

What if there was a system that provided a framework to integrate new legal or regulatory requirements that affect the organization's information assets in the shortest possible time and at the least possible cost?

What if you could systematically protect critical information assets and further protect the market value of your company?

What if you had access to an internationally recognized standard that provided a holistic level of governance across all information assets and all departments of your business?

Use an Information Security Management System (ISMS) based on International Standard 27001 as the Framework

Internationally, an increasing number of companies are using this standard as the roadmap for all their information security activities

In 2004, the Corporate Governance Task Force issued a call to action to executive management in the United States for active engagement in information security governance and in the process of integrating information security into its corporate governance program. Based on decades of evolving information security experience, executives now have access to detailed, tested and internationally recognized guidance that can be used as a foundation for this integration.

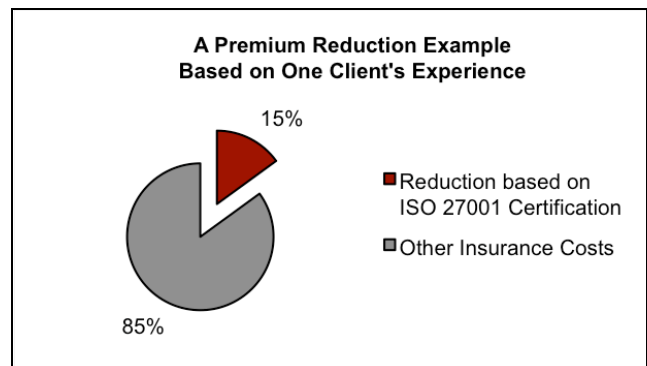
“Although information security is often viewed as a technical issue, it is also a governance challenge that involves risk management, reporting and accountability.”

continued on page 2

Certification drives Cost Savings

Insurance carriers recognize the value of information security governance through premium reductions

An increasing number of insurance carriers are offering premium reductions in Professional Liability coverage to those customers who have successfully completed the 27001 certification audit and registered their ISMS.



Using a governance approach to protect your organization's most critical assets – its information and reputation – is recognized as a legitimate safeguard resulting in cost savings for your company and for your insurance carrier. ■

Information is a critical resource of the business and must be treated like any other asset that is essential to the success and survival of the enterprise. The Task Force emphasized again and again the linkage between governance and information security.

Why are corporate governance processes and objectives increasingly dependent upon information security management? There are multiple drivers of this synergistic relationship:

- Reporting and other compliance requirements such as the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act and the Healthcare Insurance Portability and Accountability Act (HIPAA) depend on the integrity and availability of information and information assets;
- Shareholder value relies on the accuracy of information and the availability of information assets required for driving business processes and meeting business objectives;
- Information security is the common denominator in all areas of risk addressed by corporate governance including strategic, financial, technical, operational, legal and regulatory risk;
- The need to manage relationships among multiple data stakeholders in complex business environments and jurisdictions is increasing;
- The cost of litigation readiness and e-discovery can be directly tied to the ease with which information can be identified as well as how that information has been protected.

Information security, recognized as a fundamental governance process rather than simply a technology management issue, is critical in meeting overall governance objectives and fully realizing the benefits of information security to the entire enterprise. Executive leadership is therefore a key ingredient in any successful strategic information security initiative.

Implementing an Information Security Management System ensures a collection of processes and policies for use across your entire organization including:

- 1) a programmatic approach to evaluate and address vulnerabilities including internal and external threats;

- 2) a methodology for assessing the confidentiality, integrity and availability of your information assets through specific quantifiable measurements;
- 3) a framework for integrating future regulatory or legal requirements quickly and as inexpensively as possible;
- 4) a safety net to protect your information and the information entrusted to you by your customers, suppliers and other partners.

John B. Weaver, president and CEO of JBW Group International, advises executive management and board directors to be extremely cautious in how they interpret a lack of confirmed security breaches; without a systematic framework to evaluate information security, a lack of incidents could simply be the result of an organization's inability to identify the incidents.

JBW Group International would like to work with you to implement an effective information security governance system and help you join the over 5300 companies certified worldwide. ■

“The road to information security goes through corporate governance... The best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of Board and CEOs.”

National Cyber Security Summit Task Force, *Corporate Governance Report*, "Information Security Governance: A Call to Action", 2004

FOR MORE INFORMATION...

JBW Group International

P.O. Box 19373

Minneapolis,

Minnesota 55419 USA

www.jbwgroup.com

Email: info@jbwgroup.com

1.877.97.27001