

Operational Risk Control of Commercial Banks based on Bayesian Network

Xiaoling Hao^{1,2 a}

¹School of Information Management and Engineering, Shanghai University of Finance and Economics, Shanghai, 200433, China

² Key Laboratory of Financial Information Technology of Shanghai, Shanghai, 200433, China

^aemail: haoxiaolingsh@163.com

Keywords: Bayesian network; operational risk control; event tree

Abstract. Commercial banks are facing challenges in operational risk management, with the occurrence of major events of Bahrain bank and other events on the banks. Most studies have concentrated on how to measure operational risk loss based on the new Basel Capital Accord and focus on mathematic and statistical method to accurately calculate the capital charge. However, studies on how to control and reduce the affect of operational risk are relatively scarce. Therefore, it is feasible and sensible to deepen the study of root cause of operational risk and find effective control methods, which can provide meaningful result in the future. In this paper, the risk events are presented with event tree; then the event tree is transformed into the Bayesian network. Next, loss probability of each node is estimated according to the Bayesian network structure. Finally, the specific control scheme is put forward to achieve the desired control effect.

Introduction

Because of China's development in the field of operational risk management of commercial banks is relatively new, banks generally lack the awareness and effective framework on operational risk management. For Chinese commercial banks, it is necessary to establish valid models and methods of operational risk management in order to effectively reduce the operational risk and get the core competitiveness.

Due to the complexity of operational risk, we first describe the risk event in form of event tree, according to the probability of risk arising from the process nodes. According to the transformation principle of event tree to the Bayesian network, we classify the risks in the event tree, and summarize four kinds of operation risk model framework. Then we add the nodes of risk control to each kind of risk model. So, operational risk loss distribution can be estimated according to the distribution of risk probability of different nodes. Next, we can exert reasonable control of each node according to the existing Bayesian network structure. According to the desired control effect, specific control scheme is proposed for each risk model, so as to achieve the overall operational risk control effect.

In empirical study, we collect the loss data of operational risk of 20 commercial banks in recent years, and classify the risks into four types, and calculate the probability of operational risks of each type. Then the data is imported into Bayesian network, through the study of the loss distribution of operational risk originated from several risk factors, we can make a rational control scheme to eliminate or reduce the risk. Finally, the allocation of capital can be made according to the trade-off between the control cost and risk event loss.

Generally, the operator should first present the operational risk in the form of the event trees, then the researchers can converted them to the form of Bayesian networks, in order to aggregate calculations based on existing data. As the probability distribution of each node corresponds to a Bayesian network can be analyzed, the current risk of loss distribution can be known. Reasonable control, then in accordance with the reserved capital for each module on the risk of resistance in the Bayesian network system can be put out. For instance, re-allocate the probability of operational risk,

in order to get a more appropriate operational risk management method.

Operational Risk Control Model

In this paper, we put forward an operational risk control model which combines the event tree with the Bayesian network. The advantages of such operational risk management are as follows: By event tree we can get a clearer understanding of the layout of the operational risk; and Bayesian network model shows a very scientific distribution of the available data, and can produce a more reasonable and convenient management method based on specific situation [1].

A. Event Tree Analysis of operational risk

Event tree analysis (Event Tree Analysis, referred to as ETA) originated in the decision tree analysis (DTA), is a method for identification of root cause through the inference of possible consequences from the initial event [2]. An accident is a collection of many events; these events have logic relationship such as causality and sequence, which can form an event tree. This event tree like a flow chart, can express the relations among events more clearly. Because the event tree is simple and can be used in a wide range of areas, so it can be used in the framework of Bayesian network structure model. The form of event tree is like figure 1.

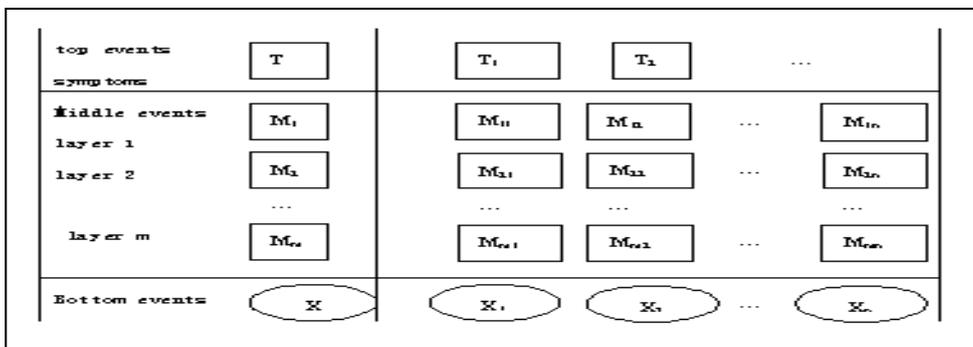


Fig.1. Event tree analysis

B. Transformation from Event tree to Bayesian network

Event tree and the Bayesian network are two complementary operational risk management methods; we should pay attention to the relationship between the events during the transformation process to make sure not to change the logic. The transformation from event tree into the Bayesian network can be carried out according to the following steps:

Step 1: number each event involved in event tree, and map it into the Bayesian network according to the logical relationship.

Step 2: analyze the status of each node.

Step 3: determine the topological structure of the Bayesian network according to the logic relation between nodes.

Step 4: determine the probability table of each node according to the topology structure.

C. Decomposition and combination Bayesian network

Different risk source may cause a variety of losses, but most loss can be classified, for example, transaction events can be classified into internal source and external source, it is also the two kinds of risk source that cause all transaction failure, so this two kinds of failure jointly build a Bayesian network, which simplifies the operational risk control and measurement. Meanwhile, the same risk may also cause different loss, so it is necessary to make proper decomposition for too complex event tree. The combination principle is as follows:

Sub Bayesian network is independent of each other. Each sub network should have certain loss results, these losses can be classified.

The initial node should be independent of each other, so as to construct Bayesian network to ensure that they can combine together to form a public Bayesian network.

Bayesian network is designed to classify the same type of loss events to achieve more effective

control. It not only can more clearly analyze the distribution of risk, but also can be more effective in exerting control for the same operational risk types.

Empirical study

A. Data Collection

Since there is rarely official statistic data about operational risk of commercial banks in China, our understanding of operational risk is mainly through the collection of public reported cases, from 2000 to 2009. Although occurrence of these operational risk cases is scattered and random, covering various types of state-owned banks, joint-stock banks and city banks, it is still meaningful to do the statistical analysis.

Based on the data obtained, and according to the risk type (4 types of risk) and business line (7 kinds of business line) of banks, we make a classification for the operation risk events according to the reasons for the loss [3]. Here all the loss is mainly classified into four categories, including internal processes of institutional factors, internal bank staff factors, external event factors and system factors, which cover the risk control environment. Therefore, the probability of the each factor can be obtained according to the loss data of the cases, as shown in table1.

Tab.1. Probability table of four kinds of risk.

| Loss type | Risk Factors | | | |
|------------|---------------|-------------|-----------------|-----------|
| | Inner process | Staff | External events | System |
| Loss value | 1145740.452 | 1584906.018 | 957911.9 | 14037.321 |
| happen | 0.3094 | 0.4281 | 0.2587 | 0.0038 |
| not | 0.6906 | 0.5719 | 0.7413 | 0.9962 |

B. Initial variable selection

Bayesian network is relatively weak to control events with small probability, so we omit the loss whose probability is less than 0.1 %. For example, in internal processes, risk loss caused by institutional factors, product defects by banks, bank, business disputes and transaction pricing errors is quite small; the loss accounts for a very small proportion in entire internal process factors, therefore these nodes may be omitted. Then we get final Bayesian network diagram of the initial variable. As shown in table 2.

Tab.2. Set of initial nodes of bayesian network

| Causes of Category | Initial node |
|-------------------------------|--------------------------------------------------------|
| Factors of internal processes | Violation of the rules, regulations and fiduciary duty |
| | Unfair business and market behavior |
| | Unauthorized authorization |
| | Error monitoring and reporting |
| | Customer information and account management |
| Staff factors | Internal fraud |
| | Internal theft |
| | Corruption and bribery |
| | Crime of money laundering |
| External events factors | Disaster / sudden event |
| | External fraud |
| | External theft |
| | Industry disputes |
| The system factors | System failure |
| | System vulnerabilities defects |

These initial variables must be independent of each other according to the requirements of the

Bayesian network. In fact, the losses caused by some nodes are interrelated, such as violation of rules and regulations and fiduciary duty, unfair business and market behavior and error monitoring report; they are all caused by the bank's internal subjective behavior of employees. Therefore, in order to better control these nodes, it is necessary to introduce a new intermediate variable node.

C. Intermediate variable selection

Probability distribution of intermediate variables can be calculated according to the data classification. The selection of the state is set according to the number of occurrences and frequency of events in the case. It is found that the loss of the event can be roughly divided into third grades: not more than ten million, not less than 100 million, and in between.

Intermediate variable selection is based on the attribution of the initial nodes, such as intermediate variable staff factors in the internal processes is a violation of the rules and regulations and fiduciary duty, unfair business and market behavior, and error monitoring and reporting together to form, so the losses of this intermediate node are caused by the three common causes of R03, R04 and R06. Like this, we make a reasonable classification according to the situation of the whole data set. The intermediate variable node of the operational risk loss probability is shown in figure 2.

D. Construct of Bayesian network diagram

According to the logic relationship of required initial node (ie, the key risk points) and intermediate nodes, we can build up the structure of the Bayesian network. Since the Bayesian network is not sensitive to node with small probability, we delete the node whose probability is less than 0.1%. Thereby we obtain a Bayesian network structure of the bank's overall operational risk, which is shown in Figure 2.

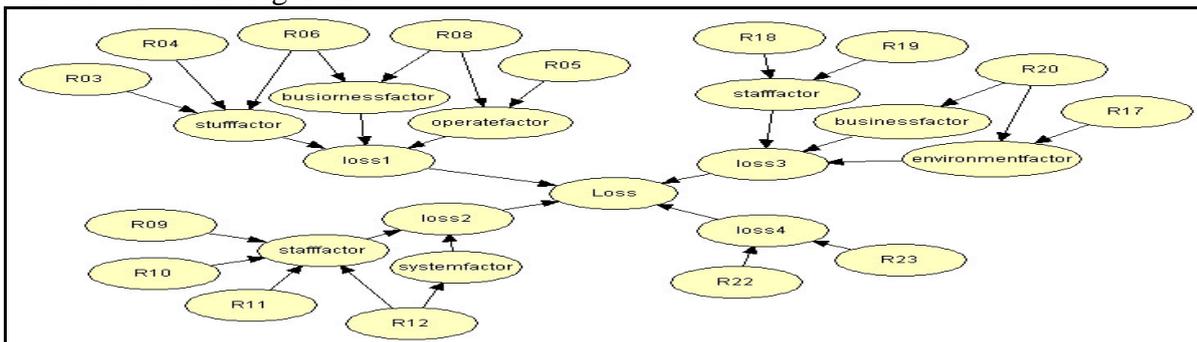


Fig.2. Structure of Bayesian network

Simulation of Bayesian Network

The probability table above is the basic components of a Bayesian network, Bayesian network structure is automatically generated by software HuginLite7.6. We can see the probability distribution of each node through the layout of the node monitoring table [4], as shown in Figure 3.

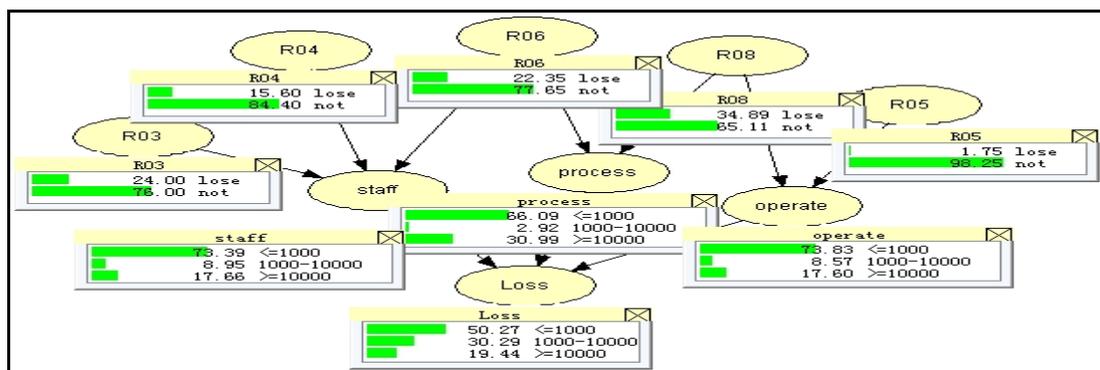


Fig.3. Node monitoring diagram

The whole structure is decided by four factors of operational risk classification, and every kind of factors is summarized into the total loss. The overall structure of Bayesian network graph can clearly show the distribution of operational risk, but the structure is too complex, the existing HuginLite version is limited in the structure of network nodes and the state, so we divide the whole network apart, and in this way we can study the conduction process and control measures for each kind of operation risk, and can flexibly control according to the causes of the four categories.

Operational risk Control management of Bayesian network nodes

With Bayesian network structure, we can assign a value to each node, thereby obtaining the final loss situation. Vice versa, we can assign the value to final node according to the overall desired control results, thereby obtaining the probability distribution of the initial node [5].

If we want to get the final loss not more than 10 million, we must first ensure that the minimum requirements for each of the key risk points. Probability of R03 node shows that the proportion of violation of rules and regulations and the fiduciary duty shall not exceed 18.43% in the internal processes, which should reduce 5.57% from 24% of the initial. R05 means that, the proportion of loss due to violation of the authorization should not be higher than 1.54% in internal processes, a 0.21% lower than the initial 1.75%. R06, error monitoring and reporting the loss probability should be 0.5%, 11.85 % lower than the initial 22.35%. R08 means the loss rate due to account management misuse should decrease from 34.89% to 12.87%, a 22.02% decrease. In contrast, R04 means unfair business loss probability can be relaxed from the initial 15.6% to 16.26%, an increase of 0.66%. This means, under the same capital requirement, we can relatively relax the control on R4, while put more capital and effort to other areas such as R08, R06, which needs more control effort to drop down the probability. The case is shown in figure 4.

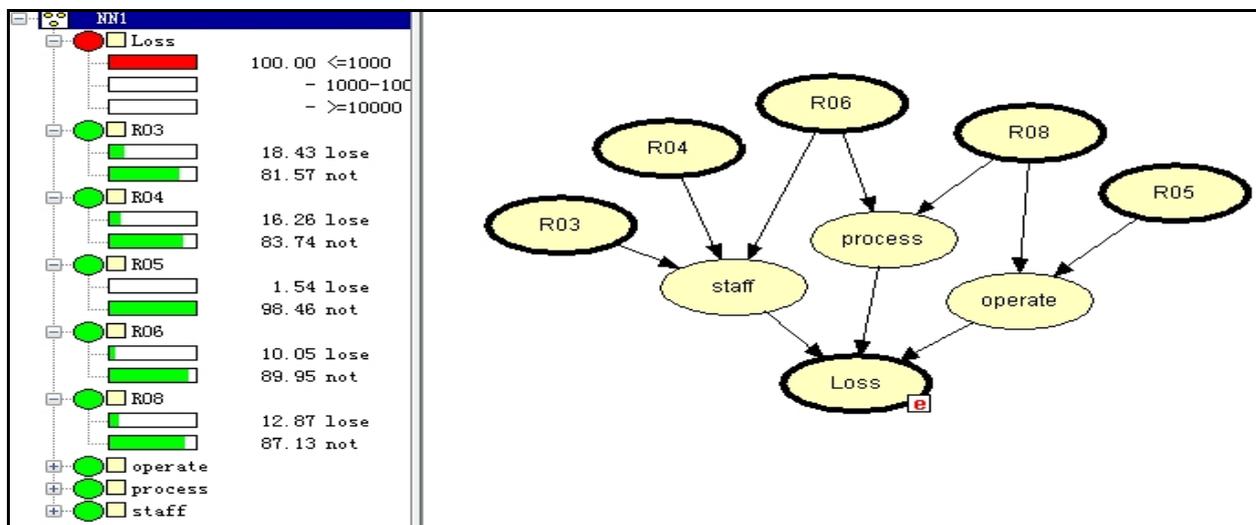


Fig.4. Bayesian model diagram of the internal flow control

In order to make a reasonable allocation of internal control resources, we have to integrate several sub-Bayesian networks and make a comprehensive diagram analysis. The sub Bayesian network node can form a new a new Bayesian network. As shown in figure 5.

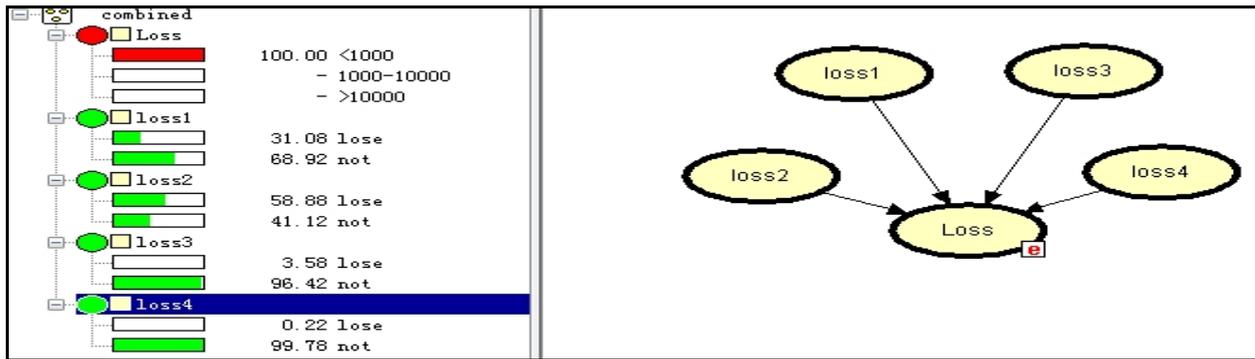


Fig.5.Comprehensive loss control based on Bayesian network model

It can be seen from figure, if we want to let the total loss caused by operational risk keep at a relatively low level, for instance, not greater than ten million, then the proportion of internal processes caused by system factors loss must be below 31.08%; the loss caused by internal bank staff factors below 58.88%; loss caused by external events below 3.58%; the risk of loss resulting from the system error is reduced to less than 0.22%. This analysis gives quantitative analysis to support the decision make to adopt concrete control measures to realize the desired risk level.

Conclusion

In this study, a new and effective method is presented to control of operational risk with Bayesian Network. First, we establish the operational risk event tree, which demonstrate the risk sources originated from the internal process of institutional factors, bank staff factors, External factors as well as System factors. Second, we established the transformation mechanism from event tree to the of Bayesian network, with which operational risks of same type are merging into the network nodes. Third, we constructed the operational risk control model based on Bayesian network. Four types of operational risk are estimated respectively with operational risk control module, which simplified the operational risk classification and control process and reach desired control effect. Finally, we use empirical cases to apply this model and the results show that the model is effective and practical.

Acknowledgment

This work was supported in part by Shanghai Natural Science Foundation (Grant No 11ZR1411900), and National Science Foundation of China (Grant No 61003022 and 71001058), the fourth phase of 211 key project funds of Shanghai University of Finance and Economics.

References

- [1] H. M. Chai, B.S.Wang, Research on the Bayesian networks model in situation assessment[J]. Journal of Xidian University, 2003, 36(3):491-495.
- [2] C. Supatgiat, C. Kenyon, L. Heusler. Cause-to-Effect Operational-Risk Quantification and Management[J],Risk Management, 2006, 8(1):16-42.
- [3] D.Dominik, Lambrigger,P. V. Shevchenko,M.V.Wüthrich. The Quantification of Operational Risk using Internal Data, Relevant External Data and Expert Opinions[J],Journal of Operational Risk. 2007, 2: 3-27.
- [4] G. W. Peters,S. A. Sisso. Bayesian inference, Monte Carlo sampling and operational risk[J],Journal of Operational Risk, 2006,1(3): 27-50.
- [5] M.Neil, N.Fenton, M.Tailor, Using Bayesian Networks to Model Expected and Unexpected Operational Losses[J], Risk Analysis, 2005,25(4):963-972