Banking , Enterprise Process Risk, and Apple Pies

David B Sidon CPA

Enterprise risk assessments are all the rage, and I think each definition of the word “rage” may apply (fury, frenzy, fume, fad, trend, etc). Banks subject to FDICIA compliance requirements (currently institutions with assets in excess of $1 billion) have had an early experience with enterprise risk assessment and control. Sarbanes-Oxley (SOX) brings the requirement to most of the stock banks. And the mutuals and closely-held stock banks are just starting to catch on to the fact that they, too, are struggling with enterprise risk. The struggle, however, lies in a lack of cognizance that assessing IT risk, GLBA risk, BSA risk, business continuity risk, and internal control risk, holistically amounts to an enterprise-wide risk assessment. The struggle is in addressing the pieces of the puzzle individually, rather than as a whole.

Is it ridiculous that regulators expect banks (especially small community banks) to have the resources to diligently carry out each and every one of these risk assessments? Conversations with bank management would elicit an unrestrained red-faced, vein-popping “yes!” answer, followed by an immediate search for an Advil, Zoloft, Prilosec, or blood-pressure pill, and mutterings about early-retirement looking better and better all the time. There’s a disconnect here, however. Enterprise risk can and should be “one-thing”, not a number of disparate, unconnected analyses.

I love to use analogies in my discussions, talks, and writings, and this, admittedly, may be my hokiest yet. Let’s bake an apple pie. There are some strategic decisions to be made at the outset. Should we outsource the crust? It’s always been debatable whether or not we have the expertise in house to handle the crust ourselves. Let’s assume outsource in order to simplify our analogy. Pre-heat the oven. Now peel, core and slice the apples. Oops! No apples. Off to the store we go. Forgot to shut off the oven while we went to the store – well, only a medium risk, we weren’t gone that long, but wasted energy just the same. OK, careful with that knife! Now mix sugar, flour, nutmeg, and cinnamon in a large bowl. No cinnamon in the house? Maybe we can borrow from a neighbor. We’re back. Pour mixture into a pastry-lined pie plate. Oh no! Don’t you remember we never got that pie plate returned last holiday? We’ll have to finish this later. You get the point. Baking the pie is one process which deserves planning and assurance that all the right ingredients, supplies and equipment are available for the task. The “cinnamon” process is not performed in a vacuum, it’s part of an overall venture.

Before I further connect the obvious “dots” back to enterprise-wide risk assessments vs. individualized, isolated risk analyses, let’s lay some groundwork for risk identification and the need for good procedures. Back to our pie. If you were baking with your child, you would intuitively point out the risks and hazards throughout the process; care not to leave the oven on, care not to burn yourself, care not to cut yourself with the knife, and care not to leave out a step or an ingredient. We have both safety risks and quality risks identified. Here’s another quality risk. Grandma’s apple pie was far and away the best. And what do we all complain about now that Grandma is no longer with us? She didn’t write down all of the details, making replication impossible.

Back to the business of banking. Enterprise risk analysis, done thoughtfully and thoroughly, provides us with a great map of the risks inherent in our business. With a process-centric approach that creates one table of contents delineating everything the institution does, we derive tremendous value, especially if we don't leave any of the details out. Put bluntly, you probably don't want your employees to take your procedural details to the grave with them.

But what's a process, and what's a procedure (functions vs. tasks)? Baking an apple pie is one of many processes that make up the homemaking enterprise. The recipe is the set of procedures. In a bank, we have processes such as opening new accounts, filing the Call report, transmitting wire transfers, closing a mortgage loan, re-setting employee passwords, etc, etc. And many of these processes might be broken down into a number of sub-processes. Closing a mortgage loan serves as an example. Scheduling, documentation, funding, registry filing, and rescission period timing represent some of the sub-processes involved in one mortgage closing. Procedures may easily be envisioned for each of these.

Why is parsing the process into such fine detail important in terms of an enterprise-wide risk assessment? Because that's where the risks are more easily identified. Using our mortgage loan closing example, a scheduling issue could carry reputation risk, documentation issues could carry earnings, compliance, or even interest-rate risks, filing snafus could carry earnings and credit risks, and many of the steps could represent a moment in time when non-public private information could get away from us as a GLB risk. The point here is that without a comprehensive list of processes (a complete table of contents) risks may not be thoroughly assessed, and the practice of starting from one complete table of contents to analyze all risks provides the efficiency needed to comply with today's regulatory demands.

Important to this task is an enterprise-wide standard with respect to process – sub-process – procedure definition. By way of example, following is a process, sub-process list for the process "Annual Report".

Annual Report
- → Content preparation
- → Content review
- → Content approval
- → Management approval
- → External audit review and approval
- → Legal review and approval
- → Management signatures
- → Print set-up
- → Print proof
- → Print
- → Distribution process
    - → Each sub-process would then have its own procedural steps

Note that the issuance of an annual report has very specific tasks that make up the entire function, and one might easily envision the procedural steps for each. Risks are focused on the reputational issues of providing an accurate and professional looking report; thus the many "checks" on such.

Gramm-Leach-Bliley (GLBA), information security risk assessments are terrific examples of how an enterprise-wide process-centric approach provides a more robust (and honest) look at where the risks really lie. If we use a risk-centric approach, i.e. think first about what could go wrong and then track backward to the impacted process, we severely limit our capabilities, and start baking without all the ingredients and supplies identified. Immediately and intuitively, we would identify breach points such as firewalls, sign-ons (complete with authentication issues), back-up resources, and many other e-issues. We would then move on to physical data issues such as data destruction (customer information shredded or put in bins managed by reputable vendors), equipment destruction techniques, and training relative to employees' awareness and diligence about protecting customer privacy. But what did we miss? Did we have an IT department incident response process capable of reacting quickly to situations such as the recent TJX breach? Does our lobby "customer interface" process include cognizance of where customers could see and steal information about other customers? Is there a full loan or deposit trial balance sitting on the CEO's credenza overnight? Do commercial lenders send e-mail announcements to their entire "book" without being trained on, and using the blind carbon copy function in their e-mail process? Does delinquent loan information go home to directors and sit in an unlocked file cabinet in the director's garage? I'm not sure we'll ever identify every possible scenario and don't suggest that such a goal is even practical. But, with a full listing of every process within our institution, we have a better chance of identifying the chinks in our armor.

Here's how enterprise-risk assessment, as one effort, may be deployed. Let's use the process "incoming wire transfers" as an example. Relevant sub-processes might be notification-retrieval-verification-posting-filing. Let's focus on "posting" and define such as the sub-process of crediting the customer account for the amount of the wire, debiting a fee, and posting offsetting general ledger tickets. As a visual aid, envision a spreadsheet with posting as the line item and multiple column headings representing all the possible risks. In this format, we might look at all the internal control issues and risks such as proper authorization, approval, accuracy, completeness, timeliness, segregation of duties and so on. Our single line item might be measured for risk categories such as earnings, liquidity, reputation, credit, compliance and so forth. Our focus could remain on "posting" with an eye to GLB, BSA, or business continuity risk concerns. SOX compliance would also look to this sub-process for its general ledger impact and the integrity thereof. The point here is that instead of performing isolated risk assessments for GLB, BCP, BSA, SOX, FDICIA, compliance, or internal risks, and hoping to remember to address the "posting" sub-process of the "incoming wire transfers" process, through such a methodology we can maintain some degree of confident thoroughness and a great degree of efficiency. "Hoping to remember" is not on the best-practices managerial menu.

So … how do we conclude this analogy? If the pie is poorly prepared, i.e. we miss a step or an ingredient, our customers react; it doesn't get eaten. Our household process map and decision tree place the pie into the trash process, further defined through the sub-processes: full bag to barrel in shed – trash day movement to end of driveway – vendor removal. However, the feedback is important, as our pie baking process may be improved to avoid future debacles. We've identified a weakness and are now empowered to control the quality of future efforts.

Why do we do risk assessments in the first place? The answer, of course is to identify our perceived weaknesses and strengthen our controls. High-risk designations serve as the qualifier for us. If the risk is high, we need to react with a fix or controls providing added confidence in the safe and sound continuity of the process. If the overall meal was terrific, the "pie-problem" might be forgiven by your customers. If we don't have a good sense of the totality of the overall effort, it's impossible to assess what could go wrong.

The message: do it once! Take three steps back and create a solid process list, a single table of contents. All, risk assessments, procedure manuals, even RFP details can then flow from one holistic view of the enterprise. One thorough risk assessment does the job!

This article was published in Connecticut Banking, 2nd Qtr, 2007.

David Sidon, CPA (sidon@navis-group.com) is principal of The Navis Group, a risk management consulting firm based in Gloucester, Mass., specializing in enterprise risk and business continuity planning – www.navis-group.com.