

Governance, risk and compliance in a mechanical engineering company

Willy Holtkamp
ifb group

How an ICS project audit can increase transparency and profitability

GRC rules impose a binding framework on corporate management. These include laws such as the Sarbanes-Oxley Act (SOX), quality and best practice standards such as COSO II, CobiT and ITIL as well as auditing standards and internal guidelines.

However, the fact that compliance with all statutory provisions alone will not suffice, is ably demonstrated using the example of a successful German mechanical engineering company that has a host of production and sales companies both in Germany and abroad. In order to bring its governance compliance system up to the requisite US-SOX level, in close coordination with its auditor, the company combined the COSO model and the CobiT best practice approach to IT into a uniform GRC framework.

Ostensibly this served to cover a host of relevant SOX and GRC requirements. However, despite this move, the system did not prevent considerable losses occurring primarily as a result of unexpected or recognised, but underestimated, risks incurred with corporate projects.

A brief analysis by the ifb group showed that

- the ICS was not sufficiently supported by IT
- processes within the group – including project management processes – were not uniformly defined, evaluated or documented
- project reports were not always sufficiently up-to-date

Resolution of these problems occurred in two phases with the aid of ifb:

Phase 1: analysis and improvement of the existing GRC system, above all by eliminating control and management weaknesses in group-wide processes.

Phase 2: analysis and optimisation of the existing internal control system (ICS) for project risks within the scope of an ICS project audit with the aim of identifying structural risk potential at an early stage of project management and installing commensurately effective protective measures.

Integrated GRC model architecture

- ▶ Level 1 **regulatory environment**
Harmonisation of regulatory requirements, such as SOX variations, the EU 8th Directive, German Corporate Governance Code, international laws etc.
- ▶ Level 2 **internal control environment**
Interlocking of control framework and application of Best Practice according to COSO, CobiT etc.
- ▶ Level 3 **processes**
Control objectives and measures, risk controlling, early warning system, control maturity model.
- ▶ Level 4 **IT support**
Monitoring/assessment of IT efficiency, data security, dataflow etc.

Integrated GRC model architecture affording consideration of regulatory environment, the internal control environment, processes and IT support



□ Phase 1: GRC optimisation

Firstly, on the basis of the above-stated defect analysis, a precise and integrated GRC model architecture was developed (see illustration) and documented in the redesigned compliance policy. This new GRC architecture integrated the following four levels: regulatory environment, internal control environment, processes, and IT support. In line with the 'COSO cube', the following three dimensions were also included: eight enterprise risk components, four entity units and four objective categories.

As a result, company practice in terms of GRC became simpler, more unified and gained considerably greater transparency thanks to the internal GRC reporting process. Adherence to the new compliance policy is analysed quarterly by means of internal auditing, as is the ongoing development of ICS quality using a maturity model.

For the purpose of optimising IT support, the obsolete IT system pertaining to the ICS was also replaced by the latest ifb ProKoRisk® software.

□ Phase 2: ICS project audit

Building on this, the ICS project audit followed in a second phase; whereby the defect analysis effected in phase one was completed and, amongst other things, a term repository was also formulated. In addition, the ICS project audit included definition and introduction of an IT-supported project risk early warning system.

Specific optimisation measures of the ICS project audit are demonstrated by way of the following two examples:

1. A new project guide was developed, using precise definitions to ensure that verbal assessments of risks and opportunities can be numerically arranged. This is a useful tool, for example, in the risk early warning system, where it allows the significance of negative variations from planning to be immediately assessed. Moreover, the binding term repository ensures that projects and their associated risks and opportunities are classified and evaluated according to clear uniform criteria.
2. Additionally, the earned-value principle was introduced for all projects. This presents project costs incurred to date against the progress achieved by the project. As such, this function provides important key ratios that enable comprehensible and uniform assessment of risk. The process is also continuously monitored technically by means of the ProKoRisk® Active Communication Server.

Following implementation of a bundle of prioritised measures, the mechanical engineering company now has an integrated ICS boasting high practical utility that links seamlessly into the GRC environment. As a result, the ICS provides the key components of the group-wide risk management system and has a process-based structure. This in turn enables the success of corporate projects to be enhanced by way of fulfilling GRC requirements. In the project risk management example, this translates into high transparency in terms of risks, costs and the status of projects, while simultaneously facilitating standardised risk assessments and protective measures and thus a reduction of losses stemming from unsuccessful projects.

Willy Holtkamp