



Risk & Compliance

IS GRC JUST ANOTHER ACRONYM OR A REAL OPPORTUNITY?

We all know that, in response to the recent financial crisis, regulators across the globe are focusing on a more robust supervision of all players in the financial services industry. A key effect of this trend is not only the launch of an increasing number of regulatory initiatives but also the fact that the Compliance function will become increasingly important in the near future.

In February 2011, one of our major clients launched a project aimed at reinforcing, mapping and harmonising the so-called “second level controls” throughout the Group, on the key regulatory areas that fall under the Compliance function remit; as a result of this initiative, our client’s Global Compliance Framework went into effect in June 2011. In addition, in May 2012, their IT Department launched a project aimed at providing the whole Group with a new platform to be able to manage all three levels of controls (from Internal Controls to Internal Audit through Compliance) on a single system. This platform is based on a market standard solution widely used in the Governance Risk and Compliance space.

The Open Compliance and Ethics Group (OCEG) defines GRC as a “system of people, processes and technology that enable an organization to”:

- understand and prioritize stakeholder expectations;
- set business objectives that are congruent with values and risks;
- achieve objectives while optimizing risk profiles and protecting value;



IS GRC JUST ANOTHER ACRONYM OR A REAL OPPORTUNITY?

- operate within legal, contractual, internal, social and ethical boundaries;
- provide relevant, reliable and timely information to appropriate stakeholders;
- enable the measurement of the performance and effectiveness of the system.

The basic building blocks of a GRC application include:

- integrated dashboards and dimensional reporting;
- enterprise-class workflow;
- document management;
- security and access control;
- import/export capabilities ;
- loss event database;
- key metrics (KPIs, KRIs, KCIs) ;
- issue remediation;
- audit trail.

Return on Investment

Although it is difficult to quantify the value added of a “global initiative”, fines and censure can highlight the potential cost of non-compliance; In any case some metrics have been developed to help calculate the potential value (see picture).

Interaction with the “baseline”

Regulatory risk assessment should be undertaken by each business line but responsibility ultimately lies with Compliance, which must perform the appropriate level of oversight and challenge. Under this framework, the business line would be able to apply its knowledge to assess the regulatory risks to which it is exposed. Compliance would then oversee this process in order to challenge the business on the identified risks.