Business Process as a Service: Chances for Remote Auditing

Rafael Accorsi
Department of Telematics
University of Freiburg, Germany
accorsi@iig.uni-freiburg.de

***Abstract*—The advent of cloud computing allows the provision of several commodities "as-a-service". For enterprise systems, a particularly interesting business model is the offer of configurable business processes for different consumers, which can then outsource their execution onto the cloud. Although such an outsourcing harbors a vast economic potential, both external and internal auditing pose a general challenge for their acceptance. This paper reviews the role of remote auditing as a means to address this issue and indicates research directions for automated tool support.**

***Keywords*-Business process as a service; Remote auditing**

I. Introduction

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned with minimal management effort or service provider interaction.

In particular, the following service models are traditionally provided [14]: infrastructure-as-a-service, platform-as-a-service, and software-as-a-service (SaaS). For enterprise system a special instance of the SaaS model appears to be relevant, namely the provision of business process as a service (BPaaS). SAP's Business ByDesing and IBM's CloudBurst are two examples of flexible platforms for the provision of BPaaS. With the popularization and wide adoption of cloud computing, we expect the provision of BPaaS to grow further, especially for small and medium enterprises that cannot afford fully-fledged enterprise solutions.

However, by outsourcing the execution of business processes, cloud consumers lose control over their data and executions [15]. In particular, auditability becomes an intricate issue both for internal and external auditors, as they do not have physical access to the processes and information system on top of which processes are running.

This can be addressed with *remote auditing* (RA). RA is the process by which auditors couple information and communication technology with data analytics to *remotely* assess and report on the accuracy of financial data and internal controls (traditional audit) and access the soundness of information system (IS audit) [34]. However, while being an interesting concept, it is neither clear what the preconditions must hold for such a RA, nor what tool support is currently available to remotely audit business processes.

This paper provides the following contributions:

- Defines the business process as a service paradigm and relates with to service oriented computing (Section II).
- Reviews the concept of RA and reports on the main properties to be considered: compliance and security for BPaaS (Section III).
- Elaborates on the prerequisites and tool support to carry out RA for BPaaS (Section IV).

Currently, effort is being put on identifying the economic value of RA to companies and auditors. Less effort can be observed on the explicit realization of this added-value through automation. The following is thus a first attempt to bring together economic science (auditing and assurance) and computer science (tool support for audits). In future, we expect a growth of security audit, mostly as a result of outsourcing through cloud computing. However, this will not only hold for BPaaS, but also for the other service models offered by clouds.

II. Business Process as a Service

The expression (business) "process as a service" (BPaaS) was coined by Wang et al. [37]. Meant thereby is the process level collaboration and outsourcing process steps. In the paper, the discussion and presentation focuses on one possible realization of this service model based upon service-oriented architecture (SOA) and correspondingly WS-BPEL to orchestrate the services. In this section, we generalize this view and present the main advantages of the BPaaS service model.

We define the BPaas cloud computing model is a special SaaS provision model in which enterprise cloud offerors provide methods for the modeling, utilization, customization, and (distributed) execution of business processes. According to [32], a *business process* is a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular customer or customers. The specification of business processes for automation, in languages such as BPEL and BPMN, is traditionally refered to as *workflow*, i.e. patterns of activity enabled by a systematic organization of resources, defined roles and information flows, into a work process that can be formalized and automated [24]. In the following, we employ these terms interchangeably.

In the BPaaS model, cloud consumers (or clients) can rely on and access pre-defined process descriptions, customize

978-0-7695-4459-5/11 $26.00 © 2011 IEEE
DOI 10.1109/COMPSACW.2011.73

these processes according to the current needs, and remotely execute the processes in the cloud. Pre-defined processes are patterns of basic activity, e.g. updating a customer record or processing a customer request. They can be put together, customized, and optimized, thereby leading to *multi-tenancy*, i.e. different instantiations and governance for each cloud client. Finally, the resultant processes can be executed in the cloud, provided the necessary data is made available. Clearly, a remote process can also happen as a steps carried out in the cloud which is combined with process steps carried out locally. Overall, one can speak of a *complete outsourcing* (the whole process is managed in the cloud) or a *partial outsourcing* (only parts the process are managed in the cloud).

Other than stated in [37], we firmly believe that BPaaS does not depend on a particular form of realization. Perhaps because of the similar nomenclature with regard to "service", all too often the provision of cloud computing models in general and BPaaS in particular are (misleadingly) equated with service-oriented computing (SOC) [38]. We notice a different emphasis in these two drives: SOC is tailored for the (enterprise) integration to exchange information among "systems of systems" by prescribing interfaces consistent with the enterprise architecture. On the other hand, cloud computing leverage the network availability to outsource IT functions across the entire stack (infrastructure, platform, and service) as a means to provide on-demand access to virtualized resources. Hence, while similar, cloud computing and SOC are different concepts that can be pursued independently or as current activities.

Business processes are paramount for the success of a company towards its concurrents in the market. Indeed, the particular design, e.g., of supply-chain and customer management processes are considered business secrets. Correspondingly, the wide-spread adoption of BPaaS demands that offerors provide a high assurance that the business process specifications remain secret on the one hand (process sensitivity) and that their execution is not visible to the offeror and other clients sharing the cloud (isolation or compartmentalization) [14], [33]. Together with the legal duties to demonstrate compliance with accounting laws [34] and regulatory frameworks [27], these requirements are usually subject of auditing. Due to the outsourced and dynamic nature of cloud computing, BPaaS auditing is in theory intensive than usual enterprise systems. The next section addresses this issue.

III. Remote Audit: Process & Properties

This section presents the remote auditing (RA) process and relates it to the characteristics of the BPaaS presented in the Section II. Teeter et al. define remote auditing as the process by which auditors couple informtion and communication technology with data analytics to access and report on the accuracy of financial data and internal control, independent of the physical location of the auditor [34]. RA thus eliminates the location constraint of an audit and is inherently connected with some form of networking to connect the entity to be audited (so-called *auditee*) and the auditor.

By outsourcing process with the BPaaS service model, both internal and external auditors do not have access to the physical systems in the cloud. In particular, external auditors will most likely have to access both the auditee's system and the auditee's compartment in the cloud in order to conduct the examination. In this case, the auditors may employ RA to examine both the auditee and the cloud provider. This clearly motivates the use development of RA as a means to make audits possible and to provide high assurance for clouds, thereby addressing their inherent loss of control [15].

In principle, RA can be used for any audit type: financial statement, compliance, and operational audits. In the light of BPaaS, compliance and operational audits are the primarily applicable kinds of examination. The purpose of a *compliance* audit is to determine whether the auditee acts (or acted) in accordance with the procedures and regulations established by an authority, e.g. management, contracts, and regulatory bodies [13]. An *operational* audit involves a systematic examination and evaluation of an auditee's operations which is conducted to test the efficiency and/or effectiveness of the auditee. A particular type of operational audit is the *information system audit* (IS audit), which focuses on the processes and data flows in the corresponding IS.[1]

A. Business Process Compliance

Given the strong demand for compliance [27], two questions emerge when conduction an audit. First, which rules do business processes have to adhere to? Second, how can the rule adherence be checked? The remainder of this section presents a survey of compliance regulations to answer the first question. In Section IV-B we present a tool support to assist this examination.

In [4], we thorougly examine the main regulatory frameworks to understand the nature of compliance rules. Specifically, we focus on the OECD guidelines, EC Directive 95/46/EC, the Gramm-Leach-Bliley Act (GLB), Health Insurance Portability and Accountability Act (HIPAA), the PATRIOT Act, and the Sarbanes-Oxley Act (SOX). The business process related sections of the above compliance regulations can be organized in a few basic classes of rules. Table I shows an excerpt of the results for a few regulatory frameworks.

The rule categories in the second left column were obtained by sifting through the compliance sources in the

[1] Note the distincion between information technology (IT) und IS auditing: IT audit examines the infrastructure with regard to, e.g., malware and dependability mechanisms; IS audit examine the automated processes or process steps and the data flows that are carried out using IT.

Table I
EXCERPT OF A CLASSIFICATION OF COMPLIANCE RULES.

		HIPAA	95/45/EC	OECD	GLB
↔	Notify usage	√	√	√	√
↔	Obtain consent	√	√	√	
↔	Check 3rd parties	√	√		√
↔	Update records	√		√	
↔	Delete after use	√	√		
⋎	Treat special data	√	√		
⋎	Purpose binding	√	√		
⧈	Data sanitization	√			
⧈	Limit data release	√	√		

top row and listing all rules that directly pertain to either the control flow (e.g. some activity has to happen before another) or the data flow (e.g. treatment of documents and their content) of business processes. After consolidating those rules that only used slightly different wording to describe the same requirement, the nine categories remained.

The resulting three rule classes are symbolized by the icons in the very left column. A double headed arrow ↔ for categories that require certain activities to (not) be performed before or after other activities. A double headed branching arrow ⋎ for categories describing the flow of data. Finally, a double square label ⧈ stands for categories directly relating to data elements.

B. Business Process Security

Considering the security of business processes, the adherence to the following properties are relevant when auditing processes [12]:

- *Authorization*: enforce access control to ensure that only authorized subjects/roles are allowed to execute task within a business process (execution).
- *Separation of duty* (SoD): assurance of additional constraints associated with the business process to limit the ability of subjects to reduce fraud risk. SoD can take different forms: *intra*-instance are specified on a business process and therefore apply to a single instance; *inter*-instance are specified in the business process executions (instead of specifications) and therefore refer to several instances.
- *Binding of duties*: Guanranteeing that subjects perform the assigned tasks during the process execution.
- *Delegation*: Controling the extension of privileges from one subject to another. Accordingly, the secure *revocation* of privileges must be ensured.
- *Conflict of interest*: Preventing the flow of sensitive information among competing organizations (i.e. cloud clients) participating in the business process or sharing the services of the same cloud offeror.
- *Four eye principle*: Control to ensure that some activities of the business processes are cleared by two different subjects, mostly playing a different role.

IV. PREREQUISITES AND CHANCES FOR TOOL SUPPORT FOR REMOTE AUDIT IN BPAAS

This section presents a few general prerequisites to the realization of reliable RA audits in clouds (and consequently in auditees). Building upon that and focusing on the BPaaS, we report on computer assisted auditing techniques (CAAT) to audit process with regard to compliance and security.

A. Technical Prerequisites for Remote Audit

RA leverages on information communication technology to carry out examination and reporting. Hence, the most essential prerequisite is the availability of a secure, reliable internet connection between the (sets of) auditors and the auditee. Furthermore, the following is necessary:

Trusted computing base: For RA in the BPaaS, it is essential that auditors obtain evidence that the platform is reliable. This includes one the one hand (mutual) *authentication* – is the auditor communicating with the right cloud respectively, is the cloud communicating with the right auditor. On the other hand, the auditor must obtain reliable evidence that the software stack used to execute and manage the business process is that settled on in the service-level agreement. These guarantees are achieved with *remote attestation* using dedicated trusted computing processors [22], [31].

While attestation techniques dedicated to cloud computing are not yet available [10], some recent advances have been made [21], [29]. A reliable trusted computing base is a cornerstone for the remaining prerequisites.

Probably authentic logs: The execution of the business processes must be stored in a *tamper resistant* and *tamper evident* way. This is primarily a requirement on the cloud offeror, which must log the process execution without interruption (complete logs). Tamper resistance ensures that fraudsters (either the cloud provider, the company, or external spies) cannot compromise the log. Complementary, if such attempts happen, they must become evident to an auditor before testing (examining) the data. This is called tamper evidence.

Tamper resistance is an architectural measure which includes strict access control rules and isolation requirements. Tamper evidence is closely related to secure logging mechanisms to ensure that entries are recorded in an integrity-preserving way. (See [2], [3], [20] for a survey of state of the art secure logging protocols). This is usually achieved with cryptographic primitives that logically connect one log entry with previous and next ones. The downside of cryptography and encryption is that it slows down the examination, requiring the selective disclosure of entries according to the audit goal. While efficient approaches to do so exist [26], this step (together with the necessary key management steps) still introduces latencies in the audit process.

Business provenance: This is a technology developed to increase the traceability of end-to-end business operation in a flexible and cost effective manner [16]. Specifically, business provenance captures and manages the lineage of business artifacts to allow for the discovery functional, organizational, data, and resource aspects of business. Hence, business provenance information is not only relevant for RA, but for audits in general.

For the BPaaS service model in particular, mechanisms must be in place to record, e.g., the "history" of a business process – i.e. the different instances of an original schema – and the interaction of processes and subjects when triggering a process. Since the process schemas and execution parameters/engine provided by the cloud offeror may change as well, their provenance must also be captured. Furhermore, since other subsystems and even cloud providers may be involved in the execution of the processes, it is important to track down their way across the system.

The examination of provenance data, in context of an audit or not, provides an insight into the causal chain of a particular system state, helping to understand how a particular state has been reached. In doing so, business provenance information enrichs the log data, correlating sets of events and states. Ideally, business provenance should thus answer the question "why did this happen?".

Currently, thorough tool support for provenance is coupled with solutions but special techniques for cloud computing are not available [25].

B. CAAT Support

The enormous potential of computer assisted audit techniques (CAAT) to improve the quality of examination and testing as the first personal computers appeared [19]. Since then and with the increasing digitalization of business activities, the application of CAAT in the audit process have been gaining on momentum. (This in spite of the reluctance on the part of auditors [17].)

Generally, CAAT for IS audit can be classified into four broad categories [30]: data analysis software; network security evaluation software; OS and DBMS security evaluation; and software testing tools. For the BPaaS service model, data analysis software, as well as software testing tools are primarily relevant.

Data analysis software: Here we see the analysis of the (authentic) execution log files to examine compliance and security properties as the main application for data analysis software. For compliance, a few approaches exist to correlate and analyze log entries [1], [9] and to detect deviations from a process model using process mining [35]. For testing security goals, some approaches employ tree structures to accelerate audit [5], others reconstruct the data flows happening during the execution to determine security violations [6], [7].

In general, the reconstruction of processes and data flows appears is a powerful method to obtain expressive models for the examination. They also help the auditor to understand the structure of processes and flows in order to determine violations. However, reconstruction algorithms only present the log data in a different manner, so that an examination against the policies is still required. Hence, room for improvement exists with regard to declarative audit policy specifications (so-called extensional policies [28]), thereby making automated analysis possible. Furthermore, reconstruction should in future take into account multi-tenancy, which is currently not the case. A particular challenge regards the case in which partial outsourcing happens. Here, techniques to consolidate the logs of the cloud client and offeror are needed, yet not available.

Software testing tools: Software testing tools analyze the business process specification and business process management system to detect compliance and security violations. The analysis of business process specifications for several compliance aspects [18], [23], [36] and security properties [8], [11] a rich research field. Still, methods to examine the underlying management system are not available, in particular the efficiency of embedded controls. Hence, RA can today only rely on tool support for business process specifications.

V. Summary

This paper argues for the need of RA as a basis means to provide for auditable cloud-based business process. Besides outlining the BPaaS service model, the paper describes the RA paradigm and the main examination modes to be expected, namely for compliance and security requirements. Finally, we summarize the main prerequisites for the provision of RA for clouds and report on some tool support and research directions to be pursued. Overall, we firmly believe that the deployment of cloud computing in general and BPaaS in particular will foster the development of novel CAAT for RA. In particular, the demand of RA will increase as small and medium enterprises start using the cloud and its BPaaS capabilities.

References

[1] R. Accorsi, "Automated privacy audits to complement the notion of control for identity management," in *Policies and Research in Identity Management*, ser. IFIP Conference Proceedings, E. de Leeuw, S. Fischer-Hübner, J. Tseng, and J. Borking, Eds. Springer, 2008, vol. 261, pp. 39–48.

[2] ——, "Safe-keeping digital evidence with secure logging protocols: State of the art and challenges," in *Proceedings the IEEE Conference on Incident Management and Forensics*, O. Goebel, R. Ehlert, S. Frings, D. Günther, H. Morgenstern, and D. Schadt, Eds. IEEE Computer Society, 2009, pp. 94–110.

[3] ——, “BBox: A distributed secure log architecture.” in *To appear in European Workshop on Public Key Services, Applications and Infrastructures*, ser. Lecture Notes in Computer Science, J. Camenish and C. Lambrinoudakis, Eds., no. 6711. Springer, 2011, pp. 109–124.

[4] R. Accorsi, L. Lowis, and Y. Sato, “Automated certification for compliant cloud-based business processes,” *To appear in Wirtschaftsinformatik*, 2011.

[5] R. Accorsi and T. Stocker, “Automated privacy audits based on pruning of log data,” in *Proceedings of the EDOC International Workshop on Security and Privacy in Enterprise Computing*. IEEE, 2008.

[6] R. Accorsi and C. Wonnemann, “Detective information flow analysis for business processes,” in *Business Processes, Services Computing and Intelligent Service Management*, ser. Lecture Notes in Informatics, W. Abramowicz, L. Macaszek, R. Kowalczyk, and A. Speck, Eds. Springer, 2009, vol. 147, pp. 223–224.

[7] ——, “Auditing workflow executions against dataflow policies,” in *Proceedings of the Business Information Systems*, ser. Lecture Notes in Business Information Processing, W. Abramowicz and R. Tolksdorf, Eds., vol. 47. Springer, 2010, pp. 207–217.

[8] ——, “Strong non-leak guarantees for workflow models,” in *ACM Symposium on Applied Computing*. ACM, 2011, pp. 308–314.

[9] R. Agrawal, C. Johnson, J. Kiernan, and F. Leymann, “Taming compliance with sarbanes-oxley internal controls using database technology,” in *Proceedings of the 22nd International Conference on Data Engineering*. IEEE Computer Society Press, 2006, pp. 92–101.

[10] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A Berkeley view of cloud computing,” EECS Department, University of California, Berkeley, Tech. Rep. EECS-2009-28, 2009.

[11] V. Atluri, S. A. Chun, and P. Mazzoleni, “A Chinese Wall security model for decentralized workflow systems,” in *ACM Conference on Computer and Communications Security*. ACM, 2001, pp. 48–57.

[12] V. Atluri and J. Warner, “Security for workflow systems,” in *Handbook of Database Security*, M. Gertz and S. Jajodia, Eds. Springer, 2008, pp. 213–230.

[13] J. Bace and C. Rozwell, “Understanding the components of compliance,” Gartner Research Paper, July 2006.

[14] R. Chandramouli and P. Mell, “State of security readiness,” *ACM Crossroads*, vol. 16, no. 3, pp. 23–25, 2010.

[15] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, “Controlling data in the cloud: Outsourcing computation without outsourcing control,” in *Proceedings of the ACM Workshop on Cloud Computing Security*. ACM, 2009, pp. 85–90.

[16] F. Curbera, Y. N. Doganata, A. Martens, N. Mukhi, and A. Slominski, “Business provenance - A technology to increase traceability of end-to-end operations,” in *On the Move to Meaningful Internet Systems Conferences*, ser. Lecture Notes in Computer Science, R. Meersman and Z. Tari, Eds., vol. 5331. Springer, 2008, pp. 100–119.

[17] R. Debreceny, S.-L. Lee, W. Neo, and J. S. To, “Employing generalized audit software in the financial services sector,” *Managerial Auditing Journal*, vol. 20, no. 6, pp. 605–618, 2005.

[18] A. Ghose and G. Koliadis, “Auditing business process compliance,” in *Proceedings of the Conference on Service-Oriented Computing*, ser. Lecture Notes in Computer Science, B. J. Krämer, K.-J. Lin, and P. Narasimhan, Eds., vol. 4749. Springer, 2007, pp. 169–180.

[19] B. Goossens and N. Schouten, “Using the computer for audit,” *Information & Management*, vol. 4, pp. 3–10, 1981.

[20] M. Gunestas, D. Wijesekera, and A. Singhal, “Forensic web services,” in *IFIP Conference on Digital Forensics*, ser. IFIP, I. Ray and S. Shenoi, Eds., vol. 285. Springer, 2008, pp. 163–176.

[21] A. Haeberlen, “A case for the accountable cloud,” *Operating Systems Review*, vol. 44, no. 2, pp. 52–57, 2010.

[22] R. Kelly, “A survey of trusted computing specifications and related technologies,” 2003, SANS Publication Series.

[23] D. Knuplesch, L. T. Ly, S. Rinderle-Ma, H. Pfeifer, and P. Dadam, “On enabling data-aware compliance checking of business process models,” in *Conference on Conceptual Modeling*, ser. Lecture Notes in Computer Science, J. Parsons, M. Saeki, P. Shoval, C. C. Woo, and Y. Wand, Eds., vol. 6412. Springer, 2010, pp. 332–346.

[24] F. Leymann and D. Roller, *Production Workflow: Concepts and Techniques*. Prentice Hall, 1999.

[25] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure provenance: The essential of bread and butter of data forensics in cloud computing,” in *ACM Symposium on Information, Computer and Communications Security*, D. Feng, D. A. Basin, and P. Liu, Eds. ACM, 2010, pp. 282–292.

[26] Y. Ohtaki, M. Kamada, and K. Kurosawa, “A scheme for partial disclosure of transaction log,” *IEICE Transactions Fundamentals*, vol. 88-A, no. 1, pp. 222–229, 2005.

[27] S. Rinderle-Ma, L. T. Ly, and P. Dadam, “Business process compliance,” *EMISA Forum*, vol. 28, no. 2, pp. 24–29, 2008.

[28] B. Roscoe, “Intensional specifications of security protocols,” in *Proceedings of the 9th IEEE Computer Security Foundations Workshop*. IEEE Computer Society Press, 1996, pp. 28–38.

[29] N. Santos, K. Gummadi, and R. Rodrigues, “Towards trusted cloud computing,” in *Conference on Hot topics in Cloud Computing*. USENIX Association, 2009, pp. 3–3.

[30] A. Sayana, “Using CAATs to support is audit,” *Information Systems Control Journal*, vol. 1, 2003.

[31] B. Schneier and J. Kelsey, “Remote auditing of software outputs using a trusted coprocessor,” *Future Generation Computer Systems*, vol. 13, no. 1, pp. 9–18, July 1997.

[32] H. Smith and P. Fingar, *Business Process Management*. MK Press, 2003.

[33] H. Tabaki, J. Joshi, and G.-J. Ahn, “Security and privacy challenges in cloud computing environments,” *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24–31, Nov.-Dec. 2010.

[34] R. Teeter and M. A. an Miklos Vasarhelyi, “Remote auditing: A research framework,” *Journal of Emerging Technology in Accounting*, to appear.

[35] W. van der Aalst, K. van Hee, J. M. van der Werf, and M. Verdonk, “Auditing 2.0: Using process mining to support tomorrow’s auditor,” *IEEE Computer*, vol. 43, no. 3, pp. 90–93, 2010.

[36] W. M. P. van der Aalst and A. H. M. ter Hofstede, “Verification of workflow task structures: A petri-net-baset approach,” *Information Systems*, vol. 25, no. 1, pp. 43–69, 2000.

[37] M. Wang, K. Y. Bandara, and C. Pahl, “Process as a service,” in *IEEE International Conference on Services Computing*. IEEE Computer Society, 2010, pp. 578–585.

[38] Y. Wei and M. B. Blake, “Service-oriented computing and cloud computing: Challenges and opportunities,” *IEEE Internet Computing*, vol. 14, pp. 72–75, 2010.