Bottom-Up approach for Compliance: The MASTER position.

Emmanuel Pigout, Philip Miseldine

(SAP Research)

1. Introduction

Compliance is the act of conforming to a set of requirements derived from internal organization policy, regulations, or standards. The process of managing the assessment of such regulations and policies, performing the associated risk analysis, evaluating the need to implement control processes as enforcement points, monitoring of such control processes, enforcing their operation, and carrying out continuous assessment of their status, is called *compliance governance*.

In general, compliance governance is a necessary practice in any organization as an important tool for internal management, but it becomes particularly decisive to ensure conformance with requirements mandated by external regulations or best practices which not only impact the internal operations but which can, in case of mishandling, affect also the organization's external image and reputation.

In this position paper we will show how crucial it is for a company to understand its internal environment in order to set cost effective control processes. For this purpose, we will provide a short description of an original bottom-up approach developed in the MASTER project to achieve this challenge.

2. A Motivating example from the HealthCare Sector: HIPAA

Why is it so important to define cost effective control processes?

Let’s take a concrete example of a regulation extracted from the Health Insurance Portability and Accountability Act (HIPAA-1996). This regulation says:

“Ensure protection of personally identifiable health information held or disclosed by a covered entity in any form including orally, written and electronically”

As with most of the regulations, HIPAA is generic and not related to IT making it problematic to apply the regulation over a business processes. Commonly, the business process owner will communicate their needs to the Chief Security Officers and Chief Information Officers (CSO, CIO), who will ensure compliance with the business process owners’ requirements, however this process is not transparent, and therefore does not leave much indication on the business process of how it was adapted to suit the regulation. This makes change management on the business process or the regulation particularly difficult.

At this time, CSO’s and CIO’s will turn towards a well known frameworks (COBIT, ISO/IEC 27002:2005, COSO…) that are standards to relate the regulatory requirements to IT implementable set of control processes that fulfil control objectives. Implementation of the control processes against the processes of the business will enable the conformity of the business process. For example, the HIPAA example shown can be related to “ISO/IEC 27002:2005 control objective 15.01.04 – Data protection and privacy of personal information” that states:

“*Appropriate policies and procedures should be implemented to ensure the confidentiality of personal data, consistent with statutory, regulatory and private requirements*.”

Even if the control processes to put in place to support the control objectives are clearer at this stage, the CSO and CIO might take arbitrary choice in selecting them due to an up-to-date knowledge of the environment where the business process is running. In the new trend of running business over service oriented architectures (SOA) the de-synchronisation between CSO and CIO knowledge and the execution environment might even be worth than in past. Indeed, flexibility, adaptability and rapidity of business process model over SOA crossbreed with outsourcing facility, which are the actual main selling points of SOA, are also the main factors in the disconnection of the management with its execution environment.

That is exactly at this point of the compliance process that in MASTER we think that an bottom-up approach will be useful and even indispensable to create cost effective controls. In the following section we are presenting this original approach that will give CSO and CIO to build controls independent of their execution environment.

3. Know your environment: Bottom-Up approach

We saw in the previous section that there is a lack of transparency when it comes to building cost-effective controls to satisfy regulations.

The MASTER's approach is to introduce an evidence model that describes the evidence that some service can produce based on the actions it performs in an abstract fashion, using ontological concepts. These concepts form a shared vocabulary with control modellers, such that both understand the meaning of the concept each uses. Consequently, using instances of the model, the CSO and CIO will be able to produce environment agnostic models of controls that reference the concepts defined in the common vocabulary. The modeller can then determine what evidence to capture to prove or disprove a control's correct application. These models will thus govern business activity and can be applied to the described services if available or any equivalent service.

Indeed as we already explained, a popular way for a company to model and implement business processes is through the adoption of the Service Orientated Architecture (SOA) paradigm. SOA requires an IT system to be architected in such a way that it can be exposed as services. These services externalise internal behaviours of the system through a common, standardised interface. Business processes are then modelled to orchestrate these services to reach the business goal required by the process. This allows the actual services that provide the business process implementation to change independently from the process specification. As such, so long as a set of services provide the same functionality, one may be dynamically chosen at runtime. This allows external entities to implement part of a business process, thereby allowing the process owner to outsource aspects of the activities of the process..

Therefore, the bottom–up approach prone by MASTER consist for a constraint to be related to service behaviours, for this purpose a model is required that allows a service to define its behaviour in a way such that supporting evidence can be inferred and collected.

4. Conclusion

A generic compliance approach consists in a top-down approach where regulators dictate the rules and punishments in case of infringement to the business process owner. The latter is then pushing their CSO and CIO to finally implement the control, who in turn pass this to the developer who will come up with hard coded controls that are costly to maintain and with a limited life time depending on the stability of the business objectives, IT landscape, and the regulation requirements. Our position in MASTER to avoid this burden of maintenance of controls is to have a bottom-up approach correlated to the top down approach. Those two approaches will met around a model describing services in term evidences produced and possible actions to conduct. This layer between control description and the infrastructure will provide the necessary element to build cost effective controls.