Towards a Value Model for Collaborative, Business Intelligence-supported Risk Assessment

Lingzhe Liu[1] and Hennie Daniels[1, 2]

{lliu,hdaniels}@rsm.nl

[1]Erasmus University, Rotterdam, The Netherlands
[2]Tilburg University, Tilburg, The Netherlands

Abstract. Collaborative business intelligence supports risk assessment and in return enhances management control on a business network. Nonetheless, it needs an incentive basis in the first place before it can be implemented, that is, the value model. Starting from the managerial challenges which arise from the needs of collaboration, we analyzed the three tiers of risk assessment in the integrated perspectives of GRC. We then identified two forms of collaborative BI, which can be applied to risk assessment. The concrete incentive scheme for the collaboration requires future research.

Keywords: Business Intelligence, Business Network, Risk Assessment, Management Control, Collaboration.

1 Introduction

Risk assessment in business network (BN) is a collaborative effort. In a BN, decision made in a member organization influences, and can be influenced by those in other organizations. Such dependency inevitably binds the management control efforts of partner organizations together. E.g., the focal organization would like to control its business process according to its customer's compliance requirement, so as to offer value-adding service beyond the value of the products or business service output. This further leads to the need for collaborative planning and management control on both strategic and operational levels, in the integrated perspective of Governance, Risk Management, and Compliance (GRC) [5].

Business intelligence technology (BI) is playing a fundamental role in supporting decision-making and risk management in business organizations. It provides visibility to managers on the status and performance of the organization, enabling proper management control.

Business network as a form of operation organization proposes new challenges for risk management and at the same time for the BI application. Here lists three of these challenges. First, the collaborative management needs intelligence from both internal and external sources, that is, collaborative BI [3] needs information sharing across organization borders. Second, as mission critical and decision-sensitive information

needs to be shared online, security issues often become a problem (if not a prohibiter) for expanding management visibility over the network [4]. Unless a proper solution be in place that out-weight collective benefit against potential information leak, organizations would have insufficient incentive to share information electronically. Last and rather importantly, management on the quality of shared information [1] also becomes more challenging, because the quality of BI analysis result is bounded by the quality of input data, and because external control power is weaker in general to ensure data quality.

This research-in-progress paper set off to address the aforementioned challenges. We work towards the development of an incentive scheme for collaborative risk management in a networked organization. The research questions are: 1) what are the incentives for partner organizations to share information for collaborative risk management, 2) what are the incentives for them to control the quality of the shared information. In session 2 we discuss the risk factors that can be assessed with BI and the situations of GRC in a networked organization where BI can be devised to enhance control. In session 3 we identify two forms of collaboration, whose value models need further research. Session 4 concludes the paper with notes on planned future works.

2 Collaborative Risk Assessment

2.1 The Risk Assessment in a Networked Organization

A global management control for a networked organization requires the integrated GRC approach, as both internal and external control on both the organization and the network level are involved. Control is for assuring achievement of the organization's own objectives, so it needs to align the behaviors of its sub-organizations' as well as its partners'. Meanwhile, as a member of the network, it must also make sure its own behavior complies with external norms and regulations.

Regarding each member organization an intelligent agent who makes rational decisions, inter-organizational cooperation and external control is based on trust. The risk assessment in a networked organization is in fact the assessment on the "trustworthiness" of an organization, in lights of accounting theory, i.e. whether the organization under question has enough capability in controlling its operations so that the uncertainty of deviation is contained within certain level. Thus, risk assessment is the auditing analysis on the focal organization itself and on its partners, and the assessment has to be done on three tiers:

1. Operations tier: assessing the risk level of the business operation (in the *controlled* system), according to operations standards.
2. Compliance tier: assessing the risk level of the management system (or, the *controlling* system), i.e. its capability to align the operations with regulations
3. Governance tier: assessing the risk level of the configuration of the business network (the value constellation, or *incentive scheme*), with criteria of how well the design of management system in each member implements its business model, and

how likely the misalignment between objectives of a member organization and the network leads to a non-cooperative behavior [4].

Provided that operations data is shared among the members, risky events and impacts on the first tier can be directly measured and assessed. The second tier assessment may be done by internal or external auditors, although external audit is sometimes required by law. BI could lend support to these two assessments with its analytical power. The third tier assessment can be simulated [4] for designing the incentive scheme on the phase of partner selection and partnership establishment, but it remains an open question how it can be done analytically with BI. As to the assessment result, first and second tier result may be shared only when there is a high level of business partnership or the other partner has a strong marketing power. The third tier result would be used internally for risk assessment and would not be shared at all. Yet this knowledge is a rather important basis for an organization to cooperate with partners.

2.2 Assuring the Quality of Input Information

To a large extent, the quality of the shared data can only be managed by the data owner. A partner would not share the data, in the first place, unless it gets something of the same value in return, basing on economy reciprocity. For instance, a partner may be benefited from the risk assessment on the complete set of shared data which are contributed collectively by all partners in the network, and thereby it is willing to add data to the collective data set. The reciprocity principle is the key for resolving the problems of data sharing and information quality.

Information quality can be a risk source itself that subjects to assessment. The quantitative assessment can be done on the first and second tier, on the capability of the data provider for the quality assurance. Alternatively, the qualitative assessment may find some indicator from third party reference: if a trusted partner uses the same shared information for analysing its own risk, this information is reliable and reusable for other partners in the BN to do their risk analysis. To further generalize this idea, if a partner has motivation to provide certain information in order to achieve some goal and to benefit from or to be responsible for the result, then, this piece of information should be trustworthily reliable.

3 Towards a Value Model for Collaborative Risk Assessment

Collaborative BI combines business data from multiple partners, making it possible to discover patterns on the network level that cannot be seen with the internal BI in individual organizations, e.g. capturing weak signals [5]. Moreover, linking partners' data is a prerequisite for establishing traceability of operations events [2], which is necessary for automatic risk analysis, e.g. on cause-effect relations.

At least two forms of collaboration can be identified. The first form is to share data horizontally with organizations (competitors) for the same purpose of analysis and to

benefit from the completeness of the data set. The inter-organizational information system FISH[1] is an example. FISH plays an important role in fraud detection and fraud prevention. Each insurance company participated in FISH is obliged to send relevant information about claims to FISH and in turn gets the right to extract information from FISH. This helps companies to discover suspicious claims by direct inspection of the FISH database. By means of the application of business intelligence and business analytics techniques companies can also get a better insight in high risk profiles.

The second form is vertical cooperation with business partners in the same value chain, e.g. supply chain, dealing with the risk stemming from the lack of visibility in inter-organization operation, besides other domain specific risks. Because of the various roles, responsibilities and liabilities, value model in this form of collaboration become rather complex, as partners may be tightly coupled in business process but loosely coupled in data sharing, e.g. in the case of cooperating with a partner with whom the focal organization do not have a bilateral relationship. In this setting, the value models for all three tiers of assessment (see session 2.1) must be consistent to one another. Compliance is the gluing element here, as it implements the requirement of BN governance (controlling non-compliance behavior) on one hand, and bolsters inter-organizational cooperation (monitoring [external] risks according to [shared] business rules or operations standards) on the other. The common ground for the cooperation is the shared risk profile (business rules). In this way, when the risk source lies in its partner's operations, the focal organization could out-source the risk management to the partner, given that the partner is trustworthy and also has sufficient incentive to undertake the task.

Additionally, the incentives for information brokers (who enable the data sharing and who may also provide intelligence as a service for the collaborative risk assessment) is a problematic area and calls for further research, as the information brokers benefit from *invisibility* in the BN which is a basis of its business model.

4 Conclusion and Future Research

Collaborative business intelligence supports risk assessment and in return enhances management control on a business network. Nonetheless, it needs an incentive basis in the first place before it can be implemented, that is, the value model. Starting from the managerial challenges which arise from the needs of collaboration, we analyzed the three tiers of risk assessment in the integrated perspectives of GRC. We then identified two forms of collaborative BI, which can be applied to risk assessment. The concrete incentive scheme for the collaboration requires future research.

[1] http://www.stichtingcis.nl/bc_upload/FISH%20protocol.pdf [Accessed December 5, 2011]

References

1. van Baalen, P. et al.: Port Inter-Organizational Information Systems: Capabilities to Service Global Supply Chains. Foundations and Trends® in Technology, Information and Operations Management. 2, 2-3, 81-241 (2009).

2. Hofman, W.: Supply Chain Visibility with Linked Open Data for Supply Chain Risk Analysis. Workshop on IT Innovations Enabling Seamless and Secure Supply Chains. pp. 20-31 (2011).

3. Rizzi, S.: Collaborative Business Intelligence. In: Aufaure, M.-A. and Zimanyi, E. (eds.) eBISS 2011, LNBIP 96. pp. 186-205 Springer-Verlag Berlin Heidelberg (2012).

4. SecureSCM: WP8 Business Aspects of Secure Computation D8.2 Risk Assessment. (2009).

5. Wiesche, M. et al.: Exploring the Contribution of Information Technology to Governance, Risk Management, and Compliance (GRC) Initiatives. ECIS 2011 Proceedings. (2011).