DoubleCheck

101 Gibraltar Drive #1e,
Morris Plains, NJ 07950
(973) 984-2229

CASE STUDY:

Integrating and expanding GRC and audit systems providing more effective risk management at Susquehanna

When Susquehanna Bancshares Inc. recognized the need to elevate its risk management and compliance capabilities, it looked into various alternatives. What it learned was that the framework for an enterprise risk management system that could also monitor Sarbanes-Oxley Act compliance already was in place – in software the company had recently begun using to manage audits.

Previously, Susquehanna used a number of diverse governance, risk management, compliance and audit methods. A universal warehouse of system controls was lacking, as was a common language when addressing risk. The company recognized the need for a more coherent and efficient approach to managing risk and compliance, and explored a variety of commercially available and in-house solutions with mixed results.

With a bit of planning and a coordinated effort linking risk management, compliance and audit, Susquehanna was able to meet a management challenge financial institutions across the United States face in an effective and cost-efficient manner. Susquehanna's audit group first started using a GRC software package from DoubleCheck LLC in 2009, two years after Ken Hobbs joined the company's IT audit group. Hobbs had a positive experience with a precursor software system at another financial institution, and believed it would also be a useful audit tool at Susquehanna. Initial meetings specified requirements and, after approvals were obtained, the DoubleCheck audit tool was tested and implemented.

"When we recognized the need to escalate GRC as a way of managing risk, and in addition needed a new SOX tool, we looked around at what was available and realized it made a lot of sense to leverage some of the good work that had gone into making the audit tool useful," said Hobbs, now Chief Information Security Officer for Susquehanna.

Though the GRC software package was initially purchased to audit operations, Hobbs believed it could adapt some common language across multiple applications in order to better assess risk within Susquehanna. He felt confident the compliance

Susquehanna

HIGHLIGHTS

With a bit of planning and a coordinated effort linking risk management, compliance and audit, Susquehanna was able to meet a management challenge financial institutions across the United States face in an effective and cost-efficient manner.

component would meet Susquehanna's SOX reporting requirements, and explored the flexibility of the system to produce an inventory of audit and SOX data and tools that could be effectively leveraged.

Susquehanna also considered other systems from feature, function and price perspectives. Ultimately, however, it concluded the best solution would be to strengthen enterprise risk management while meeting SOX requirements by expanding the DoubleCheck GRC platform. The two companies were confident they could continue collaborating on tailoring the software to meet their specific needs by way of the flexible configurability of the software modules.

"We were able to translate the audit and SOX terminology into some common broader enterprise risk management-based language," explained Hobbs. "This more coherent approach was critical for us to move forward with a system that contained efficient validation of processes and provided excellent visibility of data and management of risks. Establishing a consensus, parsing and keying data, and building risk algorithms were a very important part of this process."

It took eight months for Susquehanna to obtain an enterprise risk management system that integrated data from its audit and SOX systems. That may seem a long time, but a majority of the effort was on creating a common language for risk. The result was a solid framework for a system that management could easily access and use to better identify and measure risks across Susquehanna. Subsequently, the GRC system was up and running in 12 weeks, and the company now has a coherent inventory of controls and effective management tools.

When validating groups look at the audit and SOX data in the GRC system, they concurrently see risks and controls in a common language. The necessary audit reports are generated, while documentation for SOX Section 302 certification is produced. As assurance tests are able to provide effective controls, the validating groups can sign off on the system.

Already, Susquehanna and DoubleCheck are collaborating on expanding the flexible GRC platform to address more areas, which will enable an even broader overview and automated reporting of risks across the company's operational, financial and compliance functions. All of these groups will be validating and feeding data into the GRC system, which will yield increasingly useful insights into risks and their likelihood across divisions and business processes.

The benefits of Susquehanna's integrated approach to GRC

Susquehanna

HIGHLIGHTS

The benefits of Susquehanna's integrated approach to GRC continue becoming clearer as it moves forward. In the simplest terms, risks that threaten the attainment of company goals are scored more effectively. Processes associated with these risks are more easily identified. Causes can be mitigated, and controls validated or reassessed.

continue becoming clearer as it moves forward. In the simplest terms, risks that threaten the attainment of company goals are scored more effectively. Processes associated with these risks are more easily identified. Causes can be mitigated, and controls validated or reassessed.

From a practical level, immediate reporting of enterprise risks in a common language from different perspectives is also being made possible at Susquehanna. The use of common risk-related terminology is growing across the company. This is resulting in the compression of organizational effort and resources to manage risk across a broader spectrum of the company's operational, financial and compliance functions.

With audit and SOX reporting already integrated and efforts underway with regulatory compliance, how is Susquehanna considering further strengthening its management of risk? Vendor risk management leveraging the DoubleCheck GRC tool is actively being deployed at the company.

"We have the DoubleCheck VRM vendor risk assessment module pilot in place for Gramm-Leach-Bliley requirements," said Hobbs. "The tool is being configured to drive our vendor risk management process, an area of increasing concern to regulators. It will be picking up information that is traditionally isolated and integrating it into business processes, further broadening our enterprise risk management capabilities.

The use of integrated GRC systems for risk management within Susquehanna has evolved steadily during the past five years. The company seems determined to continue meeting the maze of compliance requirements and effectively and efficiently managing its risks and achieving goals in the highly regulated financial sector with an integrated, flexible and expandable GRC approach.

About Susquehanna

Susquehanna Bancshares Inc. is a regional financial services holding company with assets of approximately $18 billion. It includes a commercial bank that provides financial services at more than 240 office locations in the Mid-Atlantic region. Through Susquehanna Wealth Management, the company offers investment, fiduciary, brokerage, insurance, retirement planning and private banking services. Susquehanna also operates an insurance and employee benefits company, a commercial finance company, a vehicle leasing company, a mortgage division and a settlement services company. Susquehanna's extensive portfolio of financial products and services is managed locally to provide maximum value to customers and communities.

About DoubleCheck

DoubleCheck™ LLC is a leading enterprise-level governance, risk management, compliance and audit solutions software company. The DoubleCheck GRC and audit platform can automate and unify on a single platform any or all of any organization's governance, risk management, compliance and testing (GRC and audit) activities. This includes key requirements such as Sarbanes-Oxley compliance, corporate governance, risk and audit management. The solution is highly configurable, offering adaptations to easily fit each client's needs.

To learn more, visit our website at www.doublechecksoftware.com