Managing the compliance risk in banks: a draft methodology

Massimo Coletti
Banca Finnat Euramerica S.p.A.

December 3, 2006

Security and Control Systems
Published on www.mcoletti.net
Status: DRAFT

1 Introduction

This paper drafts an unofficial methodology, that I have been following for the management of the compliance risk originated by a number of norms, according to the mission of the organizational unit that is under my responsibility. The management of compliance risk is a hot topic in the banking industry, following the guidelines issued by the Basel Committee; this discussion was centered mainly on the aspects of governance, the duties of this new role, the organizational issues. There are however the practical aspects of this task, how the strategy and the principles should be translated in actions, information, reports.

The compliance issue is not specific of each single norm, as well as the organization is a single structure, so I felt the need of a single model for both the organization and the norms. Having a single model provides also a positive fallback to the other units that currently works around the organizational model of the company: human resources, internal auditing, organization.

The model was designed as an ontology, representing the elements of the organization (people, processes, structures, infrastructures, resources), as well as the elements of the norms, and the relationships existing among the two set of things. This approach, quite uncommon, resulted very interesting, thanks also to some excellent open source tools for knowledge acquisition and modeling.

2 Compliance Risk Management Goals

Compliance with applicable laws, rules, and standards is viewed as an essential mean for the promotion of the values of honesty and integrity throughout an organization. This is a general principle, that should inspire the strategy of the board of directors of an organization, as well as the daily operations of all the people working in it.

The compliance manager cannot stop at a general principle, but should design a "management" practice, providing an adequate level of reporting to the

top management, and tracking the actions that he undertakes in order to decrease the risk level. The expression "compliance risk" is defined as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a business may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its business activities (together, *"compliance laws, rules and standards"*). All this said, in order to manage effectively the compliance risk, a manager should:

- recognize the "sources" of risk, that are the "laws, rules, and standards";
- evaluate the current level of risk that the organization is facing;
- design plans for risk reduction.

All the listed activities should be properly reported to the top management, the real responsible for the compliance risk.

I have approached this problem using an ontology-based knowledge model, that represents all the concepts involved in compliance risk management. Beside this model, I have developed a reporting strategy, allowing me to provide the top management with synthetic and expressive analyzes of the "compliance risk position" of the Company.

3 Conceptualization of norms

The first step in this methodology is the recognition of the set of laws, rules, standard, policies that are the actual sources of risk. The recognition process is not a one-time activity: the manager should always be aware of the changes overcoming in the "normative environment". This is accomplished by various means: communication channels within the organization, advisory from legal consultants, business organizations, personal study, etc. For each norm, the manager will identify the relevant "concepts" described in the norm. The term "concept" is very abstract: it includes a wide set of ontological patterns that are present in every norm. Conceptualization is a useful step: you can discover what the norm requires you to do, the relevant social figures defined by the norm, the sanctions, the kind of things that the norm deals with. The taxonomy of concepts is an useful guide when you have to connect elements of your organization with parts of the norms; but the more relevant value of this taxonomy is in the holistic view that it provides to the complete set of norms.

4 Identify the requirements and related risks

When you have a complete taxonomy of concepts, you should have populated a class of concepts named *accomplishments:* each of them specify a requirement from a norm: if you are not satisfying the requirement, you risk a loss, a sanction, or a damage to your business reputation. It is important to check if a requirement is implied by another requirement: in this case it is not necessary to audit its realization, but if you don't satisfy the "extensive" requirement, you are facing two risk, one from the "extensive" requirement, one from the "overridden" one.

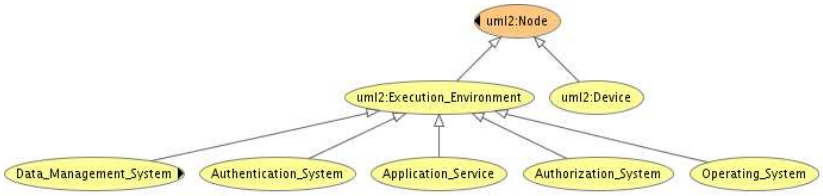

Figure 1: A fragment of the ontology representing network nodes

Another important point, during this phase, is the connection between each requirement and the "control points" within your organization. A *control point* is an element of your organization; it can be:

- a process,
- a role,
- a person,
- a physical place,
- a device,
- a perimeter,
- a resource (goods, material, information).

One (or more) control points are the elements where a "legal situation" is evaluated. For example, if a rule states that "the business capital should exceed the 15% of its net debt", the control point is the account where the capital amount is posted. If the rule is "each workstation should have an antivirus regularly updated", control points are all the personal computer in you organization.

The ontology describing the components of the organization provides a general and integrated views of your business, and can be used as the basis of several other "vertical" needs, as business continuity, information system security. The picture 1 shows a fragment of the ontology describing network nodes.

5 Evaluate the risk

Having defined the accomplishments, the control points, it is now straightforward to perform an audit of each control point, checking if all the relevant requirements are satisfied; the result will be a list of "non compliance", and a list of satisfied requirements. Your methodology should help you to prioritize the order of the audits, in order to spot as soon as possible the "non compliance" situations that are the sources of the highest risks. When you have identified a "non compliance", you should be able to evaluate the *risk level* related with this situation. The risk level is defined according to a number of criteria, at company level. It is a good practice to identify a small number of *risk levels*, according to the kind of sanctions applicable if you infringe that rule. A possible scale can be:

Level 0 if you don't have a classification of risk. This is a bad situation, because you don't know what is your situation.

Level 1 if the infringed norm have a penal sanction applicable (as arrest).

Level 2 if your risk is limited to penal sanctions, but only of monetary type.

Level 3 if you are risking a general financial sanction.

Level 4 if you are risking only the infringement of best practices or internal procedures.

Level 5 if you are compliant with norms.

6 Reporting the risk position

When the evaluation and audit process is completed, you can prepare a *Risk Position Report* for your top management. This report should express, possibly as a synthetic graphical map, how your business is positioned against risks. The report will usually include all the applicable norms, providing:

- the number of "non compliance" for each *risk level*;
- the severity of the "non compliance";
- the classification of each situation as "unacceptable", "unsatisfying", "satisfying".

This kind of report is a fundamental tool for the strategic decisions of the top management; the position of "non compliance" situation, and their severity, provides a natural priority guidance for the definition of a plan ofamendments. Clearly, a single synthetic report is not enough to define a strategic plan, it will be completed with detail situations (for each norm, each business area, each kind of resource, etc.).

7 Planning

Once you have received a formal strategic plan from the top management (or – more commonly – you have participated in the evaluation of this plan), it's time to return at a tactical level, and translate the strategic plan into a number of actions (or measures) targeted to single control points. The result will be a reduced number of "non compliance", and hence an improved risk position.

8 Conclusions

The approach described in this paper is aimed at the design of an integrated ontological model describing the requirements of norms, how the organizational components fit into the legal situations described by the norms, and the "non compliance" situations existing in the business. This work is part of a bigger project (KISS); the resulting model, as well as part of the methodology described, are being implemented inside a commercial software solution, proving their effectiveness also outside the banking and financial industry.

8.1 License

9 Notes on the tools used

As I believe in the value of FOSS (free and open source software), and I use mainly this kind of applications for my researches, I would like to mention the applications that I have used for this paper, all the names are copyright :

- LyX, an interactive editor for TeX, for the document production.
- Protégé, an excellent development platform for OWL ontologies, and Java, the language used for the development of Protégé.
- Ubuntu, the Linux distribution.