Compliance Requirements for Business-process driven SOAs

Michael P. Papazoglou

INFOLAB, Dept. of Information Systems and Mgt., Tilburg University, The Netherlands, e-mail: mikep@uvt.nl

Abstract: Business processes form the foundation for all organizations, and as such, are impacted by industry regulations. Without explicit business process definitions, flexible rules frameworks, and audit trails that provide for non-repudiation, organizations face litigation risks. This requires organizations to review their business processes and ensure that they meet the compliance standards set forth in legislation. In this paper we discuss compliance-aware implications for Service Oriented Architectures and present open research problems.

1. Introduction

TCompliance regulations, such as HIPAA, Basel II, Sarbanes-Oxley (SOX) and others require all organizations to review their business processes and ensure that they meet the compliance standards set forth in the legislation. This includes, but is not limited to, data acquisition and archival, document management, data security, financial accounting practices, shareholder reporting functions and to know when unusual activities occur. In a broader perspective compliance can pertain to any explicitly stated rule or regulation that prescribes any aspect of an internal or crossorganizational business process; including for example public policies, customer preferences, partner agreements and jurisdictional provisions.

Currently compliance to such rules and regulations is typically achieved on a percase basis. Often compliance solutions are hand crafted for particular compliance problems. Although such ad-hoc solutions achieve their objective, from a management perspective they have several undesirable characteristics. They are:

- hard to maintain as they do not follow a well established architectural pattern;
- hard to evolve as the solutions usually involve hard coding requirements across multiple systems with ill defined dependencies among components;
- hard to reuse as they are custom made to target specific compliance problems;
- hard to understand because a compliance solution often addresses several compliance requirements in a tangled manner;
- hard to formally verify that they guarantee overall compliance.

Please use the following format when citing this chapter:

Papazoglou, M.P., 2008, in IFIP International Federation for Information Processing, Volume 280; *E-Government; ICT Professionalism and Competences; Service Science*; Antonino Mazzeo, Roberto Bellini, Gianmario Motta; (Boston: Springer), pp. 183–194.

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 risks and even criminal penalties. Where business processes stretch across many cooperating and coordinated systems, possibly crossing organizational boundaries, technologies like XML and Web services are making system-to-system interactions commonplace and Service Oriented Architectures (SOAs) serve as a logical integration framework for connecting loosely coupled software modules into on-demand business processes.

2. Business-process driven SOAs

Service orientation utilizes services as constructs to support the rapid, low-cost and easy composition of distributed applications. Key to this concept is the Service-Oriented Architecture (SOA), which is a logical way of designing a software system to provide services to either end-user applications or to other services distributed over a network, via published and discoverable interfaces. Business processes form the foundation for SOAs and require that multiple steps occur between physically independent yet logically dependent software services. Underlying the need for flexibility in SOA is the ability to dynamically grow application portfolios quickly by rapidly assembling new services to address business needs.

To effectively align technical initiatives with the strategic goals at the business level, SOA is combined with Business Process Management technologies [1]. BPM is a natural complement to SOA, and a mechanism through which an organization can apply SOA to high-value business challenges. Layering BPM on top of a solid SOA allows actions within business processes to be exposed via automated services. With BPM orchestration, the exposure of key business events, processes and information to users at the appropriate times and in the appropriate contexts adds tremendous business value that might not otherwise be achieved with a conventional SOA.

When combining SOA with BPM technologies, service composition is typically provided by a process engine (or workflow engine), which invokes the SOA services to realize individual activities in the process. The main goal of such business process-driven SOAs is to increase the productivity, efficiency, and flexibility of an organization via (business) process management. Business process-driven SOAs help deliver control over business processes, fostering standardization across a company or an end-to-end process chain and compliance with regulations, policies, and best practices.

3. Compliance and Business-process driven SOAs

An important characteristic of SOAs is that they are impacted heavily by industry and sectorial regulations. Without explicit business process definitions, flexible rules frameworks, and audit trails that provide for non-repudiation, organizations face litigation risks.

Compliance regulations, such as HIPAA, Basel II, Sarbanes-Oxley (SOX) and others require all organizations to review their business processes and ensure that they meet the compliance standards set forth in the legislation. This can include, but is not limited to, data acquisition and archival, document management, data security, financial accounting practices, shareholder reporting functions. It also requires to know when unusual activities occur. In all cases, such new control and disclosure requirements create auditing demands for SOAs.

SOAs should play a crucial role in corporate governance, allowing management to ascertain that internal control measures that govern their key business processes can be checked, tested, and potentially certified with their underlying Web services.

Internal control constitutes a fundamental cornerstone in auditing, which is used to assure business process compliance, delivering objective and independent guarantees regarding virtually all accounting aspects of service-enabled business processes, including risk management, financial checks and governance processes [2].

A typical financial reporting control might mitigate the risk of misstating revenue due to inadequate physical or electronic security over sales documents and electronic files. This helps implement a compliance regulation act, such SOX section 404, which mandates that well-defined and documented processes and controls be in place for all aspects of company operations that affect financial information and reports. To achieve this functionality requires: (i) controlling and auditing who accesses financial information, (ii) controlling and auditing what financial information is accessed, and (iii) ensuring financial information is not compromised during transmission. Due to the inherent complexity present in compliance regulations, such as SOX, most companies cannot address these requirements without a strategy for automating the integration of the diverse business processes and their accompanying internal control systems throughout the enterprise.

4. Research Directions for Business-process driven SOAs

Novel service technologies should play a crucial role in allowing various types of users (including management) to ascertain that internal control measures that govern their key business processes can be checked, tested, and potentially

certified with their underlying business processes. All of this requires continuously adjusting and aligning services within end-to-end business processes that span organizations to cater for regulatory needs. Such changes should not be disruptive by requiring radical modifications in the very fabric of services or the way that business in conducted. This poses enormous methodological and technological challenges as the complexity and scale of service-based applications will expand by orders of magnitude due to the increasing need for flexibility and dynamicity posed by distributed service policies and regulatory compliance.

The challenges of compliant business processes constitute a vibrant area of service research, which has so far received only limited attention and has never been addressed to its entirety. For a holistic approach to compliant business process management (one that covers the entire compliance life-cycle from design time checking to run-time monitoring and adaptation of services) we have identified the following pressing research challenges (themes) which require real innovation:

1. Advanced mechanisms for auditing SOAs.
2. A sound methodology and an associated technology support framework to manage compliance-centric business processes.
3. A more ”human-centric” approach to compliance-driven software development that allows stakeholders to express their requirements in terms of typical compliance concerns.
4. A framework that supports the execution of high-level requests that are associated with compliance expressions and permits re-use and customization of compliant process fragments.
5. A formally grounded behavioral model for service compositions and end-to-end business processes to verify the compliance properties of composed services.
6. Monitoring facilities for tracking and validating compliance concerns that can be verified at run-time.

4.1 Auditing Business-process driven SOAs

To provide the ability to establish control and documentation, reduce risk and error potential, in cases where service-enabled processes impact financial reporting (e.g., in end-to-end sales cycles, payment cycles or production cycles), SOAs should be continuously audited. SOA auditing implies auditing business process and relies on an auditing strategy to evaluate the effectiveness of (internal) accounting control systems, which are needed to ensure that business processes execute according to predefined regulatory policies. By checking accounting control systems, risks can be mitigated while safeguarding service-driven processes and increasing their reliability.

Auditors rely on internal control systems as they provide audit evidence that helps reduce substantive testing. In addition, and perhaps more importantly, auditing the internal control systems of processes within or between organizations is a required practice. An auditing strategy should focus on those fragments of a business process that are exposed to the risk of control weaknesses, while fewer efforts need to be spent on those process fragments (and services on which they rely) with strong controls. These items become candidates for immediate evaluation and, where necessary, remediation. For example, handling salaries might be deemed a low-risk item since they are tightly controlled by a small group of people. Revenue recognition, on the other hand, might be deemed high risk because of loosely defined recognition procedures. This strategy becomes particularly significant in large, business-critical SOA-applications. According to the standard control definition given by ISA 315 [3], control activities performed on business processes (and therefore part of any SOA-based solution) may fall under the following five classes:

1. Performance reviews: reviews and analyses of actual performance versus budgets, forecasts, and prior period performance; relating different sets of data (operating or financial) to one another, together with analyses of the relationships and investigative and corrective actions; comparing internal data with external sources of information; and review of functional or activity performance.
2. Information processing control procedures: encompass application controls, which apply to the processing of individual business processes. These controls help ensure that all transactions occurred are authorized, and are completely and accurately logged and processed.
3. Physical controls: encompass the network-level security of service end-points, including adequate safeguards such as secured access/control to services; measures against data availability threats (e.g., XML attacks), and data integrity.
4. Segregation of duties: intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of the persons duties.
5. Authorization: accounting controls need to check procedures of reviewing and approving specific operations or transactions, e.g., approving the invocation of purchase orders, or change orders.

To address the above business process control activities, a service auditing methodology should accommodate the following auditing SOA tenets that are derived from intersecting core SOA with basic auditing principles [4], [3]: independent auditing by possibly using an independent auditor (human or automated); policing the SOA behavior by monitoring events or information produced by the services/processes, monitoring instances of business processes, viewing process instance statistics, and so on; real-time reporting by disclosing in real-time material events such as significant write-downs or bad debt recognition;

logging execution trails; and performing continuous auditing of business processes.

4.2 Dealing with the Effects of Business Process Changes

Changes that characterize business processes may have deep effects [5] and require that a business process be redefined and realigned within an entire process supplychain (including business partners, suppliers and customers). This may eventually lead to modification and alignment of business processes and calls for change oriented methodologies to provide a sound foundation for deep service changes in an orderly fashion that allow services to be appropriately (re)-configured, aligned and controlled as changes occur [5]. A business process change-cycle may be subdivided in different phases as described in the following.

The initial phase in a business process change-cycle focuses on identifying the need for change and scoping its extent. One of the major elements of this phase is understanding the causes of the need for change and their potential implications. For instance, compliance to regulations is major force for change. Regulatory requirements such as HIPAA and Sarbanes-Oxley provide strict guidelines that ensure companies are in control of internal, private, public, and confidential information, and auditing standards such as SAS 70 serve as a baseline for regulatory compliance by verifying that third-party providers meet those needs. All of this may lead to the transformation of services within a business process value chain. Here, the affected services-in-scope need to be identified. These assist in understanding the nature of services-in-scope and related services and provide a baseline for comparative purposes and determination of expected productivity, cost and service level improvements.

The second phase, called service change analysis, focuses on the actual analysis, redesign or improvement of the existing services. The ultimate objective of service change analysis is to provide an in-depth understanding of the functionality, scope, reuse, and granularity of services that are identified for change. To achieve its objective, the analysis phase encourages a more radical view of process (re)-design and supports the re-engineering of services. Its main objective is the reuse (or repurposing) of existing service functionality in to meet the demands of change. The problem lies in determining the difference between existing and future service functionality.

As service changes may spill over to other services in a supply-chain, one of the determining factors in service change analysis is being able to recognize the scope of changes and functionality that is essentially self-sufficient for the purposes of a service-in-scope (service under change). When dealing with deep service changes, problems of overlapping or conflicting functionality several types of problems need to be addressed [6], [5]:

1. Service flow problems: Typical problems include problems with the logical completeness of a service upgrade, problems with sequencing and duplication of activities, decision-making problems and lack of service measures.

2. Service control problems: Service controls define or constrain how a service is performed. These include problems where a service-in-scope ignores organizational policies or specific business rules and problems where external services require information that a service-in-scope cannot provide.

3. Conflicting services functionality (including bottlenecks / constraints in the service value stream): The functionality of a service-in-scope may conflict with functionality in related services. Conflicts also include problems where a service-in-scope is not aligned to business strategy, where a service may pursue a strategy that is in conflict with is incompatible with the value chain of which it is a part, and cases where the introduction of a new policy or regulation would make it impossible for the service-in-scope to function.

During the service change analysis standard continuous process improvement practices such as Six Sigma DMAIC practices or Lean Kaizen [7] should be employed. These determine the services changes and define the new services and standards of performance to measure, analyze, control and systematically improve processes by eliminating potential defects.

During the third and final phase, all of the new services are aligned, integrated, simulated and tested and then, when ready, the new services are put into production and managed. To achieve this a services integration model [1] is created to facilitate the implementation of the service integration strategy. This strategy includes such subjects as service design models, policies, SOA governance options, and, organizational and industry best practices and conventions. All these need to be taken into account when designing integrated end-to-end services that span organizational boundaries.

4.3 High-level Languages for Compliance-based Applications

Research is required in high-level declarative concepts for the specification of services languages and service-based applications that allow lay and experienced users and other stakeholders to express their views and requests in terms of what needs to be achieved rather than on how to achieve it. One direction which could be followed is expressing the requests of the stakeholders at the requirement or goal level, where a goal expresses the problem space with the core of the business process captured through high-level goals and a set of plans attached to a given goal, which represent a collection of different strategies and operating tactics. Stakeholders must be able to declare their high-level requirements in a natural and intuitive manner. For instance, a user may be able to specify that all financial business processes should comply to SOX section-409 by reporting in real-time all events that could affect financial results.

Preliminary research work on developing a service request language for XML based Web services in electronic marketplaces has been reported in [8]. This experimental service request language contains a set of appropriate constructs for expressing requests and constraints over requests as well as scheduling operators. User interaction can be perceived as a series of plans that potentially satisfy a request. This approach can be extended and combined with traditional business-process modeling and constraint-specific request language constructs to create executable business process specifications out of user formulated requests, such as compliance requirements.

Preferences and QoS are constraints could potentially be included in a user request. Such requirements must also be able to describe annotations for processes or process elements containing descriptions of behavioral, QoS or SLA features, regulations and policies. Previous work in this area has been reported in [9] where the authors use QoWL an XML-based language that comprises a subset of Business Execution Process Language (BPEL) and a set of QoS extensions for specification of QoS requirements. Constraints and preferences were studied in the area of CSP (Constraint Solving Problem) in [10] where temporal reasoning mechanisms for preferences are provided.

4.4 Compliance-aware Service Composition and Reuse Patterns

Business processes and the service compositions realizing those processes can be created faster and at lower cost if compliance-aware business process-fragments are reused. This approach requires the separation and unique identification of reusable content and its encapsulation in business process fragments (i.e. building blocks such as service patterns or templates) to rapidly tailor service compositions as users or individual application needs demand. Service patterns are a set of repeatable and parameterisable service compositions (and business sub-processes) based on best practices facilitating application and systems delivery and development. The reusable customized and/or differentiated service patterns can be offered by service providers to their customers. This can help guide users in quickly assembling and deploying optimized engagement models and problem solutions. For example, subprocess templates can be defined during modeling time of service compositions to enable faster development of compliant business processes. In addition, such templates can be continually extended with concrete parameter values to incorporate additional requirements (e.g., compliance specialization) and can be stored again as reusable units of functionality.

The ability to discover and compose templates and the ability to parameterize them in order to maintain compliance of the service composition (e.g. a BPEL process) will provide solutions for improving reusability of service compositions, which is clearly a need not addressed by the existing SOA technology landscape.

Some recent research activities address the issue of service composition reuse and specialization as described above. For example, [11] provides a higher level of abstraction for higher reuse through high-level patterns. The approach lets developers write patterns in terms of high-level functionalities. [12] introduces the concept of abstract composite Web service that can be specialized to particular concrete compositions and can be reused in the construction of larger or extended compositions, while [13] proposes a technique that provides users with a context-aware service selection by recommending combinations of services that are most appropriate in a given context. These approaches lack the support for compliance assurance and do not enable adequately the reusability of service composition artifacts that comply to business requirements.

4.5 Compliance-aware Behavior Specification and Checking

Techniques to automatically check the compliance of process models against compliance rules are particularly important for compliance-aware business processes. In addition to business process models, business protocols - which specify the external messaging behavior of services (viz. the rules that govern the service interaction between service providers and clients) - can be also be affected due to changes in policies and regulations and thus require compliance checking.

For compiance-aware business processes we need to ensure that a non-functional aspects and compliance may also be specified by the way of abstract protocols such as trust negotiation protocols, which can then be implemented by business compliant protocols. Dynamic service composition could then ensure that these non-functional aspects are correctly dealt with avoiding behavior anomalies or unexpected uses.

Research work which is interesting for such activities can be found in [14] which presents a method to improve the reliability and minimize the risk of failure of business processes from a compliance perspective. The proposed method allows separate modeling of both process models and compliance concerns. Business process models expressed in BPEL are transformed into pi-calculus and then into finite state machines and compliance rules are translated into linear temporal logic. In this way, process models can be verified against these compliance rules by means of model checking technology.

In the area of business protocols [15] points out the necessity of services including specification of their external behavior such as timed Web service protocols. Such a specification can be used to decide whether a service can be used in some dynamic service composition as part of a business process. Moreover, such a specification can be extended with non-functional requirements, for example by annotating business protocols with privacy policies [16].

4.6 Compliance-aware Service Monitoring

In SOA solutions, a services management and monitoring infrastructure provides comprehensive ways of understanding exactly what is involved in a business process so it can cross organizational boundaries and function as an integral element in an end-to-end process chain. It also provides the means of auditing business processes that cross organizational boundaries. What is required is monitoring techniques and algorithms to validate the compliance concerns at runtime and to provide remedial mechanisms in case of policy violations.

Existing auditing solutions and tools are hopelessly outdated and are not applicable to SOA solutions [[17]. These are tightly coupled to the controlled application, and assume that applications are homogenous and monolithic in nature. In particular, existing Computer Assisted Audit Techniques (CAATs), provide merely support for document management, financial data-analysis (e.g. Unit 4 Account Analyser) and standard flowcharting techniques. In addition, some expert systems, simulation and mathematical systems supporting auditing have been proposed, however, they concentrate on quantitative analysis, treat control processes as black boxes, and, are typically based on unrealistic and rather restrictive assumptions. On the other hand, existing methods and tools to manage and monitor service-enabled processes, notably Business Process Management and Business Process Activity tools, including the ARIS Process Performance Manager and HPs Business Process Insight, fall short in providing sufficient support for auditing SOAs. In particular, BPM tools merely 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.

Some already existing research results can form a sound basis for addressing the requirements of this theme. Run-time Web service monitoring is essential for real world service-oriented systems. It allows system stakeholders to detect anomalous situations and maintain high level of QoS during system lifecycle. To address such requirements [18] proposes a framework and a tool for automatically deriving Web service monitors from high-level requirements descriptions. Other approaches concentrate on capturing and monitoring negotiations that incorporate security policies and policy models that facilitate service lifecycle management [19].

5. Summary

Business processes form the foundation for all organizations, and as such, are impacted by industry regulations. Where business processes stretch across many cooperating and coordinated systems, possibly crossing organizational boundaries,

business process-driven SOAs help deliver control over business processes, fostering standardization across a company or an end-to-end process chain and compliance with regulations, policies, and best practices. Compliance regulations, such as HIPAA, Basel II, Sarbanes-Oxley and others require all organizations to review their business processes and ensure that they meet the compliance standards set forth in the legislation. Therefore, SOAs should play a crucial role in corporate governance, allowing management to ascertain that internal control measures that govern their key business processes can be checked, tested, and potentially certified with their underlying Web services.

The challenges of compliant business processes and regulation compliant-SOAs constitute a vibrant area of service research, which has so far received only limited attention and has never been addressed to its entirety. For a holistic approach to compliant business process management (one that covers the entire compliance life-cycle from design time checking to run-time monitoring and adaptation of services), several important research problems need to be addressed. These include: advanced mechanisms for auditing SOAs, a sound methodology to manage compliance-centric business processes, a more ”human-centric” approach to compliance-driven service development, re-use and customization of compliant process fragments, formal verification of the compliance properties of composed services, and, finally monitoring facilities for tracking and validating compliance concerns at run-time.

References

1. Papazoglou, M.P. (2007) Web Service: Principles and technology. PrenticeHall.
2. Rezaee Z. (207) Corporate Governance Post-Sarbanes-Oxley: Regulations, requirements and integrated processes. John Wiley & Sons.
3. International Federation of Accountants. (2006) Handbook of international auditing, assurance and ethics pronouncements, John Wiley & Sons.
4. R. Hayes et al. Principles of Auditing: An introduction to international standards on auditing. Prentice Hall/Financial Times.
5. Papazoglou M.P. (2008) The Challenges of service evolution. Proceedings Advanced Information Systems Engineering Conference: CAISE 2008, Springer-Verlag, Montpellier, France.
6. Harmon, P. (2007) Business process change. Morgan Kaufmann.
7. Martin. (2007) J. Lean Six Sigma for supply chain management. McGraw-Hill.
8. Lazovik A., Aiello M., Papazoglou M. P. (2006) Planning and monitoring the execution of web service requests. J of Digital Libraries, 6(3).
9. Brandic I., Pilana S., Benkner S. (2006) Amadeus: A holistic service-oriented environment for Gridworkflows, Proceedings 4th IEEE International Conference on Grid and Cooperative Computing.
10. Khatib L. et al. (2001) Temporal constraint reasoning with preferences. 17th International Joint Conference on Artificial Intelligence: IJCAI, Seattle, Washington, USA.
11. Melloul L., Fox A. (2004) Reusable functional composition patterns for web services. IEEE International Conference on Web Services: ICWS’04.

12. Bova R., Benbernou S., Hassas S. (2006) An immune system-Iinspired approach for composite web services reuse. Proceeding of ECAI 06 - 4th International Workshop on Artificial Intelligence for Service Composition.
13. Bova R., e. al. On embedding task memory in services composition frameworks, IEEE International Conference on Web Services: ICWE 07.
14. Liu Y., Muelle S., Xu K. (2008) A static compliance-checking framework for business process models. IBM Systems Journal, 47(1).
15. Benatallah B., et. al. (2005) On temporal abstractions of web services protocols. Proceedings Advanced Information Systems Engineering Conference: CAISE 2005, Springer-Verlag, Porto, Portugal.
16. Guermouche N., et al., (2007) Privacy-aware web service protocol replaceability. IEEE International Conference on Web Services: ICWS07.
17. Murthy U.S., Groomer S.M. (2004) A continuous auditing web services model for XMLbased accounting systems. Accounting Information Systems, Elsevier, 5(2).
18. Robinson W.N. (2003) Monitoring web service requirements. Proceedings of the IEEE International Requirements Engineering Conference, IEEE Computer Society.
19. Skogsrud H. , Benatallah B., Casati F. (2003) Model-driven trust negotiation for web services.IEEE Internet Computing 7(6).