Shuki Meirman, MBA
Yehuda Halevi 37/5
Netanya, Israel
shukim1@bezeqint.net

September 17, 2006

Comments to concept release No. 34-54122; file No. S7-11-06

Mr. Chairman and Honorable Commissioners:
Based on my experience as a consultant in various strategic projects and my last two years experience as a SOX compliance project leader in one of NASDAQ's Israeli companies, I have a few insights and ideas that I want to share with the honorable members of the Securities and Exchange Commission. I appreciate the opportunity to provide my perspective and hope you will find this helpful in your pursuit of providing a cost effective SOX compliance and auditing framework.

Objectives:

- Improve objectivity, reliability and validity of the auditing process, aimed at evaluation management's assessment of the effectiveness of the company's internal control framework.
- Set a "minimum" legal requirements definition for complying with the Sarbanes-Oxley act of 2002.
- Improve management understanding of SOX compliance process and legal expectations.
- Enhance transparency of company's internal control framework to investors and other interested parties.
- Enable companies to set different levels of control frameworks according to the company's investor's expectations (above minimum requirements).
- Enable investors to compare different companies from the internal control level point of view.

Method

My suggestion mainly involves three basic ideas:

a. Defining a set of generic process objectives and accompanied risks, common to most companies as a basis for the development and evaluation of internal control framework.
b. Developing a quantitative formal method of SOX compliance level grading instead of the existing pass/fail semi-intuitive grading system used by auditors.
c. Providing investors with results of internal control evaluation and letting them decide for their own, how they use this information on investment decisions.

Generic process Objectives and Accompanied Risks

- In order to assist companies with identifying risks and controls and enable a quantitative formal method of SOX compliance grading technique, a set of

Generic process Objectives and Accompanied Risks (GOAR) that are common to most companies, will be established, based on auditing firms accumulative knowledge.

- The GOAR will include a list of objectives, and for each objective a list of common risks, jeopardizing the achievement of the objective, will be defined.
- For my opinion there is no point in even trying to include a set of generic controls in the GOAR since the variety of controls is vast and companies have different methods in achieving the same objectives, although examples may be helpful.
- A good idea would be to divide the GOAR into three different sets: Company level GOAR, Major financial cycles GOAR and Information technology general processes GAOR.
- **Company level GOAR** will define the company's general internal control objectives and risks, classified into five sub classifications:
    a. "Control environment" objectives and risks.
    b. "Risk assessment processes" objectives and risks.
    c. "Information and communication" objectives and risks.
    d. "Monitoring processes" objectives and risks.
    e. "Antifraud program" objectives and risks.
- **Major financial cycles GOAR** will define the company's process level objectives and risks for each major financial cycle, under a sub classification of manual process vs. system/application process:
    a. Manual process objectives and risks will be classified (for each cycle) into:
        i. "Existence or occurrence" objectives and risks.
        ii. "Completeness" objectives and risks.
        iii. "Rights and obligations" objectives and risks.
        iv. "Valuation or allocation" objectives and risks.
        v. "Presentation and disclosure" objectives and risks.
        vi. "Cycle specific antifraud" objectives and risks.
    b. System/Application processes objectives and risks will be classified (for each cycle) into:
        i. "Completeness" objectives and risks.
        ii. "Accuracy" objectives and risks.
        iii. "Validity" objectives and risks.
        iv. "Restricted Access" objectives and risks.
- **Information technology general processes GOAR** will define the company's Information technology general processes objectives and risks, classified to:
    a. "System development" objectives and risks.
    b. "System change" objectives and risks.
    c. "System operation" objectives and risks.
    d. "Security and access management" objectives and risks.
    e. "Backup and restore" objectives and risks.
    f. "End-user systems and desktop applications" objectives and risks.

Management Internal control assessment process

- Management will analyze company processes, create a list of the company's objectives and risks based on the GAOR sets of generic objectives and risks and add, if required, identified unique risks that are relevant to company processes.
- For each risk, controls will be developed and defined in order to mitigate the risk and achieve the relevant objective.
- In some cases a GAOR risk might be found not applicable by a certain company, and this will be noted in the company risk analysis for the auditor to review.
- Controls will be documented and internally tested in order to support management assessment of internal controls.

The Auditing process

- Instead of providing a pass/fail attestation, the auditors will express their opinion on management's assessment of the effectiveness of the company's internal control framework using a SOX compliance grade (SCG) between 0 and 100. The SCG will be published regularly as one of the stock parameters available to any investor (ex. Yahoo-finance), thus allowing investors to take into consideration the company's level of control on any investment decisions they may take.
- On the long run a "pass" grade, that will represent a "minimum requirement level of control" from all NASDAQ traded companies, will be established.
- The SCG will be based on an aggregated grade comprised of several components weighted according to the component relative materiality (simple linear compensatory model).
- A good idea would be to distinguish components into three categories:
    a. Company level components, will be given up to 20% of total score.
    b. Financial cycles components, will be given up to 60% of total score
    c. Information technology general processes components, will be given up to 20% of total score.
- A possible SCG grading process:
    a. The auditor will review the company's list of Objectives and risks and verify that all relevant risks, of all three categories, were identified:
        i. Relevant generic risks from the GAOR set of risks.
        ii. Unique uncommon risks that he/she had identified relevant to the company.
    b. If some risks are missing the auditor will add them to the company's list and evaluate them accordingly.
    c. Company level controls and Information technology general processes controls, will be evaluated based on their expected effect on relevant risks prevention and detection and achievement of relevant objectives, a total score of level of control will be given accordingly (up to 20% of total SCG score for each).
    d. Financial cycles risks will be valuated based on each risk potential effect on financial statement ($) multiplied by its Likelihood of occurrence (%).
    e. The auditor will evaluate regarding each risk the level of effective prevention/detection coverage provided by existing controls and set the final F/S Exposure amount for the risk.

f. Total exposure will be calculated by summing all F/S Exposure amounts.
g. The final financial cycles SCG grade will be calculated based on the proportion of the total exposure amount and will be combined with Company level controls SCG and Information technology general processes controls SCG to a final SCG grade, which will be reported on the financial reports, representing the financial statement expected accuracy according to the company's internal control effectiveness.

- An example of an SCG grading process:

Objective	Risk	Effect on F/S	Likelihood	Control	Controls coverage of risks	F/S Exposure
Invoices relate to valid shipments (Existence)	Invoices are created for products not shipped	100M$	2%	Orders are not invoiced until … approval…	90%	200K$
….	…..	50M$	1%	……	70%	150K$
….	…..	20M$	5%	……	80%	200K$
….	…..	……	……	……	……	……
	Total	650M$			Total exposure	6,500k$

SCG (of Financial cycles) = (650M$-6.5M$)/650M$ = 99% accuracy of F/S

Given (for example)
SCG (of Company level controls) = 95%
And
SCG (of Information technology general processes controls) = 80%

Total SCG = (99%X60%)+(95%X20%)+(80%X20%) = 94.4%

- The SCG score will enable investors to truly evaluate the company's F/S while taking into consideration calculated risks regarding their accuracy.

Conclusion

A Quantitative method of evaluating management assessment of internal controls effectiveness will help auditors to conduct a sound auditing process, enable managers to understand expectation and commit cost/benefit trade-off in the design and maintenance of their internal control framework, and will enable investor to handle investment risks in a logical way taking into account internal control over financial reporting aspects.

I hope you will give my suggestions some serious consideration. If you have any questions or should further clarification be required or if I can be of any other service to you, please do not hesitate to contact me.
Sincerely,

Shuki Meirman