BPM and Compliance Management – From Overhead to Getting Ahead – Part 1

Neeli Basanth Kumar

The Need for Compliance Management

The importance of compliance has increased over the last few years in businesses across several industry sectors. In a survey of US firms conducted in 2009, the AMR Research group found that US firms plan to spend close to $30 billion in 2010 on compliance related activities[1]. Even after such investments, enterprises are still struggling to implement and manage the *overhead* of compliance in their applications. This situation results from the fact that compliance efforts are distributed, ad hoc and decentralized; for instance, it is often seen that one IT team works on compliance with BASEL II while another works on SOX, ISO, etc. Secondly, there could also be instances where different teams implement compliance for the same regulation on different applications in different ways. Thirdly, compliance management is getting increasingly unpredictable as the need to comply is distributed over a long period of time, based on regulations and market; for example, a situation where compliance for HIPAA is to be implemented immediately due to regulatory needs and ISO after six months. Lastly an application-centric focus during implementation adds to the complexity and results in embedding compliance requirements into application logic. For example, the privacy rules in HIPAA get *hard-coded* into Hospital Management System (HMS).

From business, minimal visibility on actual state of compliance and missing accountability on adherence to compliance are areas of concern as multiple teams update the application over its lifetime. On the other hand, from an IT perspective, there is no IT governance on the applications. Such lack of governance can lead to higher maintenance cost and minimal or no possibility of re-use. The lack of governance can also adversely affect or break the compliance when applications are changed. In order to alleviate these issues, there is a need for frameworks or methodologies to implement compliance related requirements in a structured and efficient manner.

Compliance, by definition, is a matter of ensuring that business processes, operations and procedures of the enterprise are designed and executed in accordance with a prescribed and/or agreed on set of norms and regulations. In this context, compliance usually brings to mind legislation and regulations like Sarbanes-Oxley (SOX)[2], Basel II[3] and HIPAA[4]. This strong association limits the perspective of compliance initiatives in an enterprise as a necessary *overhead* mandated by third parties that results in inefficiencies in the operations of the enterprise. On the contrary, studies[5] show that adherence to regulations can aid in improved operations in an enterprise.

Seen from the perspective of improvement of operations, compliance requirements may stem from multiple objectives. With regard *to regulatory needs*, an enterprise is mandated to adhere to legislative and regulatory bodies like Sarbanes-Oxley Act, Basel II and HIPAA. In terms of *organizational policies* and *best practices*, the enterprise processes and systems need to comply with set conditions to enable corporate governance and controlled execution of policies and procedures. From the perspective of *certification*, bodies like ISO, CMMI set some guidelines that need to be complied with. The exercise for implementing compliance should be able to efficiently

1 Hagerty, J. and Kraus, B., GRC in 2010: $29.8B in Spending Sparked by Risk, Visibility, and Efficiency. AMR Research, November 2009

2 Sarbanes-Oxley Act of 2002, Public Law 107-204-July 30, 2002. U.S. Government Information.

3 Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards: A Revised Framework, June 2004. Bank for International Settlements.

4 Health Insurance Portability and Accountability Act of 1996, Public Law 104-191-Aug, 21, 1996. U.S. Government Information.

5 Wagner, S. and Dittmar, L., The Unexpected Benefits of SOX. HBR, April 2006

manage the compliance needs vis-à-vis regulations, organization policies and best practices, and certification bodies.

To summarize, current implementations of compliance requirements are decentralized and distributed over time that result in duplication of efforts and higher maintenance costs. The lack of governance and application-centric focus results in hard-coded implementations that lead to minimal visibility into adherence, missing accountability to compliance and reporting by 'walking through the code.' This series of articles proposes an approach to implement compliance in a way that aids in getting ahead in the market rather than being an overhead. The two part series will discuss -

1. The need for a separate repository for controls
2. The concept of controls against business rules and integration with business processes.

This article discusses the need for separation of responsibilities and repositories and the concept of generic and specific controls to efficiently manage the controls spread across time periods, regions, departments, etc., in an enterprise.

Separation of Responsibilities and Repositories

As introduced earlier, lack of governance and application-centric focus results in two main issues from compliance perspective – lack of visibility and missing accountability of adherence to compliance. In order to gain clarity on these issues, four key stakeholders or roles[6] can be identified when embarking on implementation of compliance management.

Business expert: A business expert has thorough understanding of the business, its objectives, procedures and operations. In large enterprises, different persons or different organizational units carry out this role. A business expert's primary responsibilities include business optimization and efficient operations.

Compliance expert: A compliance expert has extensive knowledge of the regulations and certification bodies. This role is responsible for documenting the relevant controls as applicable to the processes and systems in the enterprise. The primary tasks are to interpret the regulations and derive controls in the context of the enterprise applications.

Allocating individual responsibilities enhances accountability of adherence to compliance with a single role of compliance expert across applications. This individual allocation must be supported by the management to handle situations when business objectives *conflict* with compliance objectives. Such conflicts typically arise when the business expert focuses on increasing the efficiency based on factors like cost, lead time, etc., and the compliance expert focuses on adherence to compliance by creating checks and balances that might apparently look like negating the efficiency goals (when seen tactically).

In some cases, this separation of roles is logical as the responsibilities of the roles vary vis-à-vis applications. For example, it is imperative that the business expert understands the compliance needs of a financial application to a much greater depth compared to an internal application like travel management.

The other two roles, i.e., internal and external auditors deal with auditing the processes and systems for compliance.

6 Namiri, K. and Stojanovic, N., Pattern-Based Design and Validation of Business Process Compliance, Springer-Verlag Berlin Heidelberg 2007

Internal Auditor: An internal auditor is responsible for checking and testing the processes and systems for adherence to set compliance needs. The internal auditor is also responsible for reports and other materials needed for external auditors to efficiently certify compliance.

External Auditor: An external auditor is a third-party independent auditor responsible for checking and certification of compliance to an enterprise.

These two roles are responsible for certification of adherence to compliance. Audits and reports on compliance as implemented in the applications are critical features in compliance implementation. These audits and reports act as a means to get certified on the compliance.

Once the roles and responsibilities are identified, the next step is to address the ownership and accountability for these roles. As discussed above, the present disjointed, decentralized and distributed approach results in a fragmented view of the state of compliance as implementation spreads across multiple systems. This minimizes the possibility of re-use of applications. This implementation does not provide efficient reporting. The only way to generate reports is to 'walk through the code,' and this proves to be expensive and time consuming affair. It becomes very difficult to manage the lifecycle of these requirements as compliance requirements are implemented across different systems. Finally the process results in a lack of overall visibility, missing governance, loss of efficiency and higher maintenance cost of compliance and IT systems.

A separate repository of controls will help to be the 'single holder of truth' and eliminate the issues of visibility and governance as all the controls across applications are implemented in a single repository. The repository will aid in enabling governance by managing the lifecycle of the controls. This is similar to the concept of process repository that provides an explicit view of all processes being executed from a single place. The repository of compliance controls should be owned by compliance experts and other components like processes that are placed in process repository, will be owned by process owners.

The bifurcation of roles and repositories enables

- accountability as each role is independently responsible for a particular aspect of business with compliance expert being accountable for compliance and business expert being accountable for business processes and applications

- separation of lifecycle management and governance of compliance controls and application components as they reside in different repositories.

Generalized and Specialized Controls

In addition to accountability and governance, the there is a need to support efficient management of controls. In an enterprise, different departments have varied controls to be complied with, in addition to global controls applicable across the enterprise with customizations as per variations in functions. Also, at times, the controls might need changes relevant to timelines based on regulations or changes in market. In a globalized market, large enterprises operate in multiple regions either directly or through their subsidiaries. In this case, the applicable controls could be impacted by the regional regulations. In such scenarios, the controls should be made specific, based on contextual parameters like departmental, regional or periodical needs.

For efficient management of compliance controls, these contextual parameters bring in a need for generalized and specialized controls. With such an approach, it is possible to configure a hierarchy of controls based on the concept of specialization. For example, an authorization

control regarding approvals of travel budgets is a generalized control, but it could be specialized to a role like Regional Head, who can approve up to a limit of $100,000. Typically, the hierarchy is two levels deep, but the depth could be higher in some cases. The same can hold true for specialization based on business entities, processes, regions, times, roles, etc. For example, consider the control on pricing. The enterprise can have a generic pricing model for its products when the control is implemented. But based on specific regional considerations, the management can configure a specific pricing for the region. In this case, the orders triggered from a particular region must comply with the specific control rather than the generic pricing control.

In an execution context, a compliance framework supporting such a specialization can be developed to choose the correct and relevant 'version' of the controls, based on different contextual parameters discussed above.

The concept of generalized and specialized controls provides the following advantages:

- A single repository provides a single view of both generalized (across the enterprise) and specialized (specific based on contextual parameters) controls.
- Simplified reporting without the need to go through the application of controls, spread across the enterprise applications
- Efficient management of the configured controls as change management and lifecycle is controlled from a single repository.

Conclusion

Those responsible for compliance implementation should take a holistic approach and focus on getting ahead of the competition instead of considering as an overhead. To be able to support such a view and reap its benefits, separation of responsibilities and repositories is necessary. This separation allows independent lifecycle management of compliance controls and applications leading to a very manageable and effective control and governance on enterprise operations. It also defines the required accountability and reporting features for internal visibility and external certification.

Business processes are among the most critical application components that need to be made compliant. The interaction and best practices to enable compliance management using business processes will be discussed in the next article.

Author

Neeli Basanth Kumar has 10 years of experience in conceptualizing, implementing, positioning in BPMS domain. Earlier Neeli Basanth was working with Cordys, provider of enterprise class BPMS and played varied roles from engineering to product management including senior product manager with responsibility of BPM stack of components. Neeli Basanth has consulted with several clients helping them with BPM initiatives and worked with analysts including Gartner and Forrester on product briefings and the trends in BPM space. Currently Neeli Basanth is working at Infosys Labs and actively involved in researching the topics around process based compliance, dynamic processes, on-demand BPM. Basanth holds master of sciences (mathematics) and master of technology (computer Sciences) and can be reached at neeli.basanth@gmail.com

BPTrends Linkedin Discussion Group

We recently created a BPTrends Discussion Group on Linkedin to allow our members, readers and friends to freely exchange ideas on a wide variety of BPM related topics. We encourage you to initiate a new discussion on this publication or on other BPM related topics of interest to you, or to contribute to existing discussions. Go to Linkedin and join the **BPTrends Discussion Group.**

