
From: srosenkranz@ScottStringfellow.com
Sent: Tuesday, January 02, 2007 10:17 AM
To: Comments
Subject: PROPOSED AUDITING STANDARD - Feedback

Dear Sir or Ma'am,

I am writing in response to Release No. 2006-007, published December 19, 2006. My concern pertains to your use of "Risk Assessments" in evaluating the effectiveness of internal controls. Speaking from a strictly information technology perspective, risk assessments are an involved and detailed undertaking comprised of both objective and subjective elements. They also vary significantly from the risk assessment I believe you are alluding to, which are subjective and operational in nature.

In my opinion, the differences between the two types or "risk assessments" must be captured and articulated before using them as the foundation for assessing whether or not a company's internal controls are effective. Based on my experience, auditors evaluating the effectiveness of information security controls as part of SOX Section 404 compliance are quick to assess a control as insufficient without identifying either the level of residual risk troubling them or how they derived that residual risk. This lack accountability in making such determinations is both frustrating and troubling. I believe that individuals performing evaluations should adhere to the same standards of due diligence and due care as the organization they are evaluating. Again this is my opinion, and I confess my perspective may be colored by the fact that I am the recipient of external audits and not the one performing them.

Finally, a variety of methodologies exist to perform information security-type risk assessments, and it might be prudent to articulate a general structure or approach which would be considered acceptable for companies to use so they are not deliberating the utility (or lack there of) of their process prior to auditors arriving to perform their evaluation and analysis.

Thank you for your attention in this matter and for working to make audits more efficient, effective and useful.

Regards,

Steve

Stephen R. Rosenkranz

CISSP, CBCP

SSI Security/Disaster Recovery Engineer

Information Systems Department

Phone: (804) 727-3438

Cell: (804) 512-9340

FAX: (804) 282-7234

1/10/2007

srosenkranz@ScottStringfellow.com

8006 Discovery Drive, Suite 300, Richmond, VA 23229

IntraOffice Mail Code: 306-87-03-00

This email message is intended only for the addressee(s) and contains information that may be confidential and/or copyright. If you are not the intended recipient please notify the sender by reply email and immediately delete this email. Use, disclosure or reproduction of this email by anyone other than the intended recipient(s) is strictly prohibited.

Scott & Stringfellow, Inc. is a wholly-owned non-bank subsidiary of BB&T Corporation.
THE SECURITIES SOLD, OFFERED OR RECOMMENDED BY SCOTT & STRINGFELLOW, INC. ARE NOT A DEPOSIT, NOT FDIC INSURED, NOT GUARANTEED BY THE BANK, NOT IN

From: srosenkranz@ScottStringfellow.com
Sent: Wednesday, January 31, 2007 5:00 PM
To: Public Affairs
Cc: Comments

January 31, 2007

Public Company Accounting Oversight Board

1666 K Street, NW

Washington, DC 20006-2803

Dear Sir or Ma'am:

On January 2, 2007, I submitted a comment to your comments@pcaob.org mailbox regarding the proposed auditing standard published in PCAOB Release No. 2006-007. Please note that the submission was made on my personal behalf and as such reflects my personal views and not the views of my employer. Please update my submission record and comment to reflect this.

Sincerely,

Stephen R. Rosenkranz

CISSP, CBCP

SSI Security/Disaster Recovery Engineer

This email message is intended only for the addressee(s) and contains information that may be confidential and/or copyright. If you are not the intended recipient please notify the sender by reply email and immediately delete this email. Use, disclosure or reproduction of this email by anyone other than the intended recipient(s) is strictly prohibited.

Scott & Stringfellow, Inc. is a wholly-owned non-bank subsidiary of BB&T Corporation.
THE SECURITIES SOLD, OFFERED OR RECOMMENDED BY SCOTT & STRINGFELLOW, INC. ARE NOT A DEPOSIT, NOT FDIC INSURED, NOT GUARANTEED BY THE BANK, NOT IN