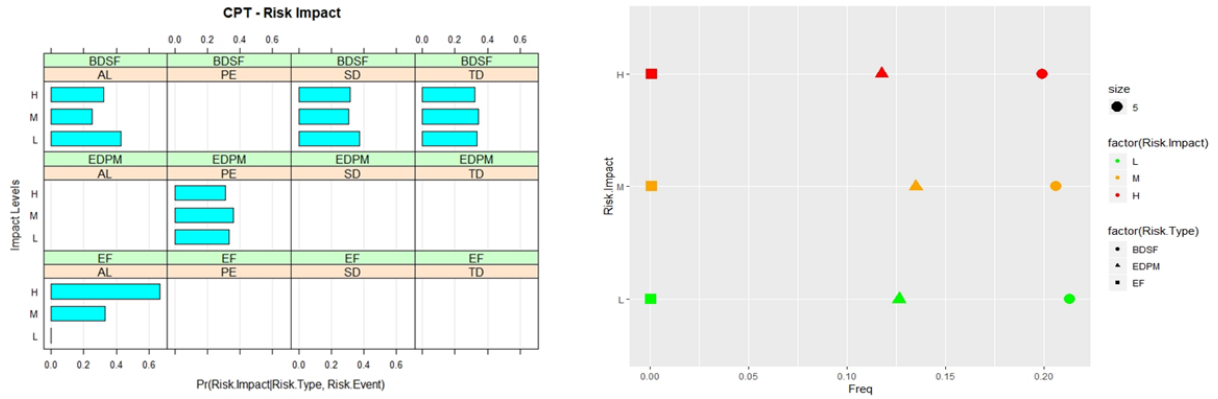

Fig 13 Set of sample charts illustrating risk reporting using inferences from the BN (a) shows the risk impact conditional on the risk event and the risk type – allowing managers to quickly visualize the area they need to focus on; (b) is a plot of the risk type against risk impact (y-axis) and frequency/likelihood (x-axis) – allowing senior managers to look at risk aggregated at a risk type, and prioritize efforts on the high frequency – high impact area of the chart.

Senior management for a business unit can receive communication at a higher level of the risk type and the probability of a high risk event happening in either of these risk types. The aggregation of the risk at a risk type level does provide consistency within the organization. They can then allocate resources to the area that is of more concern either from a risk type or if required the underlying risk event to bring the probability of a high risk event within the risk appetite defined.

V. CONCLUSION

ORM should be seen as a structured process and not viewed as a set of disjointed tasks. Educated risk management decisions can be better taken when the framework allows for integrated risk and control information [34]. The use of a BN provides such a model that allows for the integration of risk and control information to be delivered in a structured process. PGM supports a data-driven approach to model construction that is very effective [13].

In this paper, we have used the R package bnlearn to construct BNs using a simulated database of risk information. We have focused our research here purely on discrete variables, avoiding distributions, manually constructing the structure to be more custom and appropriate for the domain – which is a significant advantage in the use of BN. The parameter of the structure was subsequently learned. Through the inference capabilities – both approximation and exact inference – we have shown how meaningful risk information can be elicited from the BN and applied for effective risk management.

We have shown that through learning a BN model, a risk manager can enhance their ability to measure, monitor, and communicate risk information in a manner that enables a business manager to make risk-informed decisions. While BNs have been used to measure operational risk for capital calculation (VaR, loss distributions) and in better analyzing the risks in specific process areas, we have shown that machine learning BN models can significantly enable effective "business-as-usual" management of operational risks. They can be adopted and adapted to deliver 'risk intelligence' for business managers to effectively manage operational risk on a day-to-day basis. Risk managers following this approach can enhance their current operational risk management techniques such as loss analysis, scenario analysis, KRI design and risk reporting.

Further, this method of modeling for ORM provides direction for further research in ORM. While in this paper, we have shown how BN learned from loss/incident data can be used in risk management, we can extend this research. BNs initially learned from backward-looking information (incidents) can be supplemented with forward-looking expert opinion (RCSA) for the better management of operational risk. The use of the BN learning process can also be applied to address challenges related to aggregation of operational risks within an enterprise. These will significantly benefit the risk managers in communicating actionable 'risk intelligence' to business managers for managing enterprise risk.

REFERENCES

[1] Basel Committee on Banking Supervision 2011 Principles for the Sound Management of Operational Risk *Bank Int. Settlements* 1–27

[2] Leo M, Sharma S and Maddulety K 2019 Machine Learning in Banking Risk Management: A Literature Review *Risks***7** 29

[3] Yasuda Y 2003 Application of Bayesian Inference to Operational Risk Management

[4] Pergler M and Freeman A 2008 *Probabilistic modeling as an exploratory decision-making tool*

[5] Epstein M J and Buhovac A R 2006 *The reporting of organizational risks for internal and external decision making* (CMA Canada)

[6] Pernkopf F, Peharz R and Tschiatschek S 2014 Introduction to Probabilistic Graphical Models *Academic Press Library in Signal Processing* vol 1 (Elsevier) pp 989–1064

[7] Figini S, Gao L and Giudici P 2015 Bayesian operational risk models *J. Oper. Risk***10** 45–60

[8] Svensson K P 2015 A Bayesian Approach to Modeling Operational Risk When Data is Scarce .

[9] Sanford A and Moosa I 2015 Operational risk modelling and organizational learning in structured finance operations: A Bayesian network approach *J. Oper. Res. Soc.***66** 86–115

[10] Ibrahimovic S and Franke U 2017 A probabilistic approach to IT risk management in the Basel regulatory framework: A case study *J. Financ. Regul. Compliance***25** 176–95

[11] Bart V L 2017 Machine learning: A revolution in risk management and compliance? *J. Financ. Transform.***45** 60–7

[12] Jordan M 2003 Conditional Independence and Factorization *An introduction to probabilistic graphical models*

[13] Koller D and Friedman N 2009 *Probabilistic graphical models : principles and techniques*

[14] Bidyuk P I, Terent'Ev A N and Gasanov A S 2005 Construction And Methods Of Learning Of Bayesian Networks *Cybern. Syst. Anal.***41** 587–99

[15] Ben-Gal I 2008 Bayesian Networks *Encyclopedia of Statistics in Quality and Reliability* (Chichester, UK: John Wiley & Sons, Ltd)

[16] Margaritis D 2003 *Learning Bayesian Network Model Structure from Data*

[17] Fenton N and Neil M 2007 Managing Risk in the Modern World *Appl. Bayesian Networks*

[18] Dalla Valle L 2009 Bayesian copulae distributions, with application to operational risk management *Methodol. Comput. Appl. Probab.***11** 95–115

[19] Peters G W, Shevchenko P V. and Wüthrich M V. 2009 Dynamic operational risk: modeling dependence and combining different sources of information **4** 69–105

[20] Neil M, Marquez D and Fenton N 2008 Using Bayesian networks to model the operational risk to information technology infrastructure in financial institutions *J. Financ. Transform.***22** 131–8

[21] Alexander C 2000 Bayesian Methods for Measuring Operational Risk *SSRN Electron. J.***44** 1–15

[22] Cowell R G, Verrall R J and Yoon Y K 2007 Modeling Operational Risk With Bayesian Networks *J. Risk Insur.***74** 795–827

[23] Shevchenko P V. and Wüthrich M V. 2006 The Structural Modelling of Operational Risk via Bayesian inference: Combining Loss Data with Expert Opinions *J. Oper. Risk***1** 3–26

[24] Aquaro V, Bardoscia M, Bellotti R, Consiglio A, Carlo F De and Ferri G 2010 A Bayesian Networks approach to Operational Risk *Phys. A Stat. Mech. its Appl.***389** 1721–8

[25] Alexander C 2000 Bayesian Methods for Measuring Operational Risk *Ssrn* 1–15

[26] Fenton N and Neil M 2011 The use of Bayes and causal modelling in decision making, uncertainty and risk *Risk Inf. Manag. Res. Gr.* 1–19

[27] Neil M, Häger D and Andersen L 2016 Modeling operational risk in financial institutions using hybrid dynamic Bayesian networks *J. Oper. Risk***4** 3–33

[28] Awad M and Khanna R 2015 *Machine Learning in Action: Examples*

[29] Shalev-Shwartz S and Ben-David S 2014 *Understanding Machine Learning: From Theory to Algorithms*

[30] Scutari M and Denis J-B 2015 *Bayesian networks : with examples in R* (CRC Press)

[31] Scutari M 2010 Learning Bayesian Networks with bnlearn R package *J. Stat. Softw.***35**

[32] Nagarajan R, Scutari M and Lèbre S 2013 *Bayesian networks in R : with applications in systems biology* (Springer)

[33] Fenton N E and Neil M (Martin D . 2013 *Risk assessment and decision analysis with bayesian networks* (CRC Press)

[34] Samad-Khan A 2008 Modern operational risk management *Emphasis***2** 26–9