Towards a Methodology for Designing e-Government Control Procedures

Liu, J.; Baida, Z.S.; Tan, Y.H.

published in
Electronic Government, 6th International Conference, EGOV 2007, Lecture Notes in Computer Science (LNCS 4656)
2007

document version
Publisher's PDF, also known as Version of record

Towards a Methodology for Designing E-Government Control Procedures

Ziv Baida, Jianwei Liu, and Yao-Hua Tan

Free University Amsterdam
Department of Economics and Business Administration, Information Systems Group
ziv@baida.nl, {jliu,ytan}@feweb.vu.nl

Abstract. The EU is currently modernizing customs legislation and practices. Main pillars in the new vision are an intensive use of IT (Customs becomes e-Customs), partnerships between Customs administrations and businesses (G2B), and collaboration between national Customs administrations (G2G). But how to design new customs control procedures? Very little theory exists, and an inspection of current procedures shows that they are vulnerable to fraud, and thus badly designed. Therefore we identify a need for developing theory for the design of government control procedures. Some research has been done on designing inter-organizational controls in B2B transactions. In this paper we argue that with certain modifications control principles used in B2B are also suitable for the Government-to-Business context, and we present a conceptual model for designing government controls in G2B, based on earlier work of Bons. We use a study on customs procedures for the export of agricultural goods from the EU to Russia as a proof of concept.

Keywords: e-Customs, e-Government, G2B, design methodology, conceptual modeling, procedure redesign.

1 Introduction

Globalization, growing trade volumes and an increased threat of terrorism are main drivers behind the understanding that new customs procedures and legislation are required. National governments and the World Customs Organization (WCO) recognize this reality and set a new vision for modern customs, including a shift in roles, responsibilities and underlying assumptions. Within this shift, the EU is currently reshaping its customs legislation and practices. Main pillars in the new vision are intensive use of IT (Customs becomes e-Customs), partnerships between customs administrations and businesses, and collaboration between national customs administrations. These concepts help cope with the dilemma of on the one hand increasing security, safety, financial and health requirements, and on the other hand a need to reduce administrative burden, to keep the EU a competitive economic zone.

While a lot of focus is put on the strategic vision behind new customs procedures, it is important to bear in mind the operational goals of customs control, which must be achieved by new customs procedures. To this end, existing theory on controls should

M.A. Wimmer, H.J. Scholl, and A. Grönlund (Eds.): EGOV 2007, LNCS 4656, pp. 56–67, 2007.

be applied when designing new customs controls. This is currently not being done: we investigated two European customs control procedures and found that they do not adhere to basic control principles, and hence they fail to achieve their control goals [13, 14]. Control in a government context is more than a safeguard of monetary value; it aims to protect the public interest, including security, health and political stability. Therefore we identify the need to establish sound theory to support domain experts in designing government controls. The theory should formulate principles for the design of government control, and a systematic, methodological application of these principles. Ideally, the theory should be supported by decision support software tools. A pre-requisite for building such tools is that theory is described (semi)formally in conceptual models.

Customs controls are governmental controls that apply to international supply chains, and hence to inter-organizational settings. While a wealth of research exists on *internal* control [e.g., 16, 18], only limited academic work on *inter-organizational* control (IOC) is available. In particular, Bons et al. argue that the same principles used for internal control can be used also for inter-organizational control [5, 6, 7]. Our earlier work [13, 14] supports this claim and presents first steps in a theory for designing and analyzing government controls.

In the current paper we continue these efforts and we present a number of contributions to existing knowledge. First, we develop control principles for G2B (Government-to-Business) and argue that they are a variation of B2B (Business-to-Business) control principles. Second, we develop a conceptual model that captures G2B control principles. This conceptual model can be used as a basis for systematic software-aided design and analysis of government control procedures. Finally, we exemplify the use of this theoretical framework in a case study concerning the export of agricultural goods from the EU to Russia.

2 Development of Organizational Control Theory

2.1 From Internal to Inter-organizational Control

Research on organizational control stems from the field of internal control. The focus of internal control is limited by a single-company paradigm, where companies operated mostly as independent units. In 1992, COSO (The Committee of Sponsoring Organizations of the Treadway Commission) issued the Framework of Internal Control, which has been used by thousands of corporations to conduct their internal control. COSO defines internal control as "a process, affected by an entity's board of directors, management and other personnel designed to provide reasonable assurance regarding the achievement of objectives in : *Effectiveness and efficiency of operations; Reliability of financial reporting and Compliance with applicable laws and regulations*" [9].

In recent years, collaborations among organizations have increased dramatically. The focus shifted from research on a single company to research on business networks/business webs [20] or value constellations [15], and inter-organizational relations have gained their place in the academic world. Hence, also the notion of

control has been extended to an inter-organization context: "Inter-organizational controls are those measures that limit the risk a party runs in a business transaction due to the possible existence of opportunistic behavior by its trading partners" [5, p. 36]. Research on inter-organizational control (IOC) is still in its infancy and limited to business settings where all parties pursue commercial benefits. It is a pending issue to further develop the theory for relations between government and businesses (G2B).

2.2 Bons' Inter-organizational Control Principles

An important contribution to IOC research is Bons' five fundamental IOC principles for B2B control [7]:

1. "If a primary activity is performed by Role 1, Role 2 should testify the completion thereof using some document, which should be received by Role 1. If the party playing Role 2 is not trusted by the party playing Role 1, the primary activity should be executed after receiving the document.
2. Before Role 1 executes a primary activity it should have witnessed the performance of the counter-activity by some Role 2 if the party playing Role 1 does not trust the party responsible for role 2, unless it has received evidence that Role 2 has executed its tasks.
3. If Role 1 cannot witness the performance of a counter activity, another Role 3 should testify the completion of Role 2's activity if the party playing Role 2 is not trusted by the party playing Role 1. This document must be received by Role 1 before the execution of its primary activity, and the party playing Role 3 should be trusted by the party playing Role 1.
4. If a primary activity is outsourced to an agent and the principal role did not previously witness the counter-performance or receive evidence thereof, the agent role should witness this counter-performance before it performs the (outsourced) primary activity if the principal does not trust his counterparty. If this is not possible, the agent role should at least receive evidence of the counter-performance.
5. If the counter-activity (by Role 2) to some primary activity of Role 1 consists of only the enabling actions of Role 2 to arrange some agent (Role 3), and not the agent's performance as well, and the party that plays Role 1 does not trust the party that plays Role 2 and has not previously witnessed the counter-activity, Role 1 should receive an unambiguous promise from Role 3 that it will be the beneficiary of Role 3's performance before it executes his own primary activity. Furthermore, the party playing Role 1 should trust the party that plays Role 3".

Some important terminology has to be explained here. A *primary activity* is a "primary obligation in some underlying legal agreement" [5]. Based on the principle of economic reciprocity, a primary activity of one actor is the *counter activity* of another actor. The typical case is a delivery of goods and a payment. The delivery of goods is the primary activity of the supplier, but it is a counter activity from the buyer's perspective. These principles assume independent and non-hierarchical relationships between organizations and pay special attention to outsourcing activities and to the reciprocal

character of contracts. Bons also investigates the 'trust" relationship amongorganizations. *Trust* is defined by [17] as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another". However, "trust" is difficult to quantify and has numerous interpretations [19]. Considering "trust" as control factor creates barriers for understanding and applying controls and for designing IS support. To overcome this difficulty, we assume that no trust pre-exists under B2B context, unless there exists legal/contractual constraint or other enhancement like certification.

2.3 From B2B to G2B Control

Only limited research (e.g., [5, 10]) exists on IOC, and existing research is focused on B2B relationships. A question raised here is whether control principles for B2B can be applied in the G2B context. An extensive literature review [5-10, 16, 18, 21 and more] shows that the intrinsic components of control do not differ between business and government control. Under both settings, control is affected by the interplays among three essential components: actor, activity and documents (for details, refer to [14]). We therefore argue that Bons' control principles for B2B apply also to G2B, when following differences between B2B and G2B are taken into consideration:

- Bons' principles are bi-directional because no trust is assumed between any two parties. We assume the government to be trusted (we consider modern democracies; in other regimes and cultures this assumption may not always be valid). Thus Bons' principles can be applied only when role 1 is the government, and role 2 is a business.
- Therefore, the primary activity, in Bons' terms, is the government (control) activity. Similarly, the counter activity is a business transaction that the government (primary) activity controls.
- Yet, businesses could win the government trust by means of certifications [1, 4].
- Control under B2B normally focuses on safeguarding financial profits, however, government is not profit pursuing in most cases. In the G2B context, controls not related with economic (monetary) value are also considered important (e.g., legal compliance, security and social welfare).

An important application of G2B control is Customs control. The WCO (World Customs Organization) argues that good Customs control should rely on public-private partnerships and collaboration between government organizations [21]. In Section 4 we present a case study about this issue.

3 A Conceptual Model of G2B Control Principles

The principles of Bons et al. presented in section 2.2 provide a natural language description of a theory, but they are not suitable for automation. Furthermore, they are not specific for government control. Therefore we (1) transformed Bons' B2B control principle to G2B control (see Tables 1, 2 and 3), and (2) developed a conceptual

model to capture this knowledge (see Figure 1). As software can reason only about formalized domains, creating conceptual models of a domain (in our case: control, see Figure 1) is a pre-requisite for developing supporting software tools. Software tools will support human experts in designing government controls. They support human experts in investigating whether the current control procedures are well-designed and how to redesign a satisfactory government control (this is shown in section 4). It is not our intention to develop a software tool that would *automate* whole government controls, but rather to develop a tool that would help human experts *reason* about the design of these controls.

We map Bons' B2B terminology to G2B terminology in Table 1. Most concepts in Table 1 are assumed to be self-explanatory. The term TTP, Trusted Third Party, requires explanation. TTP is an entity which facilitates interactions between two parties who both trust it and is perceived as a widely accepted, reliable, independent, and highly secure entity that generates trust through attestation or certification [1].

Table 1. Bons' terminology transformed to G2B control terminology

Bons' terminology	**G2B control terminology**
Role 1	Government actor
Role 2	Business actor
Role 3	TTP
Primary activity	Government (control) activity
Counter activity	Business activity

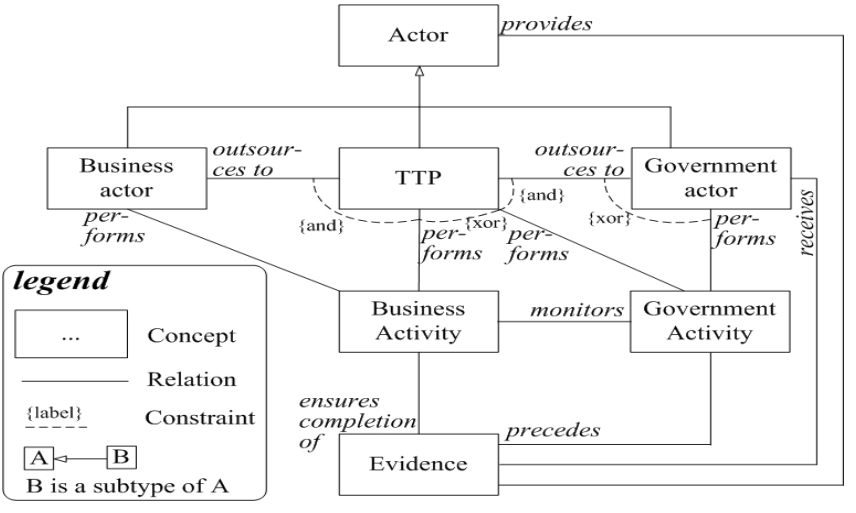

Fig. 1. A Conceptual model for G2B control principles. For details about the UML Class Diagram notation see [11].

Based on the earlier identified differences between B2B and G2B we explain in Table 2 how Bons' B2B control principles change in the G2B context.

Table 2. How Bons' principles change in a G2B setting

Principle number	G2B vs. Bons et al [7]
1	A control activity cannot take place before the business activity. The business actor is assumed to trust the government actor and need not testify the completion of a control activity. Therefore principle 1 does not apply in G2B.
2, 3	The government actor is assumed not to trust the business actor. The principles do not change.
4	Here the government actor outsources its activity. This is only possible if the third party is trusted (hence the term TTP: Trusted Third Party). Trust is typically achieved by means of certification [1]. Also, government actors typically trust each other, and hence the TTP may be another government actor.
5	Here the business actor outsources its activity to a TTP. The government actor is assumed not to trust the business actor.

This results in G2B control principles, listed in Table 3 and formalized in Figure 1.

Table 3. Government control principles for G2B

Bons' principle number	G2B control principle
1	Does not apply in G2B
2	Before a government actor executes a government activity it should have witnessed the performance of the business activity by some business actor, unless it has received evidence that the business actor has executed its tasks.
3	If a government actor cannot witness the performance of a business activity, another TTP should testify the completion of the business actor's activity. This document must be received by the government actor before the execution of its government activity.
4	If a government activity is outsourced to a TTP and the government actor did not previously witness the business performance or receive evidence thereof, the TTP should witness this business performance before it performs the (outsourced) government activity. If this is not possible, the TTP should at least receive evidence of the business performance.
5	If the business activity (by a business actor) to some government activity of a government actor consists of only the enabling actions of the business activity to arrange some TTP, and not the TTP's performance as well, and the government actor has not previously witnessed the business activity, the government actor should receive an unambiguous promise from the TTP that it will be the beneficiary of the TTP's performance before it executes his own government activity.

4 Case Study: Export from the EU to Russia

A conceptual model as in Figure 1 serves for developing decision support tools for human experts. Tools implement business rules (in our case: G2B control principles) and support humans in designing control procedures. In the rest of this section we describe how we applied the conceptual model in Figure 1 in a real-world situation to investigate whether existing G2B control procedures adhere to design principles.

4.1 Case Description

The case studied in this paper focuses on the export/import of agricultural goods from EU to Russia. When an EU company exports agricultural goods to a Russian company, two main regulations are involved: (1) The Russian buyer has to pay import duties in Russia; and (2) The EU seller applies for EU subsidies from EAGGF (the European Agricultural Guidance and Guarantee Fund). Subsidies are given to EU companies that export agricultural goods outside the EU as a means to increase the competitiveness of the European agriculture. Russian import tax is levied based on the value of the imported goods, while EU subsidies are given based on goods quantity. Following main actors are involved in this scenario: (1) seller: an EU company; (2) buyer: a Russian company; (3) EU customs at the border (e.g., the Finnish customs at the border between Finland and Russia); (4) Russian customs; and (5) EAGGF, providing subsidies. Figure 2 shows the relevant procedures; it is based on the UML Activity Diagram notation, where every column (a "swimlane") reflects the activities (rounded rectangles) of an actor, and where the arrows denote a sequence in activities. For brevity, the figure only shows the main activities.

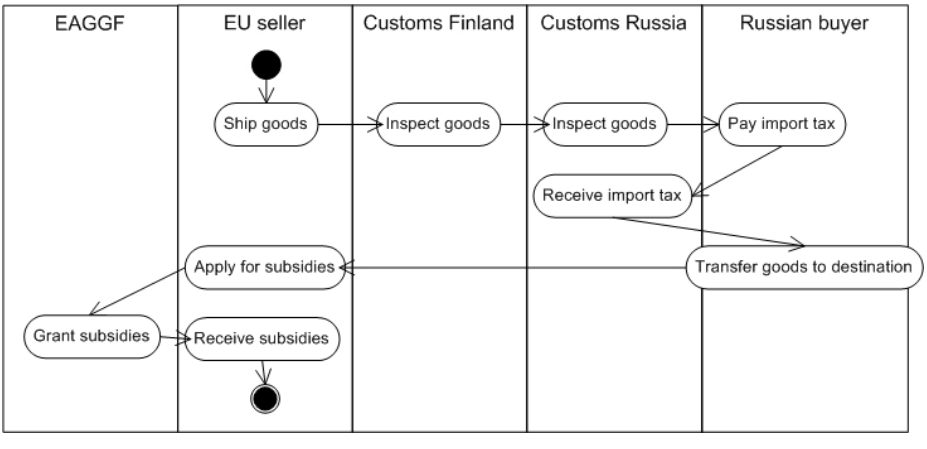

Fig. 2. Activity Diagram of the export process from Finland to Russia, focusing on EAGGF subsidies for agricultural goods

4.2 G2B Control Principles Used for Procedure Design

The conceptual model presented in Section 3 provides guidelines for designing control mechanisms to safeguard the payment of import tax in Russia and the distribution of EAGGF subsidies. Since we do not have a software tool yet, in order to test the model's computational validity, we simulate the algorithms of such a tool, and investigate the results in this section and in the next one. According to the G2B control principles, the import tax control procedure involves the following actors and activities:

- Government actor: Russian customs. Government activity: enforce tax legislation (and in particular: collect import duties).
- Business actor: a Russian buyer. Business activity: import goods.

The Russian customs does not trust the Russian buyer, and therefore requires customs control procedures (these are currently not available, as can be seen in Figure 2). This is the underlying assumption of our principles. Theoretically, an importing company could not declare any import (and thus not pay import duties), or declare a lower value of the imported goods (and thus pay less duties).

Although theoretically the Russian customs can physically inspect every shipment at the border, the lack of human resources does not allow such controls. Thus, principle 2 does not apply here because in reality the beneficiary of the business activity (i.e., Russian customs) cannot witness the buyer's performance. And indeed, in reality a practice of *double invoicing* exists. Importing companies present the real invoice to the Finnish customs, and a fake invoice – with a lower value of goods – to the Russian customs, so that they pay less import duties. According to principle 3, a third party, trusted by the Russian customs, needs to be introduced, that would testify about the imported goods.

In the interaction between EAGGF and the exporting EU companies we consider the following roles and activities:

- Government actor: EAGGF. Government activity: support European agriculture (and in particular: provide subsidies).
- Business actor: an EU seller. Business activity: export agricultural goods.

EAGGF does not trust a company that claims it has exported agricultural goods outside the EU. As EAGGF is not part of the business transaction between sellers and buyers, it has no reliable information concerning the exported goods (quantity, value). Theoretically, an exporting company could declare an export that has never taken place, or declare having exported more goods than it actually has (and thus obtain more subsidies than it is entitled to). Principle 2 does not apply here because the beneficiary of the counter activity (i.e., EAGGF) cannot witness the seller's performance. According to principle 3, a third role needs to be introduced, that would testify about the exported goods. This role must be trusted by EAGGF.

5 Designing E-Customs Control Procedures

According to principle 3, both control problems discussed above require the introduction of a Trusted Third Party (TTP) that can provide evidence of the counter

actor's performance. Double invoicing is a main problem for the Russian customs, resulting in loss of revenues. The difficulty in solving this control problem lies in the question which actor can serve as a trusted third party, with the capability to provide evidence of export from the EU to Russia.

In G2B there are mostly two types of TTPs. Either one government actor serves as a TTP for another (e.g., Finnish customs can serve as a TTP for the Russian customs; customs can serve as a TPP for health agencies), or a commercial party can be *certified* to perform certain activities as a TTP, subject to periodic audits (e.g., often security control at airports is performed by commercial companies, and not by the national authorities).

A partial solution for the *double invoicing* phenomenon (import tax fraud) is the *Green Corridor* between Russia and Finland (also Sweden is involved in this agreement). According to this agreement, Finnish companies that are certified by the Finnish and Russian customs send pre-arrival information about their exported goods to the Finnish customs, who forward this information to the Russian customs. As a result, the Russian customs receives pre-arrival information on imported goods, and double invoicing can be prevented. The Green Corridor is a typical example of e-Customs, since one of the core paper evidence documents in the control procedure, the invoice, is replaced by the direct exchange of pre-arrival information between the Finnish and Russian Customs. We see here the two types of TTPs, both of which are the result of implementing principle 3 and can be seen in Figure 3. The Finnish customs acts as a TTP for the Russian customs by forwarding pre-arrival information (government actors trust each other), and certified Finnish companies act as TTP for the Finnish customs by providing the pre-arrival information. Trust in the data sent by Finnish companies to the Finnish customs is achieved by means of certification (subject to periodic audits). While this solution works for certified companies, it does not solve the problem for most companies, because no trusted third party can provide evidence of their performance.

EAGGF also needs to introduce a trusted third party to its business process, to provide evidence of the export of agricultural goods outside the EU. EAGGF uses the Russian customs as a TTP (again: government actors trust each other). Once import duties have been paid in Russia, an import certificate is issued by the Russian customs and given to the (Russian) buyer. This certificate is forwarded by the Russian buyer to the EU seller who uses it as evidence for its performance (export of agricultural goods outside the EU) in the application for EAGGF subsidies.

Figure 3 shows a new activity diagram, where the two controls have been embedded based on Table 3. Broad arrows denote the respective concepts from Figure 1 (e.g., business actor, government actor). As there are two procedures involved, we differentiate them with different labels. *Italic* labels with a shadow background show the concepts as applied to the Russian import procedure, and **bold** labels with no fill show the concepts as applied to the EAGGF subsidies procedure. When this analysis is done using a software tool, the tool can identify situations where (e.g., in Figure 2) a control problem exists, and propose possibilities for a TTP, indicate the need for producing evidence and which actors may produce this evidence (e.g., as in Figure 3).

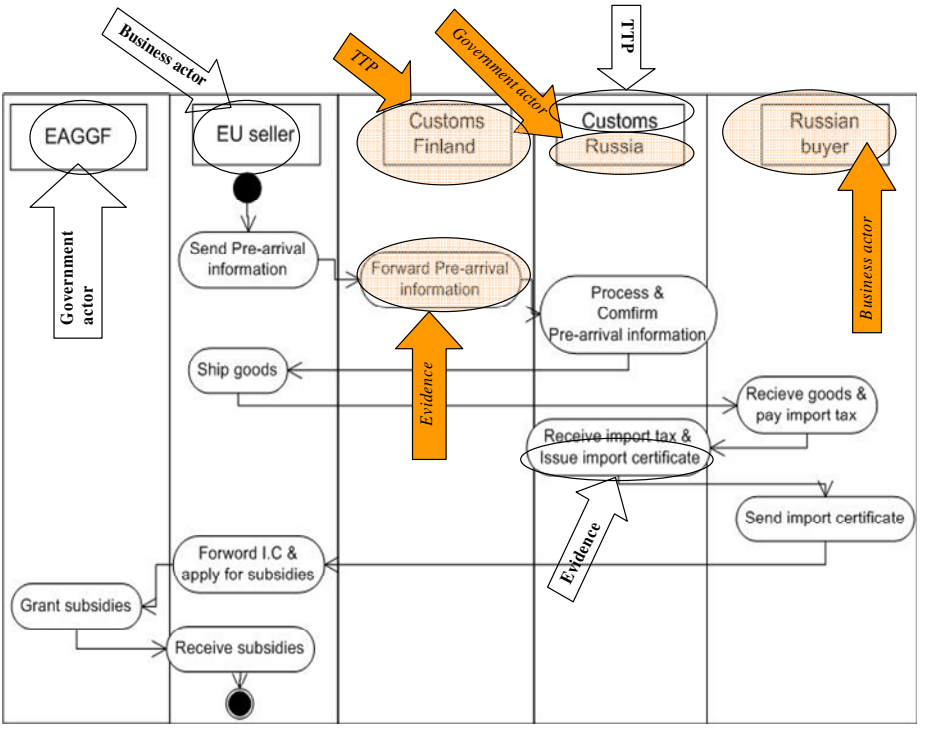

Fig. 3. Redesigned procedure for the export of agricultural goods from Finland to Russia

Due to the explorative nature of our work, no a-priori knowledge existed of how the government procedures *should* be designed. Therefore, we performed interviews with customs experts to assess the reasoning presented in Sections 4.2 and 5, and to validate the underlying conceptual model (Figure 1).

6 Conclusions and Future Work

Our goal is to develop a methodology for the design of e-Government control procedures, using Internet technology to replace paper-based customs documents by online information exchange. As such, this paper presents several contributions to existing knowledge base. First, we explore similarities and differences between G2B and B2B controls. Second, this allows us to define principles for designing G2B controls. Third, we present a semi-formal conceptual model that captures this knowledge and enables developing decision support tools to support human analysts in designing government controls and in analyzing existing controls.

Traditional research on inter-organizational control focuses on B2B. In this paper we argue that existing theory for B2B control can be used as a basis theory for G2B

control, when a number of differences between G2B and B2B are taken into consideration. The main differences between B2B controls and G2B controls are: (1) in B2B relationships we assume no trust in any direction, while in G2B we assume that government is trusted by businesses, but not vice versa; and (2) while in B2B controls are safeguards for economic value, in the government sector value is broader than Return On Investment, and includes societal, legislative and other aspects.

We take as a starting point B2B control principles as formulated by Bons et al. [7], based on acknowledged accounting and auditing theories including [8, 9, 16, 18]. We reformulate them to accommodate the differences between B2B and G2B. This results in a set of G2B control principles that are grounded in accounting and auditing theory.

We formalize these G2B control principles in a conceptual model. The main advantage of conceptual models is that they can be used as a basis to develop software support tools to assist human experts in designing and analyzing organizational artifacts. Similar models (applied to other domains) have been implemented in the past by Baida [2] and Gordijn & Akkermans [12].

A case study about the export of agricultural goods from Finland to Russia was used to test and validate our theory. Even though the case study is kept simple for demonstration purposes, we show that by applying our principles we can identify flaws in government procedures that are used daily, vulnerable to large-scale fraud. The reasoning we present in Sections 4.2 (current situation) and 5 (procedure redesign) simulates the reasoning that a software support tool would perform, once implemented based on our conceptual model. We validated with domain experts whether our analysis and its underlying conceptual model are sound and yield the desired results. In this way we establish the validity of our principles and model.

Naturally, one case study is not enough to claim that a theory is valid. Therefore we intend to apply this model to other case studies as well, covering a broad scope of government controls. We will also seek to extend Table 3 with more control principles, and extend our conceptual model to accommodate these additions. For example, the case study presented here uses *certification* as a means to establish trust instead of performing control. We will study auditing literature to formulate a principle for embedding certifications in our model.

We distinguish between (1) ICT support in the design and analysis of G2B controls and (2) ICT as a means to facilitate government control. In the current paper we present a conceptual basis for enabling the former. In [3] we focus on the latter. To this end, we are currently engaged in a number of large-scale case studies to study how ICT can change the way government controls are carried out in international trade, how roles and responsibilities can change and how administrative control can replace physical control of goods.

Acknowledgments. This research is part of the integrated project ITAIDE (nr.027829), which is funded by the 6th Framework IST programme of the European Commission (see www.itaide.org). The authors thank Saara Tveit of the Finnish National Board of Customs for useful discussions.

References

1. Ahuja, V.: Building Trust in electronic commerce. IT Professional 2(3) (1997)
2. Baida, Z.: Software-aided Service Bundling – Intelligent Methods & Tools for Graphical Service Modeling. PhD thesis. Vrije Universiteit Amsterdam, The Netherlands (2006) (last visited May 25, 2007), available via http://www.baida.nl
3. Baida, Z., Rukanova, B., Liu, J., Tan, Y.-H.: Rethinking EU Trade Procedures – The Beer Living Lab. In: Proceedings of the 20th Bled eCommerce conference, Bled, Slovenia (2007)
4. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: Proceedings of The 1996 IEEE Symposium on Security and Privacy, pp. 164–173. IEEE Computer Society Press, Los Alamitos (1996)
5. Bons, R.W.H.: Designing Trustworthy Trade Procedures for open Electronic Commerce. PhD thesis, University of Rotterdam, The Netherlands (1997)
6. Bons, R.W.H., Lee, R.M., Wagenaar, R.W.: Designing trustworthy interorganizational trade procedures for open electronic commerce. International Journal of Electronic Commerce 2(3), 61–83 (1998)
7. Bons, R.W.H., Lee, R.M., Wagenaar, R.W.: Computer-aided auditing of inter-organizational trade procedures. International Journal of Intelligent Systems in Accounting, Finance and Management 8(1), 25–44 (1999)
8. Chen, K.-T., Lee, R.M.: Schematic evaluation of internal accounting control system. EURIDIS Research Monograph, Erasmus university Rotterdam (1992)
9. COSO: Internal control – integrated framework. The Committee of Sponsoring Organization of the Treadway Commission (1992)
10. Dekker, H.C.: Control of inter-organizational relationships: Evidence on appropriation concerns and coordination requirements. Accounting, Organization and Society 29(1), 27–49 (2004)
11. Fowler, M., Scott, K.: UML distilled: Applying the standard object modeling language (1997)
12. Gordijn, J., Akkermans, J.M.: Designing and evaluating e-Business models. IEEE Intelligent Systems 16(4), 11–17 (2001)
13. Liu, J., Baida, Z., Tan, Y.-H., Rukanova, B.: Designing controls for e-government in network organizations. In: Schoop, M. (ed.) Proceedings of the 13th Research Symposium on Emerging Electronic Markets, Stuttgart, Germany, pp. 22–35 (2006)
14. Liu, J., Baida, Z., Tan, Y.-H., Korpela, K.: Design and analysis of e-government customs control: the Green Corridor between Finland and Russia. In: Proceedings of the 20th Bled eCommerce conference, Bled, Slovenia (2007)
15. Normann, R., Ramirez, R.: Designing interactive strategy: From value chain to value constellation. John Wiley & Sons, Chichester, UK (1994)
16. Romney, M.B., Steinbart, P.J.: Accounting Information Systems, 10th edn. Prentice-Hall, Englewood Cliffs (2006)
17. Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not so different after all: A cross-discipline view of trust. The Academy of Management Review 23(3), 393–404 (1998)
18. Starreveld, R.W., de Mare, B., Joels, E.: Bestuurlijke Informatieverzorging (in Dutch), 4th edn., vol. 1. Samsom, Alphen aan den Rijn (1994)
19. T3-Group: Trust across disciplines. ISTC (Institute for Cognitive Sciences and Technologies). CNR (National Research Council). Italy (2005)
20. Tapscott, D., Ticoll, D., Lowy, A.: Digital capital – harnessing the power of business webs. Harvard Business School Press, Boston, Massachusetts (2000)
21. WCO (World Customs Organization): Framework for standards to secure and facilitate global trade (last visited May 25, 2007), http://www.Wcoomd.Org/ie/en/press/wco%20-%20framework%20of%20standards%20june%2021%20final.Pdf