



Governance, Risk and Compliance (GRC) on the agenda of the CIO

Central role of the CIO is crucial for successful Governance, Risk and Compliance

High costs for Governance, Risk en Compliance

Organizations are facing an increasing number of external regulations, like SoX, Lippens, IFRS and MiFiD. Due to globalizations of markets, increasing pressure on financial markets and high expectations of stock owners and customers, the need to comply with these regulations is becoming essential.

To comply with all these relatively new external regulations high costs are involved. The basis for a good GRC-implementation is founded by centralized business applications and standardized business processes, all within the domain of the CIO.

Which types of controls should be implemented?

Many organizations have defined a number of so called *key controls* to comply with the external regulations. These key controls are primarily focussed on the integrity of the financial statement. Within organizations that are using enterprise wide business applications like SAP and Oracle EBS the following key controls are typical:

- *Procedures* (e.g. sales pricing or central vendor selection).
- *Segregation of duties* (e.g. separating the task of entering invoices and release for payment).
- *Required input fields* (e.g. required fields for the VAT number of a customer and P.O. Box of vendors).
- *Tolerances* (e.g. prevention of high payment differences and granting too high sales discounts).
- *Reporting controls* (e.g. detecting overduesalesordersandoverdueinvoices).

Proven in control

When the controls are implemented, the effectiveness should be monitored and

External regulations like SoX, Lippens, IFRS and MiFiD require that a large number of controls should be implemented. The costs of implementing and monitoring the compliance are high. An opportunity for the CIO to reduce the costs of Governance, Risk and Compliance.

evaluated periodically (*proven in control*). However, the control effectiveness is sometimes difficult to compare as the different operating companies have different process flows and practices of registering transactions in the business applications.

Both the process flows and the registration in the business applications are a joined responsibility of both the CFO and the CIO.

Opportunities for the CIO

What are the opportunities for the CIO to counter the high costs and other problems regarding the implementation of GRC?

Besides the involvement of the CFO, the CIO should play a more central role from the very beginning of the GRC implementation.

Many fundamental problems with a GRC implementation have their roots in the business applications such as SAP and Oracle EBS and the business processes. Successful and sustainable GRC begins with the standardisation of business processes (process harmonization). Controls for Segregation of Duties, reporting controls and procedures can only be defined and implemented in the business applications if the business processes are aligned. The CIO can play a bigger role by

implementing the standardized (harmonized) business processes in centralized business applications. A number of multinationals are currently in the processes of migrating to centralized business applications with common processes.

The CIO can play an important part in the process of being proven in control by monitoring the control effectiveness.

The CIO can play an important part in the process of being proven in control by monitoring the control effectiveness. Proven in control means that the organization should have a controls monitoring system to prove that the controls have been operating effectively during a specific period.

Using a central controls monitoring system the costs of collecting, analyzing and reporting the control effectiveness can be reduced significantly.

In the next issue of CxO Media an article about continuous monitoring of business processes will be included. Continuous Monitoring is a process that management puts in place to ensure that its policies, procedures, and business processes are operating effectively.

