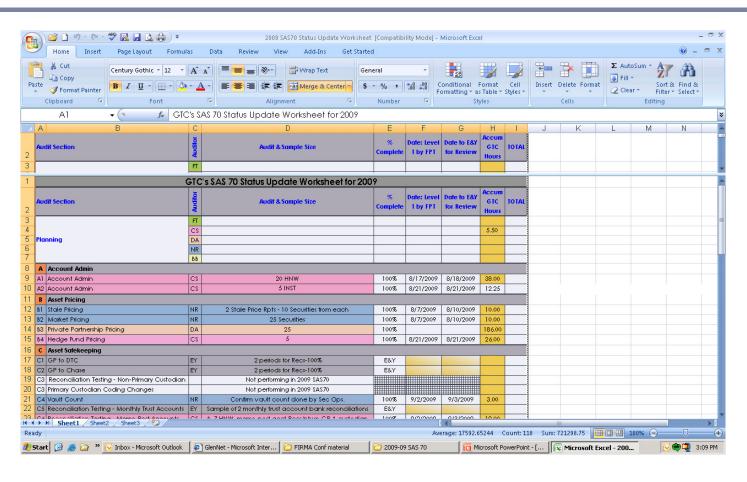
FIRMA National Risk Management Training Conference – San Francisco, CA Wednesday March 31, 2010

Internal Control Reports
Facts, Myths, and Best Practices

Francis P. Thomas
The Glenmede Trust Co., N.A.

- Extensive Planning (scope of controls, what elements are key to the audience)
- Designate an IA liaison
- Make sure all testing programs cover your key controls and are approved in advance by the CPA firm who will sign the report.
- Assignments should reflect efficiency and expertise.

- Do you obtain management's response to issues or does the CPA?
- Weekly status updates on progress.
- Target deadlines for delivery of completed sections.
- Adequate time allotted for clearing review notes, (manager reviews and partner sign off).



- Internal review / external approval
- Discuss how best to communicate results of testing for the report?
- Will report be made available in hard copy or via PDF electronically?
- Are you going to track recipients?

Does your SAS-70 give away too much information?

- Don't give flowcharts on how data moves and is controlled.
- Don't identify the actual systems you use. Say "trust accounting system" or "trade order entry system"
- Don't identify your strategic partners by name (telecommunications vendor, name brand routers and switches, etc.)

Vendor Management Committee **Duties**

- Oversee the establishment of all vendor due diligence practices and procedures
- Maintain oversight of data input to the vendor database
- Report up in the committee structure and escalate any security concerns
- Report any risk concerns to the Risk Management Committee

What is a significant vendor?

- Someone with access to client or employee NPI
- High business impact if product or service not available from vendor
- High business impact due to vendor interaction with clients/prospects
- High business impact if vendor fails

Using a vendor SAS-70

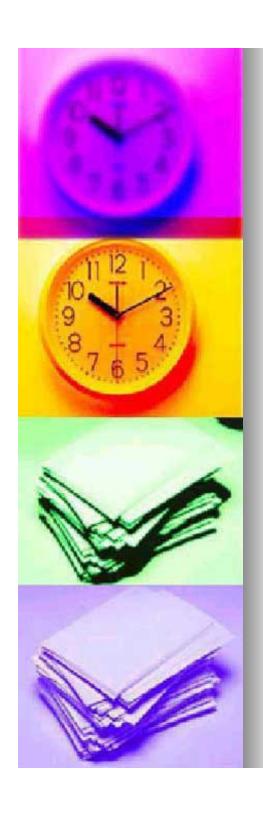
- What type of report is supplied (Type I/A or Type II/B with testing results)?
- Within the scope of the report, can you identify the product or service you purchase as being tested?
- Go to results and look for disclosures about the controls over your product or service. Are they acceptable?

Using a vendor SAS-70 cont.

- If control weaknesses were identified, are they situations that would be significant to your business? Has the vendor provided their management response?
- If significant, do you have the ability to directly discuss the action plan with the vendor?
- If you cannot communicate directly, do you have any avenue to provide input that may positively alter the corrective action?

Using a vendor SAS-70 cont.

- How are you going to document your risk management concerns?
- Do you have a way to monitor to see if the corrective action has been implemented and is working – or do you have to wait until the next SAS-70 report becomes available?
- If the situation is uncorrected or deteriorates, do you have contract options to exit your commitment or change vendors?



Questions / comments

- The clock says we're almost out of time for this session. If you did not get an answer, please see us at a break or lunch today.
- Thank you for attending this session and we hope you take home some good information
- Travel safely.