Conceptualizing Auditability

Hans Weigand[1], Paul Johannesson[2], Birger Andersson[2], Maria Bergholtz[2], Faiza Bukhsh[1]

[1] Tilburg University, P.O.Box 90153,
5000 LE Tilburg, The Netherlands
{H.Weigand,F.A.Bukhsh}@uvt.nl
[2] Stockholm University
Department of Computer and Systems Sciences, Sweden
{pajo,ba,maria}@dsv.su.se

Abstract. Compliance has become a strategic concern for many companies and organizations. To prove actual compliance, the organization must disclose itself (be auditable). A plethora of advanced tools has been developed to support compliance management and auditing processes. However, not all organizations are the same. To apply these tools effectively and efficiently, the organization itself and the maturity of its management control should be considered as well. The goal of this exploratory paper is to define auditability on a general conceptual level. We introduce four levels of auditability, where each level adds to the self-knowledge and being-in-control of the organization.

Keywords: auditing, REA, meta-control, customs control

1 Introduction

Business processes form the foundation for all organizations, and as such, are impacted by industry regulations. Without explicit business process definitions, flexible rule frameworks, and audit trails that provide for non-repudiation, organizations face litigation and reputation risks. Compliance regulations, such as HIPAA, Basel II, Sarbanes-Oxley (SOX) and others require organizations to review their business processes and ensure that they meet the compliance standards set forth in the legislation. The new control and disclosure requirements create auditing demands for the Information System (IS). The IS plays a crucial role in corporate governance, allowing the board to ascertain that internal control measures that govern their key business processes can be checked, tested, and potentially certified.

When compliance is a strong demand, the question how to optimize it becomes a strategic concern. In this context, the concept of "horizontal supervision" aims at transforming the traditional vertical relationship between government and business into one of collaboration with a common goal of both efficiency and legal compliance. Horizontal supervision is applied, among others, in the innovation of customs control [16]. To reduce administrative burdens, EC customs authorities have

developed the concept of Authorised Economic Operator (AEO). To receive the status of AEO, the company must have prepared and implemented a security and monitoring plan and taken initiative in reporting irregularities. In return, the customs authority will stop or reduce the number of audits of the administrative systems and the inspections of individual transactions. In this case, the ability to show compliance has measurable business value.

Business Process Management (BPM) and Business Process Activity (BPA) tools use to focus on business performance monitoring and continuous evaluation of process execution against service level objectives, depicting information about issues like bottlenecks, throughput and resource utilization in a graphical manner. This is not sufficient from a compliance point of view. As a reaction, we have recently witnessed substantive academic research on *compliance monitoring* [2,4,1,7] with several rigorous results that allow checking business processes at design time and at run time, and supporting reactive as well as proactive monitoring. However, little or no attention has been given to the question of how to embed these techniques successfully in the organizational context. Optimizing business value is more than compliance checking. Roughly in parallel to this academic research stream, we have seen a rapid growth of the GRC IS market, that is, software to support Governance, Risk and Compliance [3,18]. GRC software contains several functions, but the main emphasis is on the integrated management of all controls that often are scattered around the organization and hence hard to document, let only manage and optimize. For large organizations, this management is clearly useful, but applying this solution requires also a rethinking of the organization and its controls to be really effective.

In this context, the research objective of this paper is not to introduce new auditing or GRC tools, but to take a step back and conceptualize auditability first. In section 2, we develop a definition of auditability grounded in the REA business ontology. In section 3, we add a management control perspective and develop a framework of auditability. In terms of design research, this framework is the main artifact.

The practical relevance of this paper is that it allows organizations to become aware of the challenges of auditability, provides a possible roadmap to a higher auditability level and helps to understand the use of IT as enabler. However, our framework does not warrant a "one suits all" solution. The scientific relevance is that it provides a conceptualization and theoretical grounding in REA of an aspect that is of increasing importance to modern information systems, including cloud service solutions. The paper extends published research on value networks, service systems and management services, also using the REA business ontology as underlying conceptual framework.

2 Towards a Theory of Auditability

The classical work of Mautz defines (financial) auditing as being "concerned with the verification of accounting data, with determining the accuracy and reliability of accounting statement and reports" [8]. The starting-point for a theory of auditability is the auditing situation that can be described as follows. There are certain *value objects* (assets) and two parties that can be called *Principal* and *Agent* (as in agency theory [5]). The value object has value to the Principal as he is the owner or for some other

reason. The Principal has delegated a certain level of control over the value object to the Agent, expecting him to optimize its value and safeguard it in all respects. The latter assumes that the Agent respects the norms of good stewardship (general or specific, explicit or implicit). The Agent accounts for his performance with certain *statements*. The task of the auditing service (Auditor) is to give independent assurance that these statements are reliable and to check that the Agent (Auditee) has done everything he could do to protect the value object. Although these are two different things, the former relies on the latter: if the value object has been manipulated in unknown and hence unrecorded ways, the reliability of the statement is low, even if the Agent is sincere.

The most well-known case of auditing is where the value object is some capital from owners or shareholders, provided to a company, and the statement is an annual financial report. However, there are many more cases, also in the IS field, e.g. in a cloud environment, clients entrust their applications to a cloud provider, assuming that the cloud provider protects it against all kinds of risks (hacking, data leaking, etc.) [7,13]. The cloud provider makes claims in its protection policy or contract, and, in its invoice, about the resources it has used to run the application. The task of cloud auditing (cf. www.cloudaudit.org) is to check these statements. According to [6] *preventive* controls such as data encryption and all kinds of security measures are not sufficient. Equally important are "*detective* controls that promote transparency, governance and accountability of the service providers".

Other examples include tax and excise declarations, e-election systems and environmental reports. Having sketched the auditing situation, we are now in a position to give a definition of auditability. We take a service science approach by considering the object of the auditing not a process or an organization, but a service system in the sense of [14]: a collection of resources (including people and technology) connected to other service systems by means of value propositions.

Definition
A service system S using or producing a non-empty set of value objects V being of value to a stakeholder P and controlled by agent A is auditable in a context C iff
(a), there is normative framework N governing the usage of V (normativity);
(b) A makes a statement M to P about its responsible (i.e., in accordance with N) usage of V (accountability);
(c) S generates information I about the usage of V. I is independent from M and made available to P or its delegate (transparency);
(d) C ∪ I provides the grounds by means of which M can be validated (assurance).

Note that there is an *object domain* containing the value objects V and service system S, and an *information domain* containing information about V and the behavior of S. These two domains must be linked in such a way that the information I is reliable in what it states about the object domain. It does not need to be complete in an absolute sense (which is impossible), but it should be sufficient for the validation of statement M. In all but the most primitive cases, this implies that the information I is recorded on some tamper-free storage medium.

3 A framework for auditability

Having described the concept of auditability, we now proceed with the question of optimizing it. We first define what it means for management to be in control, then explore how auditability can be moved to a higher level. Particular attention is given to the IT infrastructure.

3.1 Being in control

Auditing aims to provide reasonable assurance that the information about the service system is reliable. However, this aim can be achieved in different ways. In most cases, the "agent" in the service system is in fact a group of agents, with management relationships between them. This management control is highly relevant. We model it as another agency relationship that overlaps but is not identical to the agency relationship with the owner of the resource or stakeholder. The most obvious difference is that from an owner perspective, the manager himself is an agent/auditee as well. Another important difference is that the auditor is "only" responsible for providing reasonable assurance (and it is up to the owner to take action), whereas the manager has profit responsibility and has to act himself.

Fig. 1. Basic management control cycle

The general management control cycle is depicted in Fig. 1. Note the overlap with the auditing situation. The manager plans action in the form of an operational policy (cf. *normative framework*). The policy is enforced in the operational process (cf. *service system*) where the agent manipulates value objects. On the basis of event traces and self-reports, aggregated management accounts are produced (cf. *statement*). These are evaluated by the manager ("check"), resulting in decisions ("act"). As far as this cycle is closed, the control can be called diagnostic. When the manager takes more information into account, in particular sensing the environment and internal dialogue, the control can be called interactive [12,15].

3.2 Moving auditability to a higher level

Using the management cycle as a reference model, we can distinguish at least four levels of auditability (Table 1). Each level is defined in terms of the audit focus within

this management cycle: which element is made transparent. Each level comes along with a different infrastructure and gives rise to a different audit type. The primary statement may also differ.

Moving to a higher level is assumed to be incremental: the "lower" levels remain transparent, and may still be used, but with the new level added, the audit *focus* will shift.

In certain areas, such as traditional customs, auditing is addressing transactional data only (level 1), as the level of auditability does not go beyond the operational process (events, transactions). This may be because there is no management process, i.e., the auditee is independent (really independent, like a private person, or considered independent, as a professional doctor in a hospital) or because the management process is not transparent, for some reason. The primary statement is a self-report, e.g. a customs declaration form.

	AUDIT FOCUS	INFRASTRUCTURE	AUDIT TYPE	PRIMARY STATEMENT
1	operational process	physical environment, possibly IT-based	transaction-based	self-report
2	accounts	(a) tracing infrastructure (b) accounting information system	system-based	self-report
3	operational policy	(a) policy (GRC) information system (b) enforcement infrastructure	risk-based	accounting information system
4	management process	Management Information System	governance-based	accounting information system

Table. 1 Main auditability levels

Transaction-based auditing is a labor-intensive process. If there is a management process, then there is usually an accounting information system. In this situation, the primary focus of the auditing can shift to the accounts (level 2). This is only possible if the data are reliable, which is achieved along two main lines: first, the design, existence and effectiveness of reliable tracing infrastructure, in terms of segregation of duties and persistent tamper-free recording; second, an administrative system infrastructure incorporating integrity constraints and analytical instruments such as spanning equations based on the REA duality axioms. Roughly speaking, the former is necessary to ensure the correctness and the latter the completeness of the accounts. The financial audit field has established regulations to determine these so-called audit risks (IFAC standard ISA 315). Note that a thorough system-based approach still includes data tests, but much less than in the transaction-based approach.

One disadvantage of the system-based approach is that the accounting information system typically only records the past. When shifting the focus to the operational policy (level 3), the control objective shifts from detective to preventive. This assumes that a business process specification ("service policy") is in place – described, managed and enforced – and made transparent for auditing. The auditing checks whether the operational business rules conform to the normative framework of the service system, that is, whether all controls are in place (design-time compliance).

To guarantee run-time compliance, it also checks the enforcement (both its design and actual performance), in which IT usually plays an important role. At this point, the role of the accounting information system can change: from a way of validating the audit statement (the self-report) to the primary audit statement itself. The auditor validates this statement by means of the policy audit.

We call this level risk-based as the aim of the policy is to prevent the undesirable to happen, so to reduce the risk and uncertainty. At this point, we have to extend our event concept: economic events are still at the core, but a cause analysis will also identify events that manipulate value objects indirectly. For instance, a weather alarm in the country of a supplier may have an impact on his ability to deliver. We call these events *risk events* as distinct from REA economic events.

A limitation of the risk-based approach as described here is that in complex, dynamic and interconnected environments it is very hard to implement rigid policies. Neither the policy nor the policy enforcement will be complete. As a panacea, the organization can rely on regulatory *compliance* only, as this is at least broadly accepted and has a rational basis. However, these regulations are often either too strict or not strict enough [11]. Still, it is quite tempting for companies to use just a "tick box approach", or to externalize responsibility or fall in the trap of a count-control-calculate escalation criticized by Powers [10, although this is not necessary: according to empirical research of Mikes [9], company culture plays a role here: the difference between "quantitative enthusiasm" versus "quantitative skepticism".

A next step is to shift the audit focus to the last element of the control cycle and make the management process transparent. It is the manager who is supposed to build the necessary internal controls into the operational policy and who monitors their implementation. If the manager is in control, by implication the validity of the accounts and the norm compliance of the agent performance are guaranteed. So the auditing checks "only" whether the manager is in control. This assumes the accounting information system and the policy management to be in place, but also the effective use of it. Here we get to the upper part of the control cycle: does the manager read the performance indicators (check), does he respond to it adequately (act), and is his response implemented in the operational policy (plan)? A difference must be made between corrective actions per case (incident management) and corrective or pro-active actions on the operational policy (change management). Note that on this level, the policy is no longer required to be complete. The main question is not whether things can go wrong or not (in a complex environment, they will sometimes), but whether the management responds adequately.

To check the manager actions in a transaction-based style is not feasible. So shifting to this level of auditability requires a *meta-control* cycle to be in place. If that is the case, we can apply the auditability framework recursively to the manager as agent. His actions are traced in a secure way, aggregated, cross-checked in a reliable information system and controlled by a well-specified management policy based on accepted governance standards. In principle, this recursive approach can be extended to the higher organizational levels, in particular the governance board, and even beyond the boundaries of the organization to external regulators. This development is already visible in some areas, such as the financial industry.

3.3 Business benefits

At each auditability level, the organization becomes more transparent. The motivation for moving to a higher level is increased audit efficiency and/or effectiveness. The efficiency gain has different reasons. One is that checks are made on a higher abstraction level and therefore are less labor-intensive. IT plays an important role in enabling this abstraction (see below). However, these efficiency gains are not always sufficient for motivating the costs and to convince the management.

Another benefit is economy of scope: effective use is made of instruments that are already adopted (or should be adopted) for business reasons by the management anyway. This is even more important when there are multiple independent auditings, for instance, by government agencies, regulators and supply chain partners. The more infrastructure and services they can share the better.

Without repeating all possible business benefits of management control (this is an area of its own), we want to mention a few that are closely related to auditability. Going from level 1 to level 2 is not only moving from events to accounts, but also from viewing the performance of the auditee in isolation to viewing it as part of a system, a cooperative network of actors, each with his own interests. This coherence is not immediately visible from the individual events only, so level 2 really provides more management insight. A limitation of level 2 is that is retroactive only. Going to level 3 urges the organization to become more explicit about its norms and more aware of the risk (again, things that are not directly observable). The advantage is that the efforts get more directed towards prevention, which is usually cheaper then repair and more effective as protection of the value objects in place. A possible threat is that increased security comes at the expense of business agility. Going to level 4 reinforces the responsibility of the manager in coping with a dynamic environment and optimizing business value. As such, this last shift also has an impact on organizational culture (how to evolve into a learning and adaptive organization on all levels).

4 Conclusion

Compliance is becoming a strategic concern for many companies and requires the controlled system to be auditable in the first place. Although the term “auditability” is used more and more, its conditions are seldom made explicit. In this paper, we have been able to define auditability on an abstract level and ground the concept in the REA business ontology. On the basis of this conceptualization, we have distinguished four levels of auditability. As far as we know, this is the first attempt to do so in a systematic way. Our work has also practical relevance. From our analysis we recommend companies to stay away from a narrow focus on compliance but address compliance within the wider goal of auditability.

Our research also raises new questions. It would be interesting to extend our framework into a maturity model and accompanying roadmap. We are currently contacting more companies in order to collect more examples, from different levels. Based on that information, the framework can be refined, evaluation questions can be developed for each level and the maturity model can be validated in practice.

5 References

[1] Aalst, W., van Hee, K., van der Werf, J.M., Kumar, A., Verdonk, M.: Conceptual model for on line auditing. Decision Support Systems 50, 636–647 (2011)
[2] El Kharbili, M., Stein, S, Markovic, I., Pulvermuller, E., Towards a Framework for Semantic Business Process Compliance Management. Proc. GRCIS'08 (2008)
[3] Hagerty, J. Kraus, B.: GRC in 2010: $29.8B in Spending Sparked by Risk, Visibility and Efficiency. Boston, MA (2009)
[4] Holmes, T., U. Zdun, F. Daniel and S. Dustdar: Monitoring and Analyzing Service-based Internet Systems through a Model-Aware Service Environment**.** Proc. CAiSE 2010, LNCS pp. 98-112, (2010)
[5] Jensen, M. C. and W. H. Mecklink : Theory of the Firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics 3*, 305-360 (1976)
[6] Ko , R.K.L., B.S. Lee, S. Pearson: Towards Achieving Accountability, Auditability and Trust in Cloud Computing. In: Abraham, A. et al (Eds.), Advances in Computing and Communications, LNCS, pp.432-444 (2011)
[7] Martens, B., Teuteberg, F.: Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model. Proc. AMCIS 2011, paper 228 (2011)
[8] Mautz, R.K., H.A. Sharaf: The philosophy of auditing. Sarasota, Fl, American Accounting Association (1961)
[9] Mikes, A.: From Counting Risk to Making Risk Count: Boundary-Work in Risk Management. Accounting, Organizations and Society 36, nos. 4-5 (June 2011): 226–245.
[10] Power, M.: Organized Uncertainty: Designing a World of Risk Management. Oxford: Oxford University Press (2007)
[11] Power, M.: The risk management of nothing. Accounting, Organizations and Society, 34 (6–7) (2009), pp. 849–855
[12] Simons, R.: Performance Measurement and Control Systems for Implementing Strategy. Prentice Hall (2000)
[13] Spies, M.: Rule-Enhanced Domain Models for Cloud Security Governance, Risk and Compliance Management. In: F. Olken et al (Eds), Rule - Based Modeling and Computing on the Semantic Web LNCS, pp.2-9 (2011)
[14] Spohrer, J., S. Vargo, N. Caswell, P. Maglio: The Service System is the Basic Abstraction of Service Science. Proc. 41st Annual HICSS (2008)
[15] Weigand, H, Johannesson, P., Andersson, B., Arachchige, J.J. and Bergholtz. M.: Management services - a framework for design. Proc. CAiSE 2011, LNCS pp. 582-596 (2011)
[16] Weigand, H., Bukhsh F.: Supporting Customs Controls by Means of Service-Oriented Auditing. Proc. IFIP 6.11 Conf. on e-Business, e-Services, and e-Society, Kaunas, (2011)
[17] Weigand, H., Elsas, Ph.: Model-based Auditing Using REA. Int. Journal of Accounting Information Systems (2012)
[18] Wiesche, M., Schermann, M., Krcmar, H.: Exploring the Contribution of Information Technology to Governance, Risk Management, and Compliance (GRC) Initiatives. Proc. ECIS 2011, AIS Electronic Library, paper 4 (2011)