Supporting Customs Controls by Means of Service-oriented Auditing

Hans Weigand, Faiza Allah Bukhsh

Dept. Information Management, Tilburg University, Tilburg, The Netherlands
{H.Weigand, f.a.bukhsh}@uvt.nl

Abstract. From a labour-intensive and paper-based door-keeping function Customs control is aiming now towards international trade facilitation in a way that is both efficient and secure. Digitalization of documents and automation of processes plays an important role in this transition. However, the use of modern technology, in particular SOA, is not yet optimal. The research objective of this paper is to explore the potential of SOA for innovating Customs processes by developing a service-oriented auditing approach and evaluating its added-value in the area of Customs control. Service-oriented auditing is a promising tool to implement the ideals of continuous and online monitoring

Keywords: continuous monitoring, customs control, service-oriented architecture, REA.

1 Introduction

Customs control is an area that is rapidly innovating. From the labor-intensive and paper-based door-keeping function it used to have in the past, it is aiming now towards international trade facilitation in a way that is both efficient to all parties and secure. Digitalization of documents and automation of processes plays an important role in this transition. However, the general feeling is that the use of modern technology, such as Service-Oriented Architecture (SOA) [22], is not yet optimal. Automation of current processes is useful but not sufficient: what is needed is a reengineering of the control processes by going back to the goals to be achieved and the risks to be mitigated. What complicates this problem, compared to the business process reengineering wave of the '90s, is that the control processes are inter-organizational in nature, involve many parties and are bounded by multiple levels of governmental regulations.

The research objective of this paper is to explore the potential of SOA for innovating Customs processes by developing a service-oriented auditing approach and evaluating its added-value in the area of Customs control. The paper is organized as follows. A section 2 reviews recent development in Customs control and introduces the Extended Single Window (ESW) project in which the research is located. This part is based on a literature survey and project meetings we had in 2010 with traders, Customs officers and port community system providers. Section 3 introduces a new service-oriented auditing approach, which is applied to Customs control in section 4. In terms of Peffer's design science phases [23], Section 2 contains the *identification* and *motivation*, as well as the *solution objective* of ESW, Section 3 is an exploration of the *design and development* of the core artifact, and Section 4 is the *demonstration*. Section 5 closes with conclusions and directions for future research.

2 Customs Control

Customs control is the process where Customs inspects, verifies and examines inward and outward means of transport according to the law to ensure the implementation of national laws and regulations concerning entry and exit of means of transport, goods, personal articles as well as mails and parcels. This is accomplished by declaration procedures, document inspection, examination and other related controls. In 2007, the World Customs Organization developed the so-called International Convention on the simplification and harmonization of Customs procedures (the Revised Kyoto Convention), in an effort to promote the achievement of a highly facilitative international travel and trading environment while maintaining appropriate levels of regulatory control. The Convention explicitly requires administrations to adopt the use of risk management techniques, maximize the use of information technology, implement appropriate international standards and cooperate with other relevant authorities and trade communities, as well as with private sector partners. In this section, we provide an overview of recent developments in Customs control in China and the European Union, and then introduce the Extended Single Window project that started in the Netherlands in 2010.

2.1 China Customs Reforms

China Customs has introduced a series of reforms to improve Customs inspection and supervision. The following description is based on China Customs Annual Report 2009, (http://english.Customs.gov.cn/publish/portal191/). In 2008, China Customs processed 361 million entries and exits of passengers and their personal articles, exerted control over 2.425 billion tons of import & export goods valued at USD 2.56 trillion, strongly accelerating the development of foreign trade as well as cultural and technological exchange. In 2009, China Customs put in efforts to adopt a comprehensive management on the self-compliance of the enterprises, promoting the classified clearance system and implementing the measure of "declare at home, release at port" (a cross-Customs districts clearance model under which qualified enterprises can firstly declare to the Customs house with which they have registered and then have the goods released at the ports where the actual in and outflows of goods take place) as well as the measure of helping goods transfer among different Customs districts. It improves its administration over bonded logistics and makes the clearance processes of Customs special control areas, bonded areas and frontline checking spots gear up to each other.
- *Customs control over processing trade and bond operations*: after getting promise from enterprises that there will be no loss of national revenue, Customs does not levy

duties on their import goods but exerts control over the whole process of processing until the processed goods are re-exported.
- *Audit-based Customs control*: within 3 years (or some designated time period) upon release of import or export goods or goods with import duties reduced or exempted, Customs verifies the account books, related documents and relevant import & export goods of the legal entities under Customs control, so as to supervise the truthfulness and legitimacy of their import & export activities. The priority of audit-based control is to regulate the importation and exportation of the enterprises, guide them towards compliance and self-discipline and find smuggling or violation clues through post auditing on goods of normal trade, and auditing on goods whose duty reduction or exemption has been approved.
- *Customs statistics*: the process where Customs conducts statistics compilation and comprehensive analysis. Attributes include description, quantity, weight, price, country (region) of origin, legal entity, domestic destination, domestic place of origin, trade method, transport means and relevant Customs districts (houses) of the import and export goods. The objective of these statistics is to reflect comprehensively and accurately the faring tendency of foreign trade, conduct early-warning import & export monitoring and provide information services for national macro-economic decision-making and the development of foreign trade.

2.2 EC Modernized Customs Code

The *Modernized Customs Code* (MCC) was adopted by the European Community in April 2008 but the process of implementation is still continuing. The MCC will simplify legislation and administration procedures both from the point of view of Customs authorities and traders. It aims to:
- Streamline and reduce the number of *Customs procedures* and make it easier to keep track of goods;
- Ensure the progressive *automation* of all Customs formalities, with a view to a completely ‘paperless environment for Customs and trade’. This applies to documents between traders and Customs as well as between Customs and other authorities.
- Promote the concept of ‘*centralized clearance*’, under which authorized traders will be able to declare goods electronically and pay their Customs duties at the place where they are established, irrespective of the Member State through which the goods will be brought in or out of the EU Customs territory or in which they will be consumed.
- Offer bases for the development of the *‘Single Window’* and ‘One-Stop-Shop’ concepts, under which economic operators give information on goods to only one contact point, (Single Window concept) even if the data should reach different administrations/agencies, so that controls on them for various purposes (Customs, security, sanitary,...) are performed at the same time and at the same place (One-stop-shop concept).
- Streamline and *harmonize* further the Customs guarantee systems

The concept of *centralized clearance* means that when an "authorized operator" lodges his Customs declaration at the Customs office where he is established, that office would then carry out any documentary risk analysis. Subsequently, this office would forward the results of its analysis to the border Customs office in that Member State or in another Member State where the goods are actually to enter or leave the Community. This border office would apply any physical controls to the goods being imported or exported that either office deems necessary on the basis of the result of risk analysis. Compliant and trusted traders would generally have a minimal incidence of selection for control at the place of entry or exit. Provided that there is no irregularity, and that the Customs debt was provided for at the office of import, the goods would be released directly into free circulation in the EU or for export. Under the procedure, the goods do not have to be moved to the office of import or export but could be delivered directly to the point of sale, in whatever country. So this allows multi-national companies to conduct all of their EU business with one Customs office.

2.3 Extended Single Window

The vision of the Extended Single Window project (ESW) that started in 2010 is to develop an integrated coordinated border management solution for ports and airports integrating with previous and subsequent procedures for reliable, secure, and cost effective logistic chains throughout the Netherlands as a logistic gateway to Europe. This coordinated border management solution is referred to as 'Extended Single Window'. It requires efficient and reliable handling of data to generate information for effective joint supply chain planning for shippers, goods owners, transportation companies, forwarders, terminals and other logistic service providers and to use these data also to generate information for government agencies, like Customs, agricultural and tax. Currently, shippers and goods owners are faced with a wide range of regulations and procedures when goods enter or exit the EU (border, agricultural, safety, import controls, statistics, and indirect taxes). Completion of declaration processes and risk analyses and planning and coordination of inspections by the various agencies before shipments are (un)loaded from an aircraft or vessel enables logistics actors (terminal operators, forwarders, transport operators) to plan and execute transportation of shipments with hinterland hubs efficiently (improving modal shift, throughput time (i.e. for perishable goods) and reducing congestion). Efficient and reliable government controls reduce administrative costs, increase reliability of the supply chain, and ultimately reduce transport costs for shippers and logistic operators.

Thus, ESW aims to contribute to the implementation of the MCC for both incoming and outgoing logistic flows, including integration with previous (outgoing goods for instance preceded by export) and subsequent procedures (incoming goods for instance followed by transit). Basic research in advanced information technologies is in Event Driven Architecture with a Logistic Interoperability Ontology:

- *Event Driven Information Service Bus (EISB).* This is a (virtual) technical architecture at middleware level that extends the concept of Enterprise Service Bus (ESB) as it is advocated in SOA. Basically, each logistic operation triggers an event. Discharge of a container from a vessel and loading cargo on a truck for on-carriage are examples of events. Minimally, an EISB supports publish/subscribe functionality to events, thus supporting a virtual data space.

Since the data space is virtual, relevant data can still reside with each actor depending on governance and logistic innovations at business level. Authorities can subscribe to events upon which processes can be triggered for retrieving data required by risk management systems or coordinating inspection. The EISB fully supports a SOA since service requests and responses are treated as events as well. Conversely, subscribing to a published event type is equivalent to using the event publisher as a service (typically called monitoring service or sensor service). In this way, the EISB can support traditional document-driven processes as well as new event-driven processes based on smart seals (RFID etc.) for tracking and tracing of movement of goods.

- *Logistic Interoperability Ontology Framework*. It specifies the semantics of all physical objects as shared by business actors in supply chains, e.g. semantics of containers, goods items, and trucks. The ontology also encompasses mechanisms for information sharing amongst all actors in logistic chains thus allowing that each actor shares only relevant information with one or more other actors.

Using the EISB concept it is possible to *extend* the Single Window concept in at least two significant ways. Firstly, the Single Window is based on digital documents, whereas the ESW is based on *events*, which is much more flexible. Assume that a sender (shipper) has to send a document to a number of receivers (Customs office, Tax office). He fills in the data in a document template. With Single Window, he has to send the document only once, but filling in the document is still mainly a process of copying data from one source to another. With Extended Single Window, the data collection and sending may become superfluous. Events are published only once. The receiver specifies which data he wants to see (by subscribing to events), and these data are collected then (that is, continuously) from the virtual data space fed by all the distributed events. Secondly, the Single Window only streamlines data flow in one direction, from logistic operators to government agencies, whereas the EISB also supports data flow among logistic operators and across the supply chain, among government agencies (e.g. to realize a One-Stop-Shop), and from government agencies to operators. One of the very powerful new possibilities opened up this way is end-to-end supply chain integrity as advocated by [10]. Whether such an EISB is managed by a single intermediary, or that the implementation involves an intermediary *network* with an industrial part and a governmental part, is still an open issue, but has no effect on the EISB concept as such.

Building on the EISB, the ESW project furthermore aims to reengineer Customs procedures using service-oriented technology. In the envisioned scenario, Customs can use audit services that monitor logistic flows via the EISB, preferably in a continuous and non-intrusive way. In the next section, we will develop a framework for Service-Oriented Auditing. The application of this solution approach to Customs requirements is demonstrated in section 5.

3 Service-Oriented Auditing

The primary objective of a traditional audit of an organization's financial statements is to form an opinion on the *trustworthiness* of the included information and to make this opinion public to an interested audience. Such an opinion is based on a careful analysis of the potential risks and the effectiveness of built-in control mechanisms to mitigate them, - influencing correctness and completeness - as well as a check on the company-wide integrity of the information. An auditor will look for assurance by either auditing the *design*, i.e., the implementation and effectiveness of controls, or, alternatively, by looking substantively at the *data* generated by the system. The latter approach can be very costly. These costs can be reduced by either taking a random sampling approach or, nowadays, by modern process mining techniques such as described in [1]. Of course, in practice always a combination of the two approaches will be used, as it is now, but the weight assigned to each can shift significantly.

3.1 Auditing & ICT

As modern information systems draw heavily on ICT, modern auditing cannot do without ICT either. Many tools to support the auditor are already available, e.g. ACL and IDEA. Still, we have identified many research challenges in this field:

- *Semantic gap.* According to Li [16], there is quite a gap between the IS (Information Systems) environment and the audit environment. It is not sufficient for auditors to have direct access to databases and files; they should also understand the semantics. The same applies to processes. An analysis of business modeling approaches from the perspective of process level audit risk assessment by Carnaghan [4] reveals that current approaches do have their merits but also their lacks.
- *Managing the business logic*. The interpretation steps made during the monitoring process are warranted by business rules. These business rules (the policies they capture) change over time, and therefore need to be managed properly. This change management is complicated by the above-mentioned semantic gap that exists between the execution level addressed by the IT and the policy level on which the business formulates its requirements.
- *Smart auditing.* There are more and more AI techniques that can be used to mine large amounts of data (off-line or real-time), such as neural networks, genetic algorithms, process mining and Bayesian belief networks. In addition, the intelligent use of domain knowledge can often simplify or optimize heavy data search processes [9].
- *Adaptive monitoring*. Monitoring can be a complex task that uses a configuration of numerous hardware and software resources. The question is not only whether it can be done but also how to optimize this task (in terms of time, costs on the one hand and the effectiveness in terms of risk management and control on the others), and how to cope with failures. The aim of adaptive monitoring is to allow dynamic configuration of the monitoring task according to certain performance goals.

- *Online auditing*. Online (continuous) auditing means that the auditor does not inspect the organization physically, but rather inspects databases remotely. This format has certain limitations, but also new possibilities, in particular (a) the possibility to run complex queries and (b) the possibility to cross-check with other databases (public databases or business partner databases) and (c) to do this on a real-time continuous basis [14]. Online auditing should be non-intrusive, i.e., not interrupt normal operations, and obey transparent security requirements. Online auditing is closely related to the idea of "Piggy-Backing" where auditor and auditee agree to use the same business data flow for both internal and external audit purposes.

Continuous Online Monitoring started at the end of the 90's to draw on Embedded Audit Modules. Embedded Audit Modules (EAMs) are software applications embedded in host systems or linked to host systems in order to externally monitor such systems. EAMs continuously monitor flows of transactions, identify transactions that match certain pre-determined integrity constraints and, in the event of a constraint violation, alert the auditor and copy the transaction data to a file. The adoption of EAMs has been rather low so far [6]. As already argued by [21], *web service* technology can make the implementation much simpler, and also broaden the application from single enterprise ERP systems to supply chains, and from single databases to event logs and business process audit trails.

Conceptually, a distinction must be made between Continuous Monitoring and Continuous Auditing. The American Institute of Certified Public Accountants (AICPA) defines continuous auditing as "written assurance that is provided at the time or very near the time of events that affect the financial statements". In contrast, continuous monitoring does not necessarily involve assurance, but it can be used to realize the former.

In the following, we will focus on two of the above-mentioned challenges, while considering the others as well. To address the semantic gap, we propose to base the auditing on the *REA business ontology*. To realize Continuous Online Monitoring, we propose a *SOA-based solution*.

3.2 REA business ontology

The Resource-Event-Agent (REA) ontology was first formulated in [18]. The following is a short overview of the core concepts of the REA ontology.

A *resource* is any object that is under the control of an agent and regarded as valuable by some agent. This includes goods and services. Resources are modified or exchanged in processes. A *conversion process* uses some input resources to produce new or modify existing resources, like in manufacturing. An *exchange process* occurs as two agents exchange (provide, receive) resources. To acquire a resource an agent has to give up some other resource. An *agent* is an individual or organization capable of having control over economic resources, and transferring or receiving the control to or from other agents. The constituents of processes are called *economic events*. REA recognizes two kinds of duality between events: conversion duality and exchange duality.

The reason for building Service-Oriented Auditing on REA is that REA abstracts from process details and implementation systems, and so talks the language of the business rather than the IT specialist. This is because it focuses on economic *value*. At the same time, it has been shown that REA structures also provide a solid basis for implementation. There is a direct mapping from REA models to database structures [5]. The dualities express integrity constraints that that can be used for both the design of control mechanisms (preventive) and for the detection of deviating behavior (detective) that may indicate fraud.

From an advanced audit perspective, it is not always sufficient to consider operational processes only. It may also be necessary or more efficient to include the management level. That is why the policy level of REA must be taken into account as well. The event records give an answer to the question "what has happened?", but not to the question "what is planned or scheduled – what *should* happen?" The latter is modeled at the policy level that allows talking about types and groups as well as commitments. Policies can be formalized in analogy to contracts as a group of intentional resources obeying the duality principle: resources that the agent gives in versus what he aims to achieve [27]. On the event dimension, *constraints* are what the agent gives in (directives that limit the actions of the controlled system, e.g. an authorization table) and *goals* are what the agent aims to gain in return for that (the expected result of the controlled system, in terms of evaluations). In addition, the policy may contain *assumptions* in the form of testable assertions. The constraint part of the policy is the basis for (decision services within) the operational process design, the goal part is the basis for the service monitoring design, and the assumption part is the basis for the context monitoring design.

3.3 Continuous Monitoring

In order to audit the core enterprise, the auditor must identify the Soll (de jure) and 1st (de facto) modality (cf. [1]). Buffer contents such as inventories or bank accounts may have illicit decreases or increases. Such errors have consequences for the other audit objects. For instance, an illicit decrease may lead to a potential *overstatement* of the registration, and hence of the financial statements (although possibly not material). We define the process structure that abstracts from such errors to be the Soll modality, whereas the 1st modality is obtained by incorporating the identified potential error classes. The 1st model can help to design internal controls or analyze their effectiveness in either *preventing* illicit events (preventive internal control) or being able to *notice* them when they occur (detective internal control), including being able to notice violations of the internal controls themselves (compliance procedures).

The REA event model, containing all the relevant economic events, has 1st modality. It does not incorporate *all* error causes, and so it is not a complete event model. However, as the REA model contains all resources that matter for the company, it has, by definition, a handle on all error *effects*. The REA model in terms of its duality constraints has the Soll modality. More normative constraints, such as permissions and authorizations, can be specified on the REA policy level [8]. We use "process patterns" for representing both the normative process structure and the potential deviating ones. Each process pattern is specified concretely in two layers:

the REA layer (REA events), and the implementation layer (events such as generated and available in the operational system). When the pattern matches a certain trace of operational events, then the REA layer of that pattern interprets this trace in REA terms.

The normative process structure is a combination ("weaving") of the core process with built-in controls (cf. [7,15]). Built-in controls can take many forms, including segregation of duties, restricted authorizations, required recordings (event traces), and pre-conditional checks. After we have identified different control strategies, they can be evaluated on the basis of effectiveness (as defined above) and efficiency (costs).

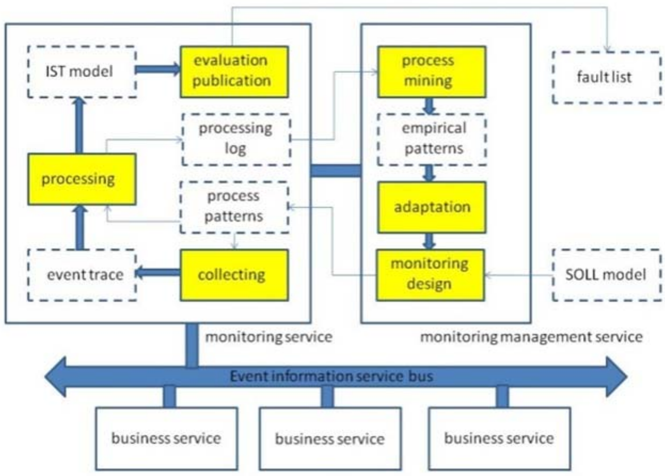

Fig. 1. Adaptive continuous monitoring service. The filled boxes represent activities, the dotted boxes informational resources.

Fig. 1 depicts the overall architecture of an adaptive service-oriented monitoring solution. Business services generate events that are published on the EISB. The continuous monitoring (CM) service also taps into the EISB, locally or remotely (as in [12]). The CM service *collects* the events using the publish/subscribe mechanism. Then it generates the IST model from the event traces by means of the specified process patterns. When the *processing* detects an operational event pattern, it generates the corresponding economic event as IST model. The IST model contains both good and bad process instances from which a fault list is generated (*evaluation*). This information can be forwarded immediately to the responsible actor, or can be logged on permanent storage for later inspection purposes (*publication*). The fault list can also be sent to the management control service of the process being monitored so that it can take appropriate measures (this does not hamper the independence of the monitoring/auditing service as long as the monitoring service is not involved in the control itself). *Monitoring management* is the activity (manual, semi-automated or perhaps fully automated) that starts with deriving process patterns from a given SOLL model. The monitoring management turns the monitoring into an adaptive process by adapting and extending the process patterns on the basis of the feedback that it gets from the processing. Adaptations can be in the form of new patterns actively monitored or in adapting existing patterns, e.g. to make the collecting more efficient. Currently, the adaptation should be seen as a manual process (but see below).

The CM service such as depicted in Fig. 1 is first of all a tool that works on the process instance (data) level. However, type level (i.e., design) evaluation can be implemented using the same service architecture, but with different process patterns. The type level REA layer consists basically of (quantified) duality axioms and other “continuity equations” [25] that relate aggregated variables (e.g. total “cash inflow” or “inventory level”). These continuity equations don’t need to be specified manually but are derived automatically from the SOLL REA model. Evidently, type level control patterns are evaluated not continuously, but periodically, although the period does not need to be as long as a year or quarter.

At the moment, there are several techniques for process mining available, and powerful SQL-like Event Processing Languages that can be used to express process pattern conditions (e.g. [26]). Still, there are several opportunities to extend the CM model. We describe what we see as the three most important ones:

1. The CM service can be strengthened by including a *validation* step. Research studies in the practice of embedded audit modules [2] found that they tend to give a huge list of false positives. As this may threaten the usability, it is better to make a distinction between process patterns that *identify* a certain event and process patterns that can be used to *validate* it, using independent evidence. Depending on the application, the evaluation can be performed on validated IST models only.
2. EAM modules and event-driven service busses usually take an event trace to be a record of structured numeric data. However, it is possible to widen the scope and include communication events such as emails, discussion groups, social media (Facebook) updates etc, and mine the text content as well. *Text mining* is still in an experimental phase, but there are already some results (e.g. [17]).
3. The basic CM service described here already supports what Hunton and Rose [13] call *dynamic auditing*, where the configuration of the monitoring service is not fixed but adaptive. The monitoring management service implements a diagnostic control loop, but with manual adaptation. The next step is self-adaptation. According to [27] a self-adaptive management service should be built as a rule-based system, where rules do not only specify under which conditions which adaptations have to be made, but also the assumptions behind the rule. The assumptions are continuously checked by a special management subservice, typically using external sources, e.g. on economic and political news. For instance, in the case of political unrest in the country of origin of a certain cargo, the standard risk assessment rule may have to be replaced by a stricter variant.

3.4 System-based Auditing

System-based auditing is already known since the ‘70s of last century. Basically, it means that the auditee shows that he is “in control” of the processes in question. Being in control means that the process is guaranteed to comply with the control norms (SOLL model) and/or that all deviations are known and addressed. This implies that the auditee has a full specification of the process including built-in controls and a complete fault list. When the process is fully automated, it is not too hard to get assurance that such a full specification is also executed, when the correct functioning of the software has been assured by IT auditing.

In a *service-oriented system-based audit*, an independent audit service continuously monitors both the auditee's process specification and the fault list upon changes. In an extended form, the monitoring also includes the governance process of reacting to deviations (the follow-up of the fault list) and adapting the specifications, according to a SOLL model of the management process. In that respect, it helps when the management is implemented as a semi-automated service itself, like the CM service above. So in that case, the auditee has a CM service as in Fig. 1, including the monitoring management, and the auditor (say, Customs) has a CM service that monitors the first one.

4 Service-oriented Customs Control

This section draws upon the Service-Oriented Auditing approach of section 3 to identify innovative web services for Customs control. We start with a top-down analysis of the Customs services and their requirements as collected in section 2.

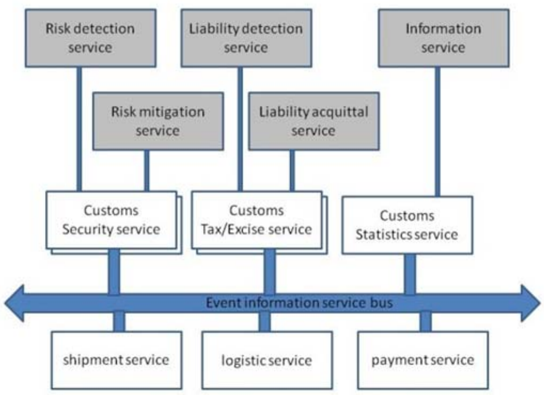

Fig. 2. Customs as a Service – global view

The main services identified are Security, Tax/Excise and Statistics. The value of a security service is that it aims at mitigating security risks, where we use Keeney's widely cited definition of risk as "the possibility that human actions or events lead to consequences that harm aspects of things that human beings value". In other words, a security service creates value by preventing the value of certain resources to be diminished. Tax and Excise services create monetary value by collecting payable duties. Customs statistics service creates value in the form of useful information, either directly to interested actors or via other governmental statistics offices. All these services are somehow related to cross-border supply chains, in which we can distinguish many business events, such as shipment, transport and payment.

The three main Customs services are complex services that make use of a limited number of generic core services. So far, we have identified five core services: risk detection, risk mitigation, liability detection, liability acquittal, and information (Fig. 2). An *information service* provides aggregated data based on all the events that it monitors. So far, this information takes the form of standard regular reports. In the future, service-oriented solutions will be possible in which the data don't need to be pushed, but can be pulled anytime by any (authorized) interested actor, according to user-defined queries (with a similar structure as the process patterns described in 3.3), and including drill-down functions to higher levels of detail. Customs tax and excises are raised according to law-governed *liabilities*. A major distinction can be made between the *detection* or creation of liabilities and their *acquittal*. We will come back to these below. A *risk detection* service is a Continuous Monitoring service such as defined above where the SOLL model is based on values to be protected, and the IST model contains a context model of all relevant events. A *risk mitigation* service takes measures to mitigate risks, e.g. by inspections or interventions.

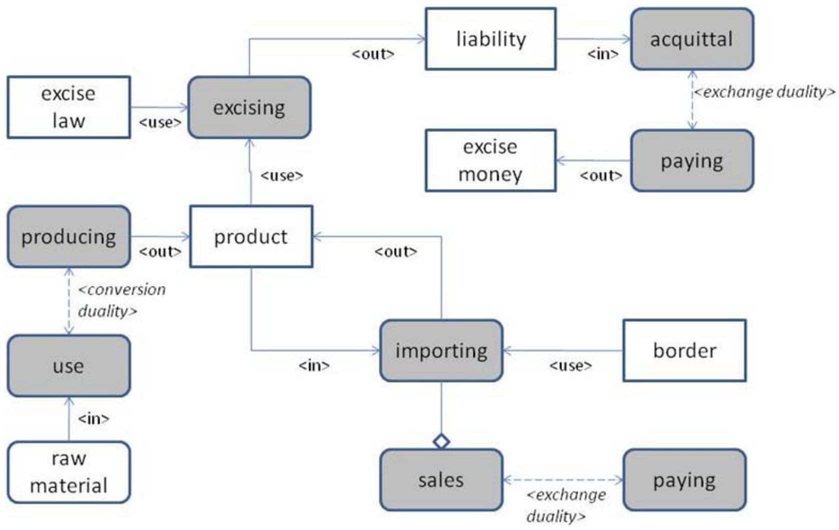

Fig. 3. REA model of excise liability life cycle

4.1 Excise management

As an example of liability detection and acquittal, we consider the case of excise management. Excise taxes are classified by the OECD as being those taxes which are "levied on particular products, or on a limited range of products … imposed at any stage of production or distribution and are usually assessed by reference to weight or strength or quantity of the product, but sometimes by reference to the value". In his description of key controls in excise administration, Preece [24] distinguishes between liability creation events and liability acquittal events. Liability is created not only by import, but may also be created by returns of deliveries, manufacturing, gains during storage or manufacturing, and bonded receipts. Liability is acquitted not only by payment, but may also be acquitted by export, bonded sale, manufacturing into new products, detoriation and losses during storage or manufacturing. Fig. 3 provides a REA model of the liability life cycle.

At the top-right, we have modeled the fundamental exchange duality between liability acquittal (in the form of a charge) and payment. This duality is a typical example of many e-government interactions with business. The acquittal process itself – including standard legal provisions for objections etc. – and the payment handling follow standard business process patterns, and it is seems very well possible that not the Customs agency itself, but a central government service takes care of this part. This does not apply to the other ways in which an excise liability can be acquitted.

The pièce de résistance is the *creation* of liability. In the model we have represented this as the "excising" event. Essentially, levying an excise draws on excise law and is attached to products (rather than to events), but triggered by events such as the production or importing. In an EISB approach, there are different ways to implement the excising event. Customs may install a rule-based decision service that monitors the EISB for the relevant events, such as "importing" in order to generate excise events that can be picked up by the acquittal service. Alternatively, companies with AEO status can include such a decision service in their own system, and Customs only needs to perform a system-based audit to check whether it is configured correctly. From an audit perspective, it is useful and often necessary to consider the generating events in a broader context. In the case of production, there is a conversion duality with the material used in the industrial production process. Importing is part of a sales process, which can be used either as independent evidence of primary source. Sales have an exchange duality with the payment, yet another independent evidence.

4.2 Security management

Shortly after 9/11, the US Customs Container Security Initiative (CSI) and Customs - Trade Partnership Against Terrorism (C-TPAT) were announced. The philosophy of C-TPAT is two-sided: on the one hand, cooperate with international trade actors to improve the security of their supply chains; and on the other hand to focus efforts and resources on potentially high-risk consignments that do *not* form part of such a secured supply chain.

The new instruments available to security management are manifold. A first distinction can be made between risk mitigation services and risk detection. Risk detection – using the CM model – can be split up in collecting, processing and evaluation. For *collecting*, a whole range of new technologies are upcoming, such as smart containers, high-energy scans, low-energy scans and GPS. Using an EISB, the monitored events can be published over the whole supply chain (although some optimization of the data distribution will be a necessary feature of the bus). As argued by Hesketh [11], current Customs "fail to recognize the strategic importance of accurate data at the point of consignment completion and export. An importer is not best placed to make a legal declaration about goods packed by the consignor". To increase safety, it is absolutely necessary to have information that can only be provided by the consignor who "packed the box". At the *processing* level, it is possible to use crime script analysis and artificial intelligence techniques [19]. Risk *evaluation* is based on risk norms. In principle these norms are derived from governmental regulations, but at the operational level it is necessary to make use of built-up experience. For the first part, it is possible to make use of legal document management services such as described in [3] for the latter the use of machine learning techniques is becoming indispensable.

The risk detection service is to be developed by each country in isolation, but such a service can greatly benefit from being integrated in an international network that exchanges risk events, crime scripts and some of the learned risk norms in a swarm intelligence style [20].

5 Conclusions

Customs control is in a massive transition process of innovation and reorganization. In this paper, we have shown that a service-oriented architecture can foster this transition by providing a flexible and adaptive integration platform. We have introduced a service-oriented auditing module that combines REA business modeling with adaptive Continuous Auditing techniques. Its application to Customs control looks promising. It allows for a loose integration of software services across the supply chain, between traders and government, and among governmental agencies.

The service-oriented auditing module is a starting point only. It is necessary to substantiate it further by actually selecting and combining the techniques mentioned above into real audit services and by developing standardized interfaces. As far as REA is concerned, more research is needed on extending its applicability from a single company to a business network or chain. Another topic for future research is the development of an analytic tool to analyze the effectiveness and efficiency of monitoring and auditing configurations in a sound and systematic way.

6 Acknowledgements

This research is supported partially by the DINALOG project Extended Single Window (www.dinalog.nl).

References

1. Aalst, W.M.P. van der, Hee, K. van, Werf, J.. van der, Verdonk, M.. Auditing 2.0: Using process mining to support tomorrow's auditor. *Computer*, *43*(3), pp.90-93 (2010)
2. Alles, M., Kogan, A., Vasarhelyi, M., Putting Continuous Auditing Theory Into Practice: Lessons from Two Pilot Implementations. Journal of Information Systems 22.2. pp.195-214 (2008)

3. Boer, A., T. van Engers, and R. Winkels. Traceability and change in legal requirements engineering. In P. Casanovas et al, editors, *AI Approaches to the Complexity of Legal Systems*. Springer LNCS (2010)
4. Carnaghan, C., Business Process Modeling approaches in the context of process level audit risk assessment: an analysis and comparison. *Int. Journal of Accounting Information Systems* 7, pp.170-204 (2006)
5. Chang, C.J., Ingraham, L.R., *Modeling and Designing Accounting Systems: Using Access to Build a Database*. Wiley (2007)
6. Debreceny, R.S. et al. Embedded Audit Modules in Enterprise Resource Planning Systems: Implementation and Functionality. Journal of Information Systems, 19(2), pp.7-27 (2005)
7. Gal, G., McCarthy, W., Specification of internal accounting controls in a database environment, *Computers & Security*, Volume 4, Issue 1, pp.23-32 (1985)
8. Gal, G., Geerts.G., McCarthy W., *Semantic Specification and Automated Enforcement of Internal Control Procedures within Accounting Systems.* Presentation at 3rd VMBO Workshop (Value Modeling and Business Ontologies), Stockholm, (2009)
9. Graco, W., Semenova, T., and Dubossarsky, E.. Toward knowledge-driven data mining. In *Proc. of the 2007 Int. Workshop on Domain Driven Data Mining* (DDDM '07). ACM, New York (2007)
10. Hesketh, D., Seamless electronic data and logistics pipelines shift focus from import declarations to start of commercial transaction. *World Customs Journal* 3(1), pp.27-32 (2009)
11. Hesketh, D., Weaknesses in the supply chain: who packed the box? *World Customs Journal* 4(2), pp.3-20 (2010)
12. Holmes, T. Zdun, U. Daniel F. and Dustdar, S.. Monitoring and Analyzing Service-based Internet Systems through a Model-Aware Service Environment. In: B. Pernici (Ed.), *Proc. CAiSE 2010,* Springer (2010)
13. Hunton, J. E., Rose, J. 21st Century Auditing: Advancing Decision Support Systems to Achieve Continuous Auditing. *Accounting Horizons*, *24* (2), pp.297-312, (2010)
14. Kogan, A., Sudit, E. and Vasarhelyi, M. Continuous online auditing: a program of research, *Journal of Information Systems*, Vol. 13, pp. 87-103 (1999)
15. Lee, R.M., Bons, R.W.H, Wagenaar, R.W. Pattern-directed Auditing of Inter-organisational Trade Procedures, In: B. Schmid et al (Eds.) *Towards the e-Society: First IFIP Conference on E-Commerce, E-Business, and E-Government, I3E* 2001, Kluwer Academic Publishers (2001)
16. Li, S.H, Huang, S.M., Lin, Y.C, Developing a continuous auditing assistance system based on information process models. *Journal of Computer Information Systems*, Fall (2007)
17. Ma, Z., O. Sheng, and G. Plant. Discovering company revenue relations from news: A network approach. *Decision Support Systems* 47: pp.408–414 (2009)
18. McCarthy W.E., The REA Accounting Model: A Generalized Framework for Accounting Systems in a Shared Data Environment. *The Accounting Review* (1982).
19. Hermanson, D. R., B. Moran, C. Rossie, and D. Wolfe. Continuous Monitoring of Transactions to Reduce Fraud, Misuse, and Errors. *Journal of Forensic Accounting*: pp.17-30 (2006)
20. Kennedy, J. R., Eberhart, C. and Y. Shi. *Swarm Intelligence*. Morgan Kaufmann (2001).
21. Murthy, U, Groomer S., A continuous auditing web services model for XML-based accounting systems, *Int. J. of Accounting Information Systems*, Volume 5, Issue 2, pp. 139-163 (2003).

22. Papazoglou, M.P. & W.J. van den Heuvel, Service oriented architectures: approaches, technologies and research issues, *VLDB Journal*, Vol.16 (3) pp.389-415 (2007).
23. Peffers, K., Tuunanen, T., Rothenberger, M., and Chatterjee, S. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), pp.45-77 (2008)
24. Preece, R. Key Controls in the Administration of Excise Duties. *World Customs Journal* 2(1), pp.73-92 (2008)
25. Vasarhelyi, M. Alles M. and A. Kogan, Principles of analytic monitoring for continuous assurance, *J Emerg Technol Account* 1 (1), pp. 1–21 (2004)
26. Wu, E., Diao, Y. and Rizvi, S. High-performance complex event processing over streams. In *Proc. of the 2006 ACM SIGMOD Int. Conf. on Management of data* (SIGMOD '06). ACM, New York, NY, USA, pp.407-418 (2006)
27. Weigand, H. Johannesson, P., Andersson, A., Arachchige, J., Bergholz, M. Management Services - a Framework for Design. In: H. Mouratidis, C. Rolland (Eds.) Proc. CAiSE 2011, Springer (2011)