

Integrating GRC Practices through Enabling Technology

World Energy® interviews Scott Wisniewski of Protiviti

Emerging global risks and regulatory pressures continue to drive energy companies to implement risk management practices that provide transparency, demonstrate corporate stewardship and reduce exposure while allowing them to pursue their strategic objectives. Energy companies face a critical choice: approach future investments in compliance initiatives as one-off, isolated activities, or use them to strengthen and unify their risk culture and align best practices to protect and enhance shareholder value.

World Energy: Given increasing demands and regulations, what risks do organizations face if they continue to manage compliance efforts as isolated activities?

Wisniewski: Many companies tend to address emerging demands in isolation of one another instead of incorporating them into a broader risk management framework. It is common for risk management teams within an organization to view risk through different lenses, rather than through a unified risk language and taxonomy. This approach has several consequences. Like a financial system without a comprehensive chart of accounts, companies without a comprehensive risk model to apply consistently across the enterprise may leave certain high-risk areas unaccounted for and, thus, unmanaged. On the flip side, certain risks simply will be called by another name, depending on the perspective of the individual risk management team. This can result in redundant allocation of risk management resources, unnecessary distraction of business/risk owners and inconsistent reporting information. The lack of a unifying framework also will make it difficult to analyze the interdependency among risks.

World Energy: What benefits will energy companies gain by instituting an integrated risk management process?

Wisniewski: Risk managers who integrate governance, risk and compliance (GRC) practices into their organization can better face today's market challenges. The value of an integrated GRC program is to do three things:

- Give management a more comprehensive view of enterprise risk.
- Reduce total loss exposure.
- Optimize resource allocation to reduce the total cost of risk management.

World Energy: Are there barriers that companies must overcome to implement a truly integrated risk management program?

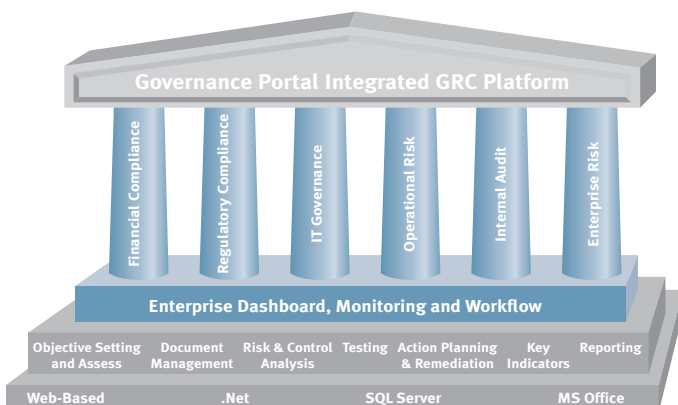
Wisniewski: Yes. While the value of an integrated GRC program is becoming more widely recognized, risk managers do face several key challenges when adopting this approach. One is the development of a unified risk management framework that supports cross-team coordination. Risk management teams still tend to work in isolation from one another and have compiled historic data using their individual risk frameworks. This is a barrier to change. It is essential to develop a uniform risk taxonomy, which includes the development of an enterprise risk model, process classification framework and governance structure. It also is important to note that risk management teams must continue to have the flexibility to identify business unit-specific risks, key risk indicators (KRIs), events and applicable response strategies. The integrated risk framework simply provides a method for organizing and aggregating this information into key enterprise risk themes.

World Energy: Are there GRC technology tools on the market that can help companies execute and manage an integrated risk management program?

Wisniewski: Technology plays an important role in establishing an integrated GRC program and provides many benefits for executing and managing it. Several tools are on the market today.

Protiviti's Governance Portal is an integrated platform that facilitates a unified risk management approach, enabling a sustainable, repeatable and cost-effective GRC program. This approach is supported through each of the Governance Portal's licensed modules for the following types of programs:

- Controls management – A framework that supports control documentation, analysis and testing.



- Risk management – A framework for assessing inherent, tolerable and residual risk across defined enterprise categories.
- Incident management – A system for collecting actual, estimated and “near miss” operational losses.
- Assessment management – A robust survey engine designed to enable a sustainable, ongoing self-assessment program across multiple governance and compliance activities.
- Internal audit management – An internal audit planning and execution system that supports key audit phases.

World Energy: Can GRC technology provide companies with greater efficiency and benefits?

Wisniewski: Yes, definitely. In fact, GRC technology platforms are designed to do three things. First, they enforce consistent application of a unifying risk management framework. Second, they facilitate the coordination of multiple risk management team efforts, while distributing effort and accountability to business/risk owners across the enterprise. Third, they provide holistic identification, assessment, management and reporting of enterprise risks.

As mentioned previously, the development of a unified risk framework is essential. Once the organization has developed its uniform risk taxonomy, the implementation of a GRC technology platform will enforce usage and consistent application across the enterprise.

The development of a unified risk framework applied through technology also can help organizations optimize their resource allocation through coordinated risk management efforts. Often, organizations struggle to determine which risk management group owns a particular risk. For example, the risk of internal fraud often can have both an operational and a regulatory impact, which means that risks are not mutually exclusive to one particular risk area.

World Energy: Is there a particular area where companies do tend to assign risk ownership?

Wisniewski: Many companies are beginning to drive risk ownership to the business/risk owner. Typically, they ask the business/risk owners to identify specific events that could result in significant losses in their area and assess the effectiveness of their response strategies. Through the GRC technology platform, risk managers can view and leverage analysis already performed within a given area of the business. This capability limits business/risk owner distraction caused by redundant requests for information, while allowing risk management teams to analyze the impact of business unit-specific events in their respective contexts.

While it is important for the GRC platform to enforce the consistent application of a uniform risk taxonomy, it also must allow for the mapping of business-unit-specific analysis

to different risk management contexts. For example, a specific risk event identified by the business may relate to a given regulatory objective, financial reporting objective and operational objective all at once. In this regard, each of the different risk management teams must be able to relate this single event to its particular vantage point.

World Energy: What is the ultimate aim of a GRC platform, and how might an energy company benefit from this?

Wisniewski: Ultimately, an integrated GRC program should provide holistic identification, assessment, management and reporting of enterprise risks. Energy companies are well versed in quantifying certain risks, such as those that are market-related. However, the industry is challenged to find methods of quantifying operational risk exposure, largely due to the lack of credible operational risk data. While a degree of subjectivity is inherent in any operational risk assessment, GRC technology brings various data points together to support a more objective, forward-looking risk and control self-assessment (RCSA).

Three key inputs into the RCSA exercise are loss event data, KRIs, and the results of audits or tests performed around particular risk areas. These data points assist risk managers with triangulating around a more valid assessment of the impact of a particular risk event and the effectiveness of related response strategies. An RCSA also will support the identification of new risks and development of remediation plans so that the past does not necessarily become a prelude to the future. By providing a composite view of risk based on empirical data, GRC platforms improve the integrity of the underlying data used to report and quantify exposure across a broader set of enterprise risks.

Scott Wisniewski (scott.wisniewski@protiviti.com), a director at Protiviti, leads the Risk Technology Solutions Product Management team. He is responsible for the direction, design and development of Protiviti’s governance, risk and compliance (GRC) platform. Mr. Wisniewski has worked extensively with Global 1,000 clients in all industries, including energy, to implement the Governance Portal, a GRC technology solution, and create a sustainable, cost-effective GRC program. Mr. Wisniewski has been a speaker at several risk management and internal audit conferences. He is based in Chicago, Illinois.

Protiviti (www.protiviti.com) is a global consulting and internal audit firm composed of experts specializing in risk and advisory services. The firm helps clients solve problems in finance, operations, technology, litigation and GRC. Protiviti’s energy and credit risk professionals assist clients in managing the exposure associated with volatile energy commodities.