Internal controls in a network organization

Joris Hulstijn[1]

Tilburg School of Economics and Management

j.hulstijn@uvt.nl

Abstract. Current frameworks for designing and assessing internal controls, such as COBIT and COSO, are focused at the enterprise. However, increasingly companies collaborate in network organizations, such as supply chains, value chains, online platforms, or smart business networks. Current societal challenges such as compliance, cyber security, resilience, supply chain visibility, or sustainability, also demand solutions that operate at the network level, not at the level of individual firms. In this paper, we will review existing frameworks for internal controls, and how they deal with network organizations. Next, we will discuss various challenges at the network level, and derive objectives for something that plays the role of an internal control system, at the network level. We will make initial proposals for design principles to coordinate internal controls at network level. The paper ends with three examples, in order to illustrate the relevance and feasibility of such an approach.

1. Introduction

Companies must demonstrate compliance with rules and regulations. For example, companies publish annual financial accounts, to be accountable to the stakeholders. Companies file tax reports, customs declarations, and all kinds of reports concerning quality or sustainability of production, to enhance consumer trust. Reporting is increasingly based on 'Big data': large amounts of data that need to be collected, processed, analyzed and summarized for different audiences (Chen, Chiang, & Storey, 2012). Ensuring the reliability of such reports takes a lot of effort, sometimes called administrative burden (Tan, Bjørn-Andersen, Klein, & Rukanova, 2011). In particular, data quality is a large concern (Martijn, Hulstijn, & de Bruijne, 2015). Conversely, when government regulators assess the reliability of reports, they have to rely on evidence provided by the company itself. This leads to a paradox: evidence must be collected and evaluated in order to demonstrate compliance, but that evidence is generated by the company and can in principle be manipulated. In general, it is believed that this paradox can be solved by the company implementing *internal controls*: organizational, procedural or technical safe guards which help to ensure that the evidence collected is reliable (COSO, 1992). Consider controls such as data collection immediately at the source, segregation of duties, maintaining an audit trail, access control, baseline security, back-up and retrieval, supervision and monitoring, risk awareness, and management control (Romney & Steinbart, 2015 Ch7-Ch10). In general, those internal controls that are built into information systems and processes are considered to be more reliable, because they are relatively harder to manipulate. Therefore ERP systems play an important role (Mundy & Owen, 2013).

Frameworks for internal control, such as (COSO, 1992, 2004) or (ISACA, 2012) are mostly focused on the enterprise level. This shows in their name: internal controls are meant to strengthen the company, to be able to face external auditors. However, many challenges, which ought to be countered by some sort of internal controls, occur at the network level. For example, during the credit crisis the widespread adoption of Enterprise Risk Management did little to stop or slow down the risks (Power, 2009). Systemic risks were not captured and dealt with. As more and more data are shared among partners, often the data quality depends on external parties. Also challenges like resilience to disruption, safety, cybersecurity and sustainability can only be solved at the network level (Helbing, 2013). These challenges involve sharing of data, shared responsibilities, and standardization issues. The ability to deal with such challenges will also depend on a governance structure and business model that distributes the costs and benefits in such a way to ensure long term collaboration (Hulstijn, Hofman, Zomer, & Tan, 2016), and by availability of inter-organizational systems (IOS) for sharing data across a supply chain (Rukanova, van Stijn, Henriksen, Baida, & Tan, 2009; Suomi, 1988).

The research method of this paper is conceptual. We will analyze the challenges and solutions based on literature. . In particular, we will discuss the fundamental question whether control objectives at a

[1] My views on this topic are inspired by many conversations with Ype van Wijk, whose contributions are gratefully acknowledged.

network level are compositional, and can be fully decomposed into control objectives to be solved at a local level, compare (van Wijk, van Beest, de Bakker, & Wortmann, 2014). We will propose an initial solution, motivated and illustrated by examples from literature. Such a solution would consist of three elements:

- mechanism to decompose a network control objective into local control objectives (in as far as possible), and distribute them among network partners, to be solved by internal controls
- business model, to distribute the benefits and costs of investing in shared internal controls,
- inter-organizational system, for sharing data, both about controls and about primary business.

The paper ends with a discussion on limitations and opportunities for subsequent research.

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly, 36*(4), 1165 - 1188.

COSO. (1992). *Internal Control - Integrated Framework*. Retrieved from

COSO. (2004). *Enterprise Risk Management — Integrated Framework*. Retrieved from

Helbing, D. (2013). Globally networked risks and how to respond. *Nature, 497* 51-59.

Hulstijn, J., Hofman, W., Zomer, G., & Tan, Y.-H. (2016). Towards Trusted Trade-lanes. In H. J. Scholl (Ed.), *Proceedings of 15th IFIP Conference on E-Government (EGOV 2016), Guimarães, Portugal* (Vol. LNCS 9820, pp. 299-311): Springer.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Retrieved from Rolling Meadows, IL

Martijn, N., Hulstijn, J., & de Bruijne, M. L. C. (2015). Determining the effects of data governance on the performance and compliance of enterprises in the logistics and retail sector. In M. Janssen, Mäntymäki, M., Hidders, J., Klievink, B., Lamersdorf, W., Van Loenen, B. & Zuiderwijk, A. (Ed.), *Proceedings of the 14th IFIP Conference on e-Business, e-Services, and e-Society.* (pp. 454-466): Springer.

Mundy, J., & Owen, C. A. (2013). The Use of an ERP System to Facilitate Regulatory Compliance. *Information Systems Management, 30*(3), 182-197.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*, 849–855.

Romney, M. B., & Steinbart, P. J. (2015). *Accounting Information Systems* (13th ed.): Pearson Education.

Rukanova, B., van Stijn, E., Henriksen, H. Z., Baida, Z., & Tan, Y.-H. (2009). Understanding the influence of multiple levels of governments on the development of inter-organizational systems. *European Journal of Information Systems, 18*, 387–408.

Suomi, R. (1988). Inter-organizational information systems as company resources. *Information & Management, 15*(2), 105-112.

Tan, Y. H., Bjørn-Andersen, N., Klein, S., & Rukanova, B. (Eds.). (2011). *Accelerating Global Supply Chains with IT-Innovation*. Berlin: Springer Verlag.

van Wijk, Y. W., van Beest, N. R. T. P., de Bakker, K. F. C., & Wortmann, J. C. (2014). *Assurance in Collaborative ICT-enabled Service Chains*. Paper presented at the 16th International Conference on Enterprise Information Systems, Lisbon.