



Information Security Governance Framework: 7 Key Questions for Audit Committees

[WEBWIRE](#) – Monday, July 23, 2007

The Information Security Governance Framework is a holistic, enterprise risk management model for a Board of Directors. It measures governance, compliance, and operational (legal) risks on identity theft and consumer protection. Boards of Directors of financial firms have a fiduciary and regulatory obligation to prevent corporate identity theft. The model:

CONTACT INFORMATION

Beck Miller
President
IP Governance Task Force
239-777-4638
miller@ipgovernance.com

- synchronizes relevant regulations for the banking industry. These include GLBA, FDICIA Section 112, FTC ACT, Lanham Act, Sarbanes-Oxley, California's AB 1950 and FINCEN's Identity Theft Suspicious Activity Report requirements, plus Basel and CAMELS, within 3 security layers per GLBA 501(b), 521 and 523, i.e., IT or Information Technology Governance, Network Vulnerability and IP or Intellectual Property Governance. IP Governance addresses corporate identity theft, a root source of rampant federal crimes against consumers per President's Identity Theft Task Force. Fraudulent domain names used within phishing, email spam and fake web sites are Unfair and Deceptive practices that attack trade secrets or sensitive customer information, inside and outside of bank IT networks, resulting in operational losses, operational risks and reputational harm for corporations and consumers.

- automates an independent risk management function with external peer review metrics from public information.

- generates a positive ROI by minimizing corporate identity theft, operational risks and losses, and capital reductions under Basel.

- includes 7 key questions and answers, i.e.,

What are our operational (legal) risk exposures and operational losses for information security governance per Basel and CAMELS?

In a scenario analysis, what are relevant litigation and regulatory enforcement cases?

What impact will operational risks have on our capital, credit ratings and CAMELS ratings?

Are disclosure statements accurate and complete for GLBA 503, FDICIA Section 112, Sarbanes-Oxley and Suspicious Activity Reports?

What are the board-approved risk tolerances, using effective metrics, for operational risk exposures and operational losses?

Do we have adequate internal controls with independent risk verification, effective metrics and periodic board reports on information security governance?

Do we have adequate resources for managing and reaching Board-approved risk tolerance levels?

Audit Committees seeking answers to these questions are encouraged to contact the IP Governance Task Force. The Task Force, which provides the Information Security Governance Framework, was formed in 2006 as a multi-disciplinary team of IP professionals. Members include industry thought-leaders from auditing, legal, and technology companies.

<http://www.isgovernance.com>

This news content may be integrated into any legitimate news gathering and publishing effort. Linking is permitted.

[WebWire®](#) 1995 - 2007