

Business Process Management and Governance Risk & Compliance Management: two separate worlds?

The Linkage of BPM and GRC topics

Reading a newsletter of Leonardo Consulting you would not be surprised to find the word “Business Process Management” in the headline. Not that common is the topic “Governance, Risk & Compliance”, which is indeed becoming more and more important: Quality standards (e.g. ISO 9000) in various business areas as well as laws and regulations that have been introduced and are binding. This article puts a spotlight on both Management areas in order to illustrate, how they are linked to each other.

Business Process Management is well known as an approach to improving an organisation’s processes, by aligning all relevant aspects of an organisation promoting effectiveness and efficiency. Corporate Governance describes the regulation framework for a target-oriented, responsible and ethical administration and a regulated control of organisations in accordance with the existing law. Risk Management integrates the handling of risks that threaten the achievement of strategic and operational business objectives and therefore covers topics like risk identification, risk evaluation, risk mitigation and risk monitoring. The Compliance Management, last but not least, is the fulfilment of all relevant internal and external, binding and voluntary requirements of all stakeholders. So much for the definitions, but how are the GRC topics related with BPM?

A good example is the Internal Control System (ICS). Being influenced by the US Sarbanes Oxley Act in 2002 which put a spotlight on risk inheriting processes and process steps as well as reasonable controls and their ongoing execution, the topic ICS became more and more common and important. See also the best-practice guidelines set by the Australian Stock Exchange (ASX) which requests companies to implement a risk-management process within their Risk & Control Management systems and its assessment. However the guideline is not compulsory for organisations to follow. But it makes it obvious: no business without business processes. And these processes and process steps inherit risks. Business Process Management is therefore an ideal basis for risk evaluation, risk mitigation and risk monitoring.

The existing process knowledge should be used in order to support the Risk Management succeeding in these topics. Once the risks have been identified it is about setting up appropriate controls, mitigating the evaluated risks. If specific laws have to be followed, (e.g. SOx with a financial focus) the relevant process areas are clearly defined. BPM can support these compliance aspects by providing the process knowledge and, if any tools are used, the maintenance of the GRC related data as well as its communication. Risks and controls could be assigned to process steps and specified with responsibilities and information about application systems or tests to be executed to ensure the controls effectiveness. The BPM repository, if a tool including a database is used, would ensure a sustainable approach by offering GRC specific reports or having the data required to feed a workflow tool handling the risk evaluation as well as the testing of designed and implemented controls.

These are just two examples substitutionally for various business cases, where BPM and GRC are linked to each. In conclusion, it is worthwhile to look at BPM and GRC questions in a combined approach, as both Management areas do contribute to each other in specific business areas and therefore the effectiveness and efficiency of both BPM and GRC related aspects could be increased.