Continuous Control Monitoring-Based Regulation: A Case in the Meat Processing Industry

Joris Hulstijn[1,3], Rob Christiaanse[2], Nitesh Bharosa[1], Friso Schmid[3],
Remco van Wijk[1,3], Marijn Janssen[1], and Yao-Hua Tan[1]

[1] Delft University of Technology
[2] VU University
[3] Thauris B.V., The Hague
j.hulstijn@tudelft.nl

Abstract. Regulation based on Continuous Control Monitoring could reduce the administrative burden for companies. Often, companies already have elaborate internal control and quality management systems. Instead of periodic physical inspections, regulatory supervision can partly be automated and performed on a continuous basis. The regulator gets access to a validated copy of key data elements from the company's internal information systems, which serve as indicator of compliance to specific control objectives. In this paper we describe an information architecture for continuous control monitoring, and show how it can be applied to supervision of regulatory compliance. The approach is illustrated by a pilot project in the Netherlands of applying continuous control monitoring to food safety regulations in the meat processing industry. Participants concluded that the approach is technically feasible but requires a different mindset towards regulation, and a clear business case.

Keywords: Regulatory Compliance, Continuous Control Monitoring.

1 Introduction

In the wake of the financial crisis there is a call for more and more stringent regulation on financial institutions. Also in other sectors such as health care or food processing, there is an increase of governance guidelines and regulations. In particular after incidents, new regulation is introduced. Power [1] calls this the audit society. As a result, companies must keep an increasing amount of records to demonstrate compliance with laws and regulations, as well as corporate standards and guidelines. Regulators, on the other hand, are under political pressure to provide more security, i.e. reduce risks for society [2], while reducing costs and administrative burden for businesses. One way to deal with these contradictory regulatory demands is by information systems. In particular, information systems may help with evidence collection and analysis. Key data elements which are indicators of compliance to specific control objectives are monitored automatically, on a continuous basis. This approach is called *continuous assurance* or *continuous control monitoring* (CCM) [3-5]. CCM can be applied to any kind of control system, be it financial, quality or safety related. We are especially interested in the following research question:

C. Salinesi and O. Pastor (Eds.): CAiSE 2011 Workshops, LNBIP 83, pp. 238–248, 2011.

How can we apply continuous control monitoring to improve regulatory compliance?

In this paper we discuss five design principles (pillars) for continuous control monitoring, and show how they can be applied to improve regulatory compliance. When CCM is specifically applied to control objectives derived from laws and regulations, we call it Continuous Control Monitoring-based Regulation (CCM-R).

Consider the norm in the meat processing industry that, in order to prevent diseases like BSE, animal waste may not re-enter the food chain. To demonstrate adherence to this norm we need to oversee the whole supply chain. By using a standard data representation format like XBRL with a shared semantics, we can compare data from different parties, even when underlying commercial data is stored in different formats. This allows reconciliation over the supply chain and makes it possible to verify completeness as well as accuracy. To model the flow of goods we use Starreveld's [6] value cycle. For example, the sum total of waste from slaughterhouses in a region, should equal the sum total of waste entering the certified destruction company for that region. If not, some waste is not accounted for. To detect unreported waste for a slaughterhouse requires spanning reconciliation: comparing the ingoing (animals) and the outgoing flow of goods (meat products and waste), according to normative ratios.

The design principles are illustrated by a pilot project of applying CCM-R in the meat processing industry in the Netherlands. The pilot shows that developing a system for CCM-R is a complex social process. We discuss technical design issues as well as challenges concerning legal and social aspects.

The remainder of the paper is structured as follows. In Section 2 we discuss our vision of continuous control monitoring, and show how it can be applied to regulatory compliance. In Section 3 we discuss the pilot project in the meat processing industry. The paper concludes with lessons learned.

2 Continuous Control Monitoring-Based Regulation

In brief, our vision on CMM-R is as follows. On the basis of key performance indicators (KPI) the continuous control monitoring system verifies on behalf of the regulator whether production proceeds in a controlled manner and whether regulations are being followed. The monitoring system will signal exceptions and report them to the regulator. Irregularities must be explained – proactively or on the basis of additional queries by the regulator. In case of incidents, the system shows whether countermeasures were implemented successfully and production resumes its regular pattern. Companies which sign on to such a 'heartbeat monitor' signal that they are able to control the process and are willing to be transparent.

The CCM-R vision rests on five principles, or pillars: (1) automated verification, (2) continuous monitoring, (3) verification over the supply chain, (4) internal control and (5) regulatory policy. Although we believe all pillars are necessary to realize the full potential of CMM-R, the pillars can also be seen as dimensions which describe specific regulatory settings. For instance, without (5) we get commercial mechanisms for controlling quality in a supply chain. Without (3) we get regulation focused on individual companies. Without (1) and (2) we get old fashioned manual auditing.

2.1 Automated Verification

To verify controls build into computer systems, an auditor generally takes original data from the system and puts it into a simulation tool, which runs a set of test transactions. The simulation represents behaviour expected on the basis of standards and guidelines ('soll'). The results are compared to the results of actual behaviour ('ist'), taken from the computer system. Outcomes which do not align are called exceptions, which either need to be explained or dealt with. An exception may not necessarily amount to a violation. Guidelines could be incomplete or underspecified. For example, in supply chain management, the return flow of goods often raises exceptions. Guidelines do not specify under what account returns should be booked.

Parties need agreement about the key performance indicators to be verified, and about the specific norms or standards to verify them against. The indicators should be selected to provide evidence of the main control objectives, which are again derived from the original rules and regulations, as well as from requirements suggested by experts and other stakeholders. Note that not all data needs to be reported. For example, to measure hygiene, a general requirement for meat processing plants, only a few indicative microorganisms need to be measured and reported[1] [7].

We consider three ways in which compliance can be demonstrated, compare [8]. First, evidence of performance itself. For instance, low microorganism levels indicate that hygiene is being observed. Second, evidence of actions or control measures being in place, which should normally result in the stated objective. For instance, records that the floor is being cleaned regularly twice every day. Third, evidence of competence of staff, which should result in the objectives being actively observed. For instance, evidence that all staff have followed the hygiene-at-work course.

2.2 Continuous Monitoring

Vasarhelyi and colleagues [3-5, 9-11] have been an ardent proponent of what was initially called continuous auditing. Continuous auditing is defined as "a methodology for issuing audit reports simultaneously with, or a short period of time after, the occurrence of the relevant events" [12]. Crucial is the frequency of reports, and the fact that the flow of events may still be adjusted. The term continuous auditing may seem odd, suggesting a human auditor being present, but in fact it refers to continuous confrontation of data to a norm. The approach is also called continuous assurance [10], as the objective is to provide assurance that objectives are met, on the basis of a system of control measures and continuously monitoring their effectiveness.

In Figure 1 we show an architecture for continuous assurance adapted from [3]. Although very general, this overview already highlights some design choices. First, data is drawn from the company's enterprise information system at the application layer; not from the database. This would be impossible both for legal reasons (auditors may only access company data with approval) and security reasons (no one may access data directly, only through the application layer). Second, performance data is stored in a separate database, under control of the auditor. This database also contains the audit trail (way it was obtained). In this way the auditor can perform his

[1] For example E. Coli shows whether water is polluted with faecal material, and the presence in food of Staphylococcus Aureus generally indicates contamination from human handling.

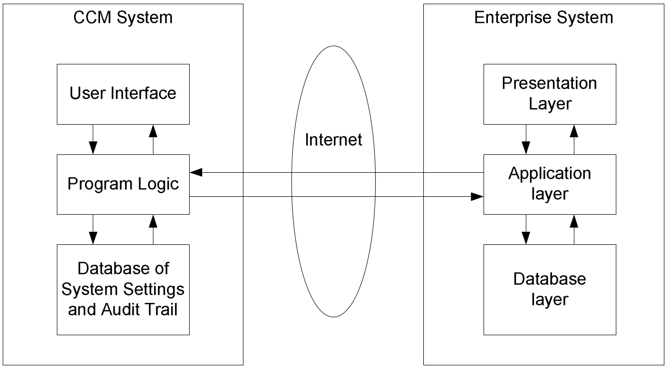

Fig. 1. Generic architecture for continuous assurance, based on Alles et al [3]

or her analysis independently of the host. Data can be queried, stored and retrieved using analytic tools built on top of a usual DBMS. Third, the CMM system is controlled by a module containing the 'Program Logic' specifying auditing behaviour: which data to take from the system, how to store and how to manipulate it. The complete CCM system is controlled by a user interface. More elaborate compliance architectures are provided by Lotz et al [13] and Accorsi et al [14].

Kogan et al. [5] discuss the trade-off between *control-oriented* and *data-oriented* procedures for continuous auditing. The first approach is also known as system-based auditing; it relies on a coherent system of internal control measures. Provided that such measures are in place, the idea is that less effort can be spent on substantive testing. Consider the audit risk model [15], but see [17] for a critical discussion.

audit risk = *inherent risk* × *control risk* × *detection risk*.

Inherent risk is the risk that misstatements or violations occur in the first place. This is beyond the control of the auditor. Control risk is the risk that control measures do not prevent, or detect and correct a misstatement or violation. Detection risk is the risk that remaining misstatements or violations are not detected by the auditor. In case of strong preventative internal controls, the auditor can perform less inspections or substantive tests, while keeping the net audit risk within acceptable boundaries. This suggests adopting application controls in information systems which leave little room for error or manipulation: *compliance by design* [16]. However, especially with modern business intelligence tools, focused data analysis can also be very powerful. Given basic data reliability guaranteed by information technology and the presence of irreplaceable preventative controls (i.e. segregation of duties, identification and authentication, audit trail), data analysis can establish misstatements efficiently.

2.3 Reasoning and Reconciliation over the Supply Chain

Once we have a continuous stream of performance data being monitored, there are several kinds of reasoning which can be used to establish compliance. Here is a brief overview of what can be done, for individual companies:

- **Time series and trends**: is performance improving? Is performance developing in a natural way, or are there abrupt changes, indicating bold interventions?
- **Alerts and red flagging**: when performance reaches some critical level, an automated signal can be generated. Sometimes, a combination of critical factors taken together may be evidence of an increased risk of a disruption.
- **Reconciliation:** different variables can be reconciled, based on the underlying causal, fiscal, or trading relationships [6, 17]. For example, the number of test samples in the laboratory for a given day, should equal the number of animals being slaughtered, as counted by independent sources.

Once we have data assembled from several different companies, spanning part of the supply chain, we can also perform the following kinds of reasoning.

- **Benchmarking**: comparing performance to peers in the same sector, or to previous performance of the same plant. For example, it could be determined that on average, for each animal, 4 kilograms is left over as Category 1 waste. This produces a normative ratio that can be used in reconciliation.
- **Reconciliation over the supply chain:** variables from different trading partners can be compared. Output from one party should equal the input for subsequent parties in the chain. In particular when some parts of the chain are controlled, this can be used to establish completeness, as well as accuracy of the reported data.

The underlying theory of reconciliation is based on Starreveld [6], commonly taught in Dutch accounting courses. See Blokdijk et al [18] for an English introduction. Our exposition here is based on Christiaanse and Hulstijn [19] .

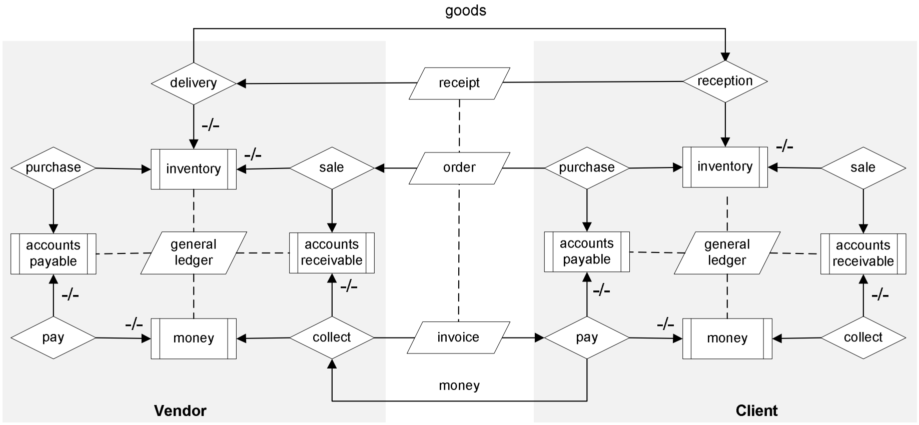

Fig. 2. Interconnected value cycles of vendor and client with communication

Essentially, each business can be modelled as a value cycle: interconnected flows of money and goods. Figure 2 shows two interconnected value-cycles of a vendor and a client, both trading companies. For other sectors (production, service industry), other typologies are known. We use the following notation. Decisions (authorizations) are indicated by a diamond. An actual decision is an event or change of state. Double rectangles are states of a certain value to the company, such as inventory or accounts payable. Records of states, i.e. accounts, are related through reconciliation relationships, indicated by dashed lines, which come together in the general ledger. Influence is indicated by arrows. The sign, '+' or '–/–', indicates an increment or decrement of the corresponding account, where '+' is often left out. Thus, a purchase leads to an increment of the accounts payable, while the purchased goods are added to the inventory. A sale leads to an increment of the accounts receivable and a decrement of the inventory, etc. Messages representing economic transactions are also shown. A typical reconciliation relationship (3-way match) holds between invoice, purchase order and receipt, i.e. evidence of the arrival of the goods.

In Starreveld's work [6] there are two general 'laws'. First, the *rational relationship between sacrificed and acquired goods* states that, for all events *e* such that *s <e> t* in Fig 2, the values of *s* and *t* before and after an event are related in a rational way.

(1) $incr(e,t) = f \bullet decr(e,s)$, for some normative ratio f.

For example, if we look at a sales event, we have: *increase in accounts receivable* = *sales price* • *decrease in inventory*. Second, the *relationship between state and events* holds that, for all states *s*, the value at the end of a period should equal the value at the beginning, with all increments added, and decrements subtracted.

(2) $s_{\text{begin}} - s_{\text{end}} + \Sigma_e \, incr(e,s) - decr(e,s) = 0$

For example, inventory at the end of the day should equal inventory in the morning, with all goods received during the day added and all cleared goods subtracted.

A similar role to these laws is played by what Vasarhelyi et al [10] call continuity equations. Griffoen et al [17] use Petri nets and equation modeling to capture these constraints. Crucial is that these reconciliation equations can be used to verify compliance, also in non-financial domains. In commercial traffic, trading partners usually have *opposed interests*: a buyer prefers a low price and a high quality, a seller prefers the opposite. Therefore each party will carefully verify data. Original data from commercial traffic are therefore relatively trustworthy, at least more than reports filed with the only purpose of being compliant. This may be called the piggy-backing principle: compliance rides along on the back of commercial traffic [20].

2.4 Trust and Internal Control

Like in various other forms of self-regulation, e.g.[21, 22], in CCM-R the regulator must rely on evidence provided by the company being controlled. That means that the regulator should be able to distinguish those companies which are 'in control' and can be trusted to provide reliable information, from those which are not. Often this is achieved through some form of certification based on an elaborate audit. Compare AEO certification for trusted companies in European customs legislation [22].

When do we say that a company is 'in control'? One can take the feedback-control loop from engineering, and apply it to management. An influential exponent is Deming's plan-do-check-act cycle [23]. Similar ideas can be found in total quality management (TQM) [24]. The ability to learn and improve is a property of the organization as a whole. Capability maturity models (CMM) can be used to assess the maturity level of an organization in a specific domain, for instance software development [25]. CMM distinguishes the following levels: 1. Initial (ad hoc), 2. Repeatable, 3. Defined, 4. Managed, and 5. Optimizing. At level 3 and higher the organization is ‘in control’: they can make sure that business objectives are being met.

2.5 Regulatory Policy

Regulatory agencies are under pressure to cut costs, but on the other hand to protect the interests of society, such as safety, security and financial stability. In many cases, regulatory policies have developed historically and need not be optimal.

The regulator should try and spend most inspection and enforcing effort on those companies, which generate risks for society. The underlying decision to inspect, or after incidents, to enforce is *risk-based*. Based on evidence of company behaviour, location and kind of business, the likelihood and impact of violations are estimated.

Similar to responsive regulation [21], the regulatory policy is adjusted to the behaviour of the company being regulated (Table 1). A company should be both willing and able to comply. Being in control is an indicator of being able to be compliant. Companies which are not in control and not compliant are a risk to society, and should be guided towards the left, or else the license withdrawn. Companies which are in control, but not compliant, are apparently able, but not willing to comply. Here enforcement (sanctions) might work. Companies which are not in control, but (trying to be) compliant, should be assisted in improving their internal controls. The regulator could refer to best practices from branch organizations. Strict enforcement would be counter-productive. Finally, companies which are in control and compliant, need less regulatory intervention. Here the number of inspections can be reduced without fear for public safety.

Table 1. Regulatory approach towards companies based on being in control and compliant

	Compliant	**Non Compliant**
In Control	Advance Guard, = > reduce inspection effort (e.g. less physical inspection)	Opportunistic, = > enforce compliance (e.g. apply sanctions)
Not in Control	Struggling, either compliant by accident, or only with additional effort = > assist in improving controls	Rough trade = > put out of business (e.g. withdraw certificate)

In addition, in all cases the regulator must regularly audit the implementation of the CMM-R system and underlying internal controls, in order to make sure the system is not only internally consistent -- all transaction performed according to specification-- but also externally consistent: reported data actually connect to the real world.

3 Pilot Study: CCM-R in the Meat Processing Industry

We report on a recent proof of concept of CCM-R. Figure 3 gives a general overview of the parties involved in the meat processing industry in the Netherlands. On the left, the food chain starts with agriculture producing crops which are converted and sold as foodstuffs. Farms raise cattle or pork, which are slaughtered at the slaughterhouse and sliced into cuts by meat packing firms, according to demand from retail. Those pieces which are left over (by-products), as well as dead animals which are unfit for consumption (ill, contaminated by manure), are taken to a certified destruction company. Generally by-products are re-used industrially; for example gelatine is an important rest product. All parties keep computerized registrations of transport of goods, much of which is regulated. On the right we see the various regulators in the meat processing industry, among which the Food and Consumer Product Safety Authority (VWA) which oversees animal welfare and food safety.

The main safety concern in the meat processing industry is that animal waste and by-products not fit for human consumption, will not re-enter and contaminate the food chain. Among other reasons, this is to prevent illnesses like BSE (mad-cow disease). A strict separation is maintained between meat and by-products (red and blue factory lines). So called Category 1 and 2 by-products (for example some organ tissue like brains, bone marrow, unwashed intestines, semen, milk, contaminated meat) must be kept separate. This material may only be transported and be disposed of through the services of a certified destructor firm, see EC 1774/2002 [26]. Category 3 by-products (like left-over meat, blood, hide, hoofs, etc. of healthy animals) may be transported and processed by category 3 destructors, of which there are several.

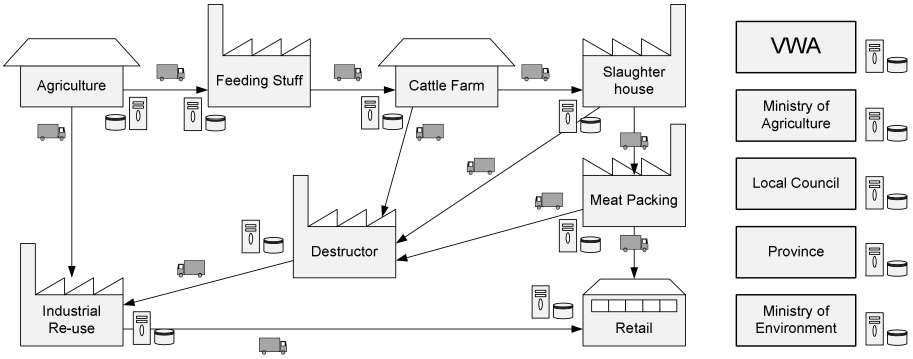

Fig. 4. Simplified overview of the flow of goods in the meat processing industry

3.2 Pilot Project

To test the viability of CMM-R in the meat processing industry a number of parties collaborated to develop a proof of concept[2]. Participants were two slaughterhouses, one for pork and one for beef, a Category 1 and 2 destruction plant, a Category 3 destruction plant, the Food and Consumer Product Safety Authority (VWA). The pilot focuses on information being exchanged concerning regulations EC 1774/2002 [26] explained above, and EC 2073/2005 [27], which is about microbiological criteria for food, in order to promote hygiene and protect public health. A project organization

[2] See: http://sggv.nl/casussen/sggv-in-de-vleesindustrie/omschrijving, accessed 02/Feb/2011.

was set-up, with experts on the regulatory domain (by-products, microbiological criteria), and experts of process optimization and technical support. The project took seven months, during which requirements were drawn, prototypes build and tested, and a practice test was performed to the satisfaction of two auditors of VWA.

The pilot feasibility test used XBRL as standard data representation format, and the Netherlands Taxonomy (NT) as definitions for the semantics of reports. A specific extension of the taxonomy was developed for microorganism samples (EC 2073/2005) and by-products bookkeeping (EC 1774/2002). Although it may seem a long detour to use a data standard intended for financial reporting in the meat processing industry, it turned out to be a good choice. Required knowledge about meat processing was limited to knowledge of the way a piece of meat is classified as category 1 or 2 (must be destroyed) or category 3 (may be re-used), and to how microorganism samples are being taken. Required expertise relates to the practices used to make sure records are also externally consistent, i.e. connect to reality.

The pilot used a gateway for secure exchange of compliance reports, built according to the GEIN reference architecture (GEneric INfrastructure) used in Dutch Government. The same architecture is used in the gateway for uploading XBRL reports to Dutch government agencies, like tax office, bureau of statistics and filing the annual financial statements. The gateway is built using open standards, in particular services for SOAP and web interface definitions, and BPMN for process definitions (both manual and technical). The gateway also provides database functionality for storing, querying and retrieving messages, and for archiving.

3.3 Results

Participants in the pilot feasibility test concluded that the CCM-R concept is indeed viable, in the sense that the XBRL data definitions, message reports, interface connections and auditing procedures performed as intended.

However, participants also agreed that to make this into a success, a mind-shift is needed. Many auditors in VWA are trained as veterinary surgeons. They have always been checking meat processing from within the slaughterhouse. From numerous incidents, they have learned to mistrust meat processing firms. As all good auditors, they are sceptical by nature, whereas CCM-R requires a certain level of trust in the professional conduct of meat processing firms. A particular example concerned the audit of the practice test. How do you audit something new? The auditors who had to assess the proof of concept found it hard to come up with suitable assessment criteria. This underlines the need for a general audit model suitable for CCM solutions.

Another outcome concerns the business case. The pilot project was funded by the Ministry of Economic Affairs. In a real situation, meat processing firms would need a clear incentive – reduced inspections – in order to join. One participant in the project already has a very elaborate quality management system. They would like CCM-R to force less advanced and cheaper competitors out. Another participant entered the project much more opportunistically: they can see the economic benefit of less physical inspections. Currently, inspections are compulsory and performed by VWA, but paid by the meat processing firms themselves.

4 Conclusions

Continuous control monitoring can be applied to regulatory compliance, to make it more efficient and possibly more effective. In this paper we presented five ‘pillars’ of applying CMM to business regulation: (1) automated verification, (2) continuous monitoring, (3) verification over the supply chain, (4) internal control and (5) regulatory policy. These pillars can also be seen as independent dimensions characterizing specific regulatory situations. For instance, without (4) we get direct supervision of performance by the regulator, as for instance in monitoring pollution.

A pilot study in the Netherlands shows that CCM is technically feasible. In particular, existing data representation formats and message infrastructure protocols can be either reused or can be relatively easily adapted where needed (XBRL). Legal barriers can be overcome, by having the company voluntarily supply data, instead of the regulator pulling data out of commercial systems directly. Furthermore the pilot project illustrates the general idea: that CMM allows for more effective audits, with less physical inspections and therefore in the long run potentially less costs.

On the other hand, the pilot has revealed some non-technical challenges in the realization of CCM-R. A significant challenge is that of trust. Like other forms of self-regulation, CCM requires trust in the reliability of the data supplied by the company. Auditors are sceptical about reliability of automated controls. In addition, there is a need for a general audit model which fits system-based auditing approaches and CCM solutions. Another potential barrier is uncertainty about investments and the business case for joining a scheme like CCM-R.

Acknowledgments. We would like to thank the Food and Consumer Product Safety Authority (VWA) for their cooperation in this project.

References

1. Power, M.: The Audit Society: Rituals of Verification. Oxford University Press, Oxford (1997)
2. Beck, U.: Risk society – Towards a new modernity. Sage, London (1992)
3. Alles, M., et al.: Continuous monitoring of business process controls: A pilot implementation at Siemens. Accounting Information Systems 7, 137–161 (2006)
4. Alles, M., Kogan, A., Vasarhelyi, M.: Putting Continuous Auditing Theory Into Practice. Journal of Information Systems 22(2), 195–214 (2008)
5. Kogan, A., Sudit, E.F., Vasarhelyi, M.: Continuous online auditing: a program of research. Journal of Information Systems 13(2), 87–103 (1999)
6. Starreveld, R.W., de Mare, B., Joels, E.: Bestuurlijke Informatieverzorging (in Dutch), Samsom, Alphen aan den Rijn, vol. 1 (1994)
7. Notermans, S.H.W., Mead, G.C.: Microbiological Contamination of Food: Analytical Aspects. In: International Food Safety Handbook, pp. 549–566 (1999)
8. Eisenhardt, K.M.: Control: Organizational and Economic Approaches. Management Science 31(2), 134–149 (1985)
9. Vasarhelyi, M.A., Halper, F.B.: The Continuous Audit of Online Systems. Auditing: A Journal of Practice and Theory 10(1), 110–125 (1991)

10. Vasarhelyi, M.A., Alles, M., Kogan, A.: Principles of analytic monitoring for continuous assurance. J. of Emerging Technologies in Accounting 1(1), 1–21 (2004)
11. Alles, M.A., Kogan, A., Vasarhelyi, M.A.: Feasibility and economics of continuous assurance. Auditing: A Journal of Practice and Theory 21(1), 125–138 (2002)
12. CICA/AICPA, Continuous auditing, Research report, The Canadian Institute of Chartered Accountants (CICA), Toronto, Canada (1999)
13. Lotz, V., et al.: Towards Systematic Achievement of Compliance in Service-Orientied Architectures: The MASTER Approach. Wirtschaftsinformatik 50(5), 383–391 (2008)
14. Accorsi, R., Sato, Y., Kai, S.: Compliance monitor for early warning risk determination. Wirtschaftsinformatik 50(5), 375–382 (2008)
15. Knechel, W., salterio, S., Ballou, B.: Auditing: Assurance and Risk, 3rd edn. Thomson Learning, Cincinatti (2007)
16. Governatori, G., Sadiq, S.: The journey to business process compliance. In: Handbook of Research on Business Process Management, pp. 426–445. IGI Global (2009)
17. Griffioen, P.R., Elsas, P.I., van de Riet, R.P.: Analyzing Enterprises: the value-cycle approach. In: Database and Expert Systems Applications, pp. 685–697. Springer, Heidelberg (2000)
18. Blokdijk, J.H., Drieënhuizen, F., Wallage, P.H.: Reflections on auditing theory, a contribution from the Netherlands. Limperg Instituut, Amsterdam (1995)
19. Christiaanse, R., Hulstijn, J.: Neo-Classical Principles for Information Integrity. Faculty of Technology, Policy and Management, Delft University of Technology (2011)
20. Tan, Y.H., et al. (eds.): Accelerating Global Supply Chains with IT-Innovation. Springer, Berlin (2011)
21. Ayres, I., Braithwaite, J.: Responsive Regulation: Transcending the Deregulation Debate. Oxford University Press, Oxford (1992)
22. Burgemeestre, B., Hulstijn, J., Tan, Y.-H.: Rule-based versus Principle-based Regulatory Compliance. In: Governatori (ed.) JURIX 2009, pp. 37–46. IOS Press, Amsterdam (2009)
23. Deming, W.E.: Out of the Crisis. MIT Center for Advanced Engineering Study (1986)
24. Hackman, J.R., Wageman, R.: Total quality management: empirical, conceptual, and practical issues. Administrative Science Quarterly 40, 309–342 (1995)
25. Paulk, M.C., et al.: The Capability Maturity Model: Guidelines for Improving the Software Process. Addison-Wesley, Reading (1995)
26. EC, Regulation No 1774/2002 laying down health rules concerning animal by-products not intended for human consumption, European Parliament and the Council (2002)
27. EC, Regulation No 2073/2005 on Microbiological criteria for foodstuffs, The Commission of the European Communities (2005)