Advances in Business-Related Scientific Research Conference 2015 in Milan
(ABSRC 2015 Milan)
December 10-11, 2015, Milan, Italy

COMPLIANCE ACHIEVEMENT AND ASSURANCE OF PROCESSES AND SERVICES IN A DYNAMIC ENVIRONMENT

Ivana Šabatová

University of Economics in Prague, Faculty of Informatics and Statistics, Department of Systems Analysis

Czech Republic

sabi@sabi.cz

Abstract

Compliance achievement and assurance of processes and services with regulations, standards, and business requirements become a complex task in the permanently and increasingly changing environment. It should be resolved already in the stage of information systems' design and implementation. This paper introduces new concept of continual compliance management in dynamic service oriented architectures that reflects the most recent achievements in the field of information and communication systems. A system, process or a particular service is considered to be reliable and credible only if we are able to prove its compliance with the defined requirements in a trusted way. If the particular business process or business service is supported with an IT system, then the compliance assurance relates also to these supporting systems. This paper presents a methodology filling the gap between the potential of latest technologies implementation and business strategy development.

Keywords: Compliance Algorithm, Risk Assessment, Control, Business Process Management, Business Rules Management, Key Assurance Indicator (KAI)

Topic Group: Organizational information and communication systems

INTRODUCTION

With the latest IT technology development we are facing revolutionary change, a real shift of paradigm in how we can use IT systems and accommodate them according to almost daily changes in various businesses. On the other hand the organizations are under increasing pressure caused by multiple external and internal influencers, regulatory requirements not least among them. A lot of time and money is spent for compliance assurance related activities either required by external authorities and by those conducted consentingly and proactively on internal basis. These activities include various types of audits, but compliance achievement and assurance should be considered in wider context especially together with operational risk management processes. This context is described for instance by Doucek et al. (2008) in the area for IT security.

Audits are always focused on business process in business domains relevant to the subject of compliance assurance. The importance of process approach is significantly emphasized in the

latest updates of Quality Management Standard ISO 9001:2015 introduced recently by International Standardization Organization, ISO (2015) for example. This trend prospectively represents the end of paper load of internal directions lying untouched in the drawers. Deployment of emerging business process automation frameworks becomes useful not only for compliance assurance, but essentially for reasonable business outputs achieving.

Handling the complexity of risk analysis and risk management issues, strategic and business planning, compliance requirements definition, business process analysis together with its automation and complex IT systems management requires wide knowledge and extensive experience, the most likely not covered by one single manager. This complexity and lack of deep knowledge causes inconsistences between desires of the main business stakeholders and week day reality in performance of business processes.

The challenge is decreasing the complexity by introduction of comprehensive but understandable methodology based on usage of advanced IT systems.

THEORY

The auditing domain is well developed and documented by acknowledged frameworks originated in particular areas of compliance assurance. Because of IT relation of the topic I concentrated on those best practices spread in the area of information security, where the CoBIT introduced by ITGI (2007) framework is the lead, as also Doucek et al. (2008) and Fanta et al. (2009) confirm. Both former and recent practices of regulatory compliance analysis as a basis for potential automation of compliance achievement and assurance were introduced by Fanta et al. (2009).

Risk analysis is essential source for control goals setting and represents a link between them and regulatory requirements as the external influencer according to the Business Motivation Model (BMM) by OMG (2015). The elements of BMM relevant to the compliance achievement are highlighted in the figure 1. Risk identification and modeling uses different approaches and methods in different business domains as we introduced in Refsdal et al. (2011). Besides the information security based risk management standard ISO/IEC 27005:2008 by ISO (2008) there is another ISO document focused on general approach to operational risk management ISO 31000:2009, Risk management – Principles and guidelines also introduced by ISO (2009). Information security area of risk analysis used to be guided also by NIST Special Publication 800-53 issued by National Institute of Standards and Technology, NIST (2007), which is considered to be more practical and giving better methodological guidance to risk management implementations, as presented by Fanta et al. (2009) and Doucek et al. (2008).

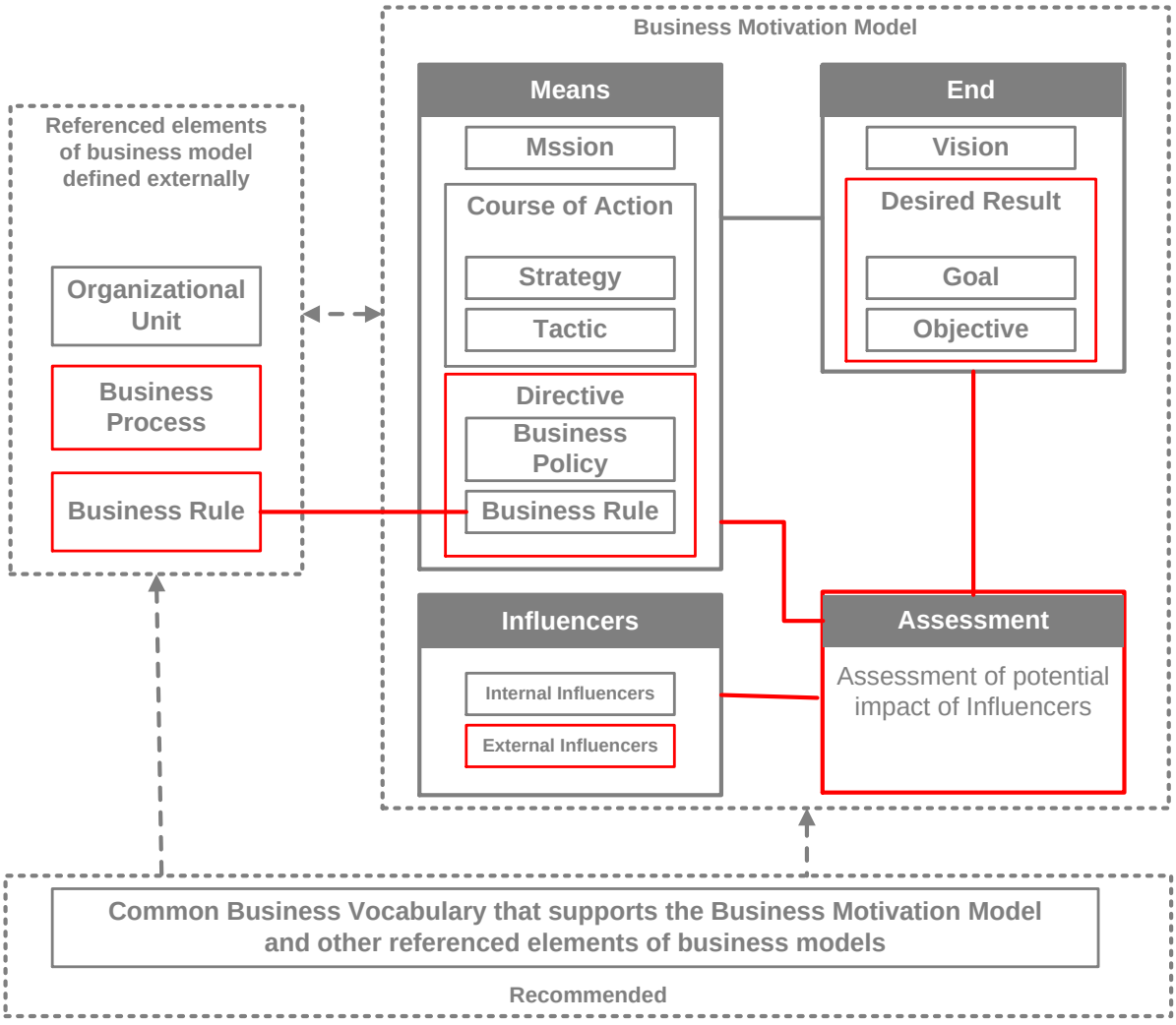
All three above mentioned frameworks relate the risk assessment to certain assets belonging to the particular organization, even if the ontology of their risk models and algorithms for risk calculation differ significantly. This fact restraints consolidation of cross sectional risk management, each business function treats their operational risks differently in accordance with respective best practices, patterns as well as supporting systems in their fields.

Opposite to the above mentioned methods there is the COSO framework relating the identified risks to the business goals of respective organization. COSO Enterprise Risk Management - Integrated Framework was published and later updated by Committee of

Sponsoring Organizations of the Treadway Commission, COSO (2015). Thanks to this "on goals" orientation COSO is better applicable in relation with Business Motivation model by OMG (2015) than the others.

Regarding business process modeling there are many methods and notations available, both open source and proprietary, widely used or developed for very specific purpose. The variety of business process modelling approaches was digested by Řepa (2012). Among the most spread and used BPM notations the Event Driven Process Chain (EPC) diagram is ranked, originally introduced by Sheer (1999) for ARIS business process platform. This notation is widely used and acknowledged as a well understood by business (non IT) people in the role of subject matter experts and/or process owners.

Figure 1: The highlighted elements of Business Motivation Model are relevant to compliance analysis.



Source: Author's chart based on BMM by OMG (2015)

Together with the starts of business process automation the BPEL (Business Process Execution Langue for Web Services) was introduced. Besides other resources this notation is understandably described by Juřič (2006). The problem was that BPEL is well understandable by IT experts in the environment business process automation platforms, but not useful for

business process communication among business people. In 2008 Object Management Group, OMG (2013) published the first version of Business Process Modelling Notation (BPMN v. 1.1), later upgraded to Business Process Model and Notation 2.0.2. BPMN notation became widely used both for formal description of business process flow and for full process automation using Business Process Management Systems (BPMS) at short notice. BPMN 2.0 has been adopted by the most of BPMS vendors as listed e.g. in the Gartner Magic Quadrant for Intelligent Business Process Management Suites by Sinur et al. (2012).

The idea of regulatory requirements formalization with the aim of compliance assurance automation originally comes from Sinclair et al. (2009). The idea was to implement Property Specification Language (PSL) introduced by Accellera (2004) for definition of a set of constraints expressing the control policy derived from control activity and/or control process assuring particular risk mitigation. I developed this idea into compliance algorithms definition based on PSL and described these formal expressions and their construction in detail in Šabatová (2011b, 2015).

METHODS

The findings, discussion and conclusion in this paper results from literature recherché, interviewing domain experts, designing the concept of compliance achieving and assurance in the environment of service oriented architecture according to Rosen (2008) and business process management systems (BPMS). The domain experts were among others senior auditors of integrated management systems, IT security auditors, IT architects, and senior BPMS consultants.

The designed concept was verified on the two case studies of real business processes analyzed in Hospital San Raffaele in Milan, Italy. First of them is an internal business process regulated by regional law, the second study is an example of compliance with business requirement achievement and assurance in multi-domain environment of iterated dynamic outsourcing. The initial situation of these use cases was described in detail in Sanna (2009). These case studies were verified by simulation with subject matter experts and business process activities performers of the hospital personnel.

FINDINGS

Compliance achievement and assurance concept

Compliance assurance concept includes a few new definitions related to compliance achievement and assurance resulting from the research published by Di Giacomo (2009) followed by Julisch (2010, 2011). For an effective automated system design we first of all have to define the way of automated compliance assessment, particularly the metrics and their constructs. Basic prerequisite for effective implementation and use of such metric is availability of all the data needed for its calculation. Possible technological approach to building compliance assurance monitoring architecture is fully described in Rodrigues (2011). When designing compliance assessment metrics we simply have to start with thoughts about the end.

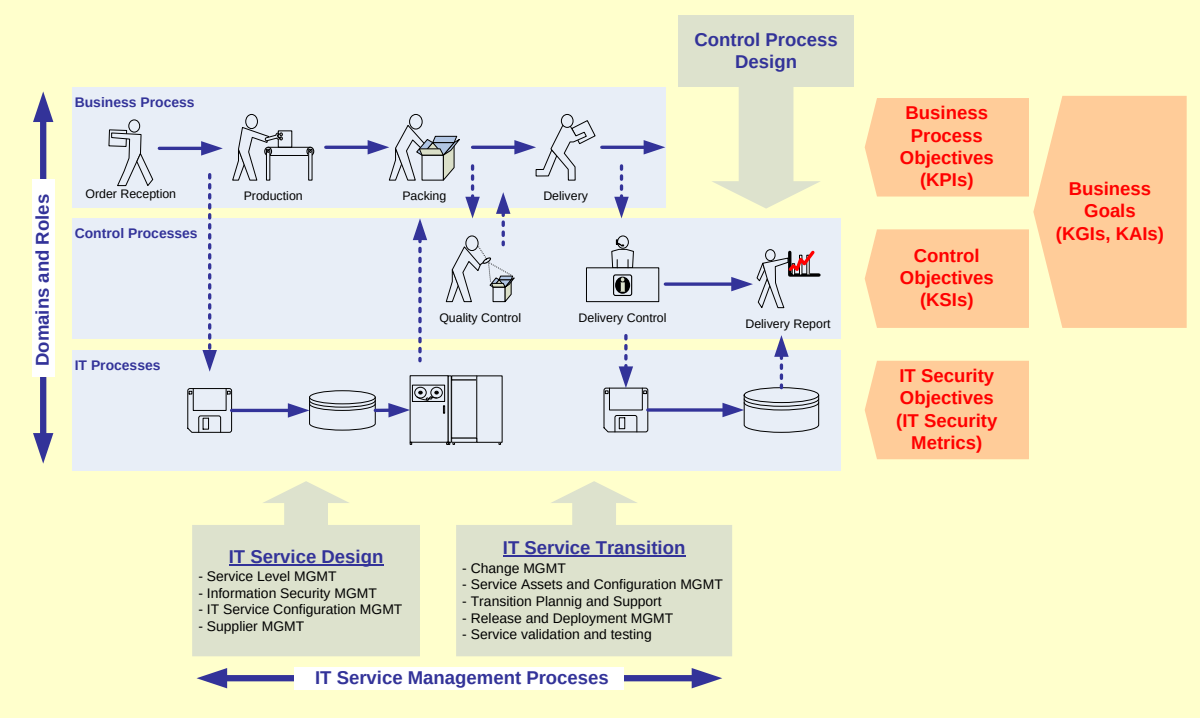
Analogically to classical audit planning when designing automated compliance assessment metrics we have to proceed from the initial identification of control objectives resulting from

risk analysis, thorough detailed business process analysis up to design of control activities and processes. Only then we are able to construct applicable compliance assessment metrics.

According to Julisch et al. (2011) and Šabatová et al. (2011) we define the ideal process as a target process compliant to the audited requirement resp. to respective control objective. The target process consists of the business process enhanced with control process. In simple cases control process can be represented by only one activity, then we call it control activity. The overall approach is depicted in the figure 2. In terms of productivity business processes are measured using Key Performance Indicators (KPIs). KPI tells us the measure of particular business goal achievement. We have to define a metric which will tell us the measure of particular control objective achievement. This is Key Security Indicator (KSI) that tells us the measure of comprehensiveness and efficiency of implemented control, realized by respective control process.

Nevertheless the compliance has to be assessed on the entire target process. Therefore the Key Assurance Indicator was defined as a measure that tells us whether all control processes derived from particular compliance requirement are implemented and used.

Figure 2: Business process and control process form together the target process.



Source: Author.

For the automated compliance assessment these indicators are defined in the following way:

1. Kea Assurance Indicator (KAI) is designed and calculated as a ratio of the number of target process instances conformal to the ideal process to the total number of target process instances.
2. Key Security Indicator (KSI) is designed and calculated as a ratio of target process instances with correctly performed control processes to the ratio of all target process

instances where the control process had to be triggered or applied according to control objectives.

The indicators can be calculated per certain time period (e.g. per day, week, months etc.), per certain number of triggered target process instances (e.g. per 100 instances) or per all instances since the target process was triggered the first time (to date). Obviously more than one of these indicators can be applied to one target process, since more than one control objective and more than one control process can be implemented for one business process.

Compliance Algorithm

After definition of compliance assurance metrics the following task was to invent the way how to automatically recognize the conformity and correctness of the target process to be able to calculate the KSIs and KAIs. There were two different approaches considered to define the ideal process. One way could be the identification and definition of all possible target process sequences and assigning those of them which represent the ideal process variants. This approach faces one important stumbling-block. In the most cases of real business processes it is not possible to identify the ultimate number of possible sequences. Therefore it is not generally applicable.

Sinclair et al. (2009) suggests application of Property Specification Language (PSL) for compliance requirements formulation as a set of constraints for particular target process. The advantage of PSL for these purposes is that the formulated expression can be easily transformed to automatically evaluable form. Using PSL we can for example express requirements on sequence of certain events, or set a required time limit or interval based on Linear Temporal Logic (LTL).

Šabatová (2015) introduced and described in detail two possible patterns of constraints formulated using PSL. The first one is compliance assessment pattern for the case study related to regulatory requirement for separation of duties, the other pattern represents the formalization of time bounding requirement.

Based on these considerations the Compliance Algorithm is defined as a logical statement formulated using PSL expressing the set of constraints for the target process. If this statement is true based on automated evaluation of target process instance data then the respective target process instance is designated to be conformal to the ideal process.

Compliance achievement and assurance methodology

This methodology represents a recommended procedure for compliance achievement and assurance system introduction beginning with identification of compliance requirements, following with design and development of control processes up to their implementation including formulation and implementation of the KSIs and KAIs.

This procedure results from the verification of the Compliance achievement and assurance concept using two business case studies mentioned above and in detail described in Šabatová et al. (2011).

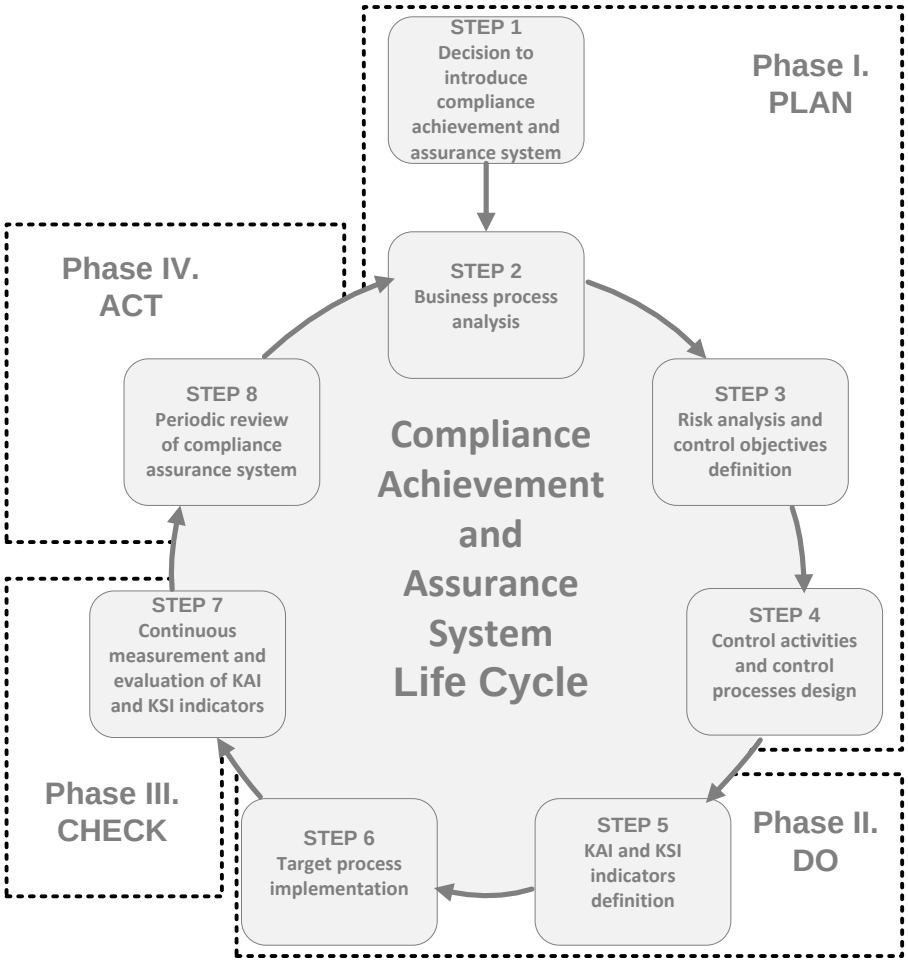
Creation of this methodology was inspired by modification of Deming Cycle PDCA (Plan, Do, Check, Act) similarly as used by Doucek et al. (2008) for describing the security incident

management life cycle. Compliance achievement and assurance life cycle is divided into four phases and eight steps as depicted in the figure 3.

Phase I Step 1: Decision to introduce compliance achievement and assurance system
Compliance achievement and assurance system design and implementation is a strategic initiative that requires full support and commitment of all stakeholders, especially of the organization's top management. This step represents the initial decision followed by elaborating initiation documents i.e. project chart, project plan and business case. An important source of information for them is represented with organization's business plan ideally structured by Business Motivation Model according to OMG (2015).

Phase I Step 2: Business process analysis
Business process analysis is related to the organization's goals and to the risks identified by assessment of relevant external influencers' impact on these goals. With respect to future automation business process model is designed using BPMN notation by OMG (2013). The main output of this second step is AS-IS model of the respective business process.

Figure 3: Compliance achievement and assurance system life-cycle.



Source: Author's modification of scheme introduced by Karjoth et al. (2011, 2011b).

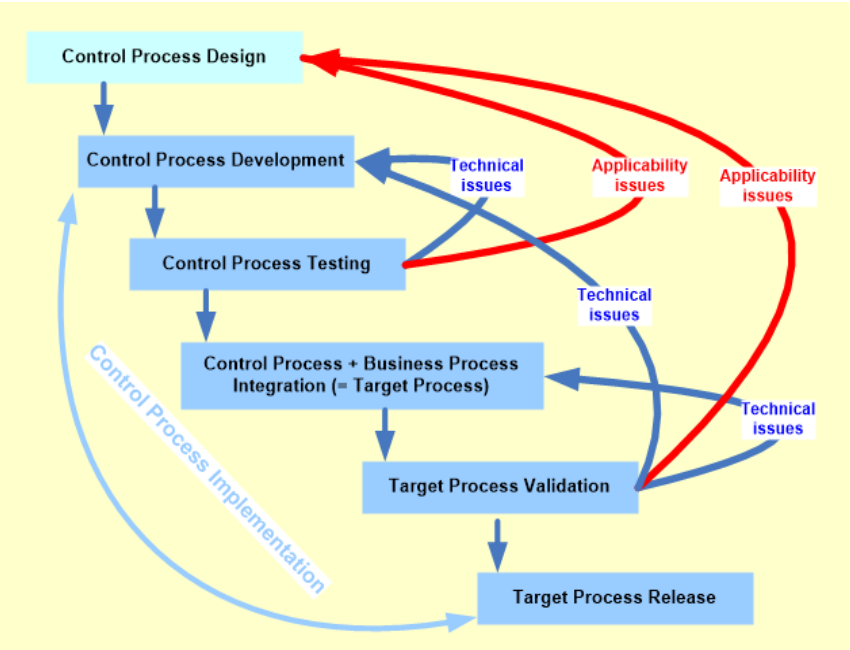
Phase I Step 3: Risk analysis and control goals definition
The main activity here is the GAP analysis identifying the differences between existing business process described in the AS-IS analysis and the compliance requirements derived from the identified risks. The main output of this step is formulation of control objectives leading to mitigation of the identified risks relevant to the business process.

Phase I Step 4: Control activities and control processes design
Based on the control objectives in this step the control processes are designed with respect to the existing business process and its business objectives.

Phase II Step 5: KAI and KSI indicators definition
The KSI and KAI indicators are formulated with respect to the future target process realization in order to be able to retrieve all process instance data necessary for the indicator's calculation. This step must be verified in the simulation environment and often we have to return to the step 4 and redesign the control process in order to be able to get such data without any extreme increase of expenses of business process operations.

Phase II Step 6: Target process implementation
Implementation of the control processes to the business process and realization of the target process is a crucial phase of the entire compliance management system life cycle. During this step the completeness of control processes must be verified together with verification of covering all respective control objectives. If the verification process identifies any inconsistency or missing element the implementation team must return to the planning phase II and revise the control objectives definition, the control processes design as well as the formulation of the indicators. Figure 3 explains the relations and types of issues to be resolved during control process implementation in a control process implementation cascade scheme. I described this process in detail in Karjoth (2011, 2011b)

Figure 4: Control process implementation cascade.



Source: Author's contribution to Karjoth et al. (2011b).

During implementation process the standard procedures of release management and change management must be respected and followed. The main output of this stage is the implemented, tested, documented and introduced target process.

Phase III Step 7: Continuous measurement and evaluation of KAI and KSI indicators
In the service oriented environment where the target process is implemented in the business process automation platform the indicators measurement is performed instantly and continuously. It allows us to review the compliance status of the business process at any time and undertake any necessary corrections or countermeasures when the compliance indicators show breach of the regulatory requirements.

Phase IV Step 8: Periodic review of compliance assurance system
Besides the continuous monitoring of KAI and KSI indicators also regular reviews should be undertaken in order to analyze the relevancy of the implemented compliance assurance system. Especially in highly regulated and turbulently changing environments it is a categorical imperative. In this step the formulation of control objectives and all the compliance assurance system elements derived from them must be confronted to the updated business plan, particularly to the assessment element of Business Motivation Model, if it is applied.

DISCUSSION

In Julisch (2011, 2011b) we distinguished between two types of Key Security Indicator. First is the KSI correctness, its definition corresponds to the KSI definition used in this paper. Additionally KSI coverage is defined as a ration of all target process instances where control process was triggered to the total number of process instances. In my opinion this metric is not relevant to the compliance assessment directly. However it can be useful for assessment of compliance implementation expenses and for the considerations related to

The compliance achievement and assurance methodology introduced here also differs from that introduced by Julisch (2011, 2011b) in the steps sequence. There was a dispute about the best order of steps related to control process design and formulation of the KAI and KSI indicators. Which has to come first, the chicken or the egg? Only after publishing of Julish (2011, 2011b) the compliance assurance verification proved that we can't define the exact KSI and KAI formulas in PSL sooner than we have exact control process and target process model. Till then we don't have the information model of the target process and don't know the data objects' attributes that we will be able to use for this calculation. It is obvious and I had to redesign the methodology according to these findings.

CONCLUSION

During last few years the process automation technologies have shown a significant advancement. Beside others its concept moved from pure BPM (Business Process Management) to ACM (Advanced Case Management), technology vendors agreed on BPMN (Business Process Modeling Notation) as a unified process modeling notation for process automation purposes. Neither of them has introduced any complex approach to the automatized business process analysis. The methodology introduces in this paper has been developed to over bridge this gap.

Practical experience together with study of relevant theoretical frameworks as well as system approaches to process design and modeling lead to recommendations that may become a good practice example for process analysts, consultants and programmers.

One important motivation of Business Process Management Systems (BPMS) and Business Rules Management Systems (BRMS) is their convergence of IT tools and the business people. The business process owners directly cooperate on the design and optimization of the business process model. Therefore unified ability to use the syntax as well as understanding its semantics by all project participants is very much important. Creation of a unified methodology represents a significant contribution to their understanding. Vice versa absence of a methodology can be important even critical inhibitor of the entire compliance achievement and assurance project.

IMPLICATIONS

I haven't included the technical recommendations for compliance management systems implementation to this paper; it will be subject of future publications.

Detailed description of implementation of the compliance achievement and assurance methodology is described by Šabatová (2015) in Building Assurance of Regulatory Compliance in Dynamic Service Oriented Systems. In future I plan to concentrate on the application of Business Rules Management Systems (BRMS) for KAI and KSI indicators. The latest versions of these systems allow easy formulation of logical expressions without necessity of programming. The calculation of KAIs and KSIs is performed by calling business rules webservices, where the business rule condition part represents the exact formulation of particular compliance policy.

ACKNOWLEDGEMENTS

The findings in this paper is partially based on my work and experience from participation in MASTER FP7-216917 the research and development project financed by the European Commission's Seventh Framework Programme.

REFERENCES

Accellera (2004). Property Specification Language Reference Manual Version 1.1. URL: http://www.eda.org/vfv/docs/PSL-v1.1.pdf

COSO (2015). Enterprise Risk Management - Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission. URL: http://www.coso.org/publications/executive_summary_integrated_framework.htm

Di Giacomo V., Julisch K., Burri S., Karjoth G., Martin T., Miseldine P., Bielova N., Crispo B., Massacci F., Neuhaus.S., Rassadko N., Pretschner A., Refsdal A. (2009). D2.1.1 Protection and assessment model for single trust domain. Official public deliverable of MASTER FP7-216917.

Doucek P., Novak L., Svatá V. (2008). Řízení bezpečnosti informací. Professional Publishing. ISBN 978-80-86946-88.

Fanta J., Svojanovsky P., Sabatova I., Julisch K., Pigout E., Worledge C., Micheletti A. (2009). D1.1.2 Regulatory Compliance Analysis. *Official public deliverable of MASTER FP7-216917*.

ISO (2008). ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management.

ISO (2009). ISO 31000:2009 Risk management – Principles and guidelines.

ISO (2015). ISO 9001:2015 Quality management systems – Requirements, International Standardization Organization.

ITGI (2007). CoBIT® 4.1. IT Governance Institute. ISBN 1-933284-72-2

ITGI (2007b). IT Assurance Guide: Using CoBIT® 4.1. IT Governance Institute. ISBN 1-933284-74-9

Julisch K., Miseldine F., Lim H.W., Bielova N., Neuhaus S., Refsdal A., Presenza D., Gallego-Nicasio Crespo B., Kearney P., Sinclair D., Neisse R. (2011). D2.1.3: The MASTER Final Protection and Assessment Model. Official public deliverable of MASTER FP7-216917.

Julisch K., Miseldine P., Lim H.W., Bielova N., Neuhaus S., Refsdal A., Presenza D., Gallego-Nicasio Crespo B.. Kearney P. (2010). D2.1.2 Protection and Assessment Model for Multiple Trust Domain. Official public deliverable of MASTER FP7-216917.

Jurič M.B., Mathew Benny, Sarang P. (2006). Business Process Execution Language for Web Services. Packt Publishing Ltd. ISBN 1-904811-81-7.

Karjoth G., Asnar Y., Louat B., Cui Z., Scholte T., Sinclair D., Sabatova I. (2011). D3.1.3: Methodology Handbook v.3. Official public deliverable of MASTER FP7-216917.

Karjoth G., Asnar Y., Louat B., Cui Z., Scholte T., Sinclair D., Sabatova I. (2011b). The MASTER Methodology – a Handbook for Practitioners. Official public deliverable of MASTER FP7-216917.

NIST (2007). NIST Special Publication 800-53. National Institute of Standards and Technology, US Department of Commerce, revision 2, 2007. URL: http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

OMG (2013). Business Process Model and Notation (BPMN) Version 2.0.2. OMG Document Number: dtc/2009-08-14. URL: http://www.omg.org/spec/BPMN/2.0

OMG (2015). Business Motivation Model Version 1.3. OMG Standard Document Number: formal/2015-05-19. URL: http://www.omg.org/spec/BMM/1.3

OMG (2015b). Semantics of Business Vocabulary and Business Rules (SBVR) Version 1.3. OMG Document Number: formal/2015-05-07. URL: http://www.omg.org/spec/ SBVR/1.3/PDF

Refsdal A., Stølen K., Asnar Y., Kearney P., Di Giacomo V., Presenza D. Sabatova I., Svojanovsky P. (2011). D1.1.3: Risk Analysis Modelling. Official public deliverable of MASTER FP7-216917.

Řepa V. (2012). Procesně řízená organizace. Grada. ISBN: 978-80-247-4128-4.

Rodriguez C., Daniel F., Casati F., Anstett T., Schleicher D., Burri S. (2011). D6.2.2 Warehouse model and diagnostic algorithms. Official public deliverable of MASTER FP7-216917.

Rosen M., Lublinsky B., Smith K.T., Balcer M. (2008). Applied SOA – Service Oriented Architecture and Design Strategies. Wiley Publishing, Inc., 2008. ISBN 978-0-470-22365-9

Šabatová I. (2011b). Kontinuální řízení shody v servisně orientovaných systémech. Sborník prací účastníků vědeckého semináře doktorského studia 17. února 2011. Vysoká škola ekonomická, Fakulta informatiky a statistiky. Nakladatelství Oeconomia, 2011. ISBN 978-80-245-1761-2

Šabatová I. (2015). Building Assurance of Regulatory Compliance in Dynamic Service Oriented Systems. Journal of Systems Integration Vol 6, No 2. ISSN: 1804-2724.

Šabatová I., Svojanovský P. (2011). D1.3.4: Security Compliance Guidelines. Official public deliverable of MASTER FP7-216917.

Sanna A., Marino D., Potral J.J., Hall M., Bastos-Rodriguez Ch., Soria-Rodriguez P., Sobota J., Miksu J., Asnar Y. (2009). D1.2.1: MASTER Scenarios. *Official public deliverable of MASTER FP7-216917*.

Sheer A.W. (1999). ARIS – od podnikových procesů k aplikačním systémům. COMSOFT. ISBN 80-238-4719-8.

Sinclair D., Neuhaus S., Gallego-Nicasio-Crespo B. (2009). D3.3.1: Specification of PRM property language and semantic model for verification and validation. Official deliverable of MASTER FP7-216917.

Sinur J, Schulte W. R., Hill J.B., Jones T. (2012). Magic Quadrant for Intelligent Business Process Management Suites. Gartner report G00224913.