Considering “everything”

David B Sidon CPA
The Navis Group

Have you Googled an address lately using the Satellite imagery function? WOW! You can actually see the cars in the parking lot at the office building you’re traveling to. But … as a C-level executive, could you look down into your enterprise with the same sort of detailed view?

As managers, we strive to see the big picture, take the long view, guide the overall vision. But with growing pressures and requirements to take ultimate responsibility for the integrity of the entire enterprise, we’re now having trouble seeing the trees for the forest. We now have to be able to assert that we understand the role, risks and controls for every “tree”.

Sarbanes-Oxley compliance demands a control structure that identifies the risks and attendant controls for absolutely everything a business does. Gramm-Leach-Bliley compliance demands that information and identity security be considered and controlled at every business step. Enterprise risk management asks that everything be risk-assessed. Business continuity asks how you might continue everything after a disaster. And regulators examine the existence of internal controls, policies, procedures and best practices for everything. Catch the common thread? “Everything”!

The daunting task of compliance is exacerbated by the fact that the list of “everything” has been different for each compliance need such as SOX, enterprise risk management, GLB, continuity, policies, procedures, controls, etc. But it shouldn’t be. So … the “simple” part of the “difficultly simple” oxymoron is that there clearly should be one list of “everything”; one table of contents that may be used as the basis for each compliance and analytical process.

My favorite example (and inspiration for the “everything” theme) follows. Simon Winchester, in his book “*The Meaning of Everything*” chronicles the 80-year project of creating the initial Oxford English Dictionary. The project management lessons to be gleaned from a reading of Winchester’s book are elegantly simple, and beneficially applicable to our current compliance woes, particularly with respect to SOX. The concept of getting a grip on the totality of the English language back in the 19th century started with the basic premise of capturing “everything”, which over 80 years, and analogical to 21st century business processes, was/is a moving target. But, as clearly as the starting point for the creation of the world’s first complete dictionary was identifying “everything”, so too is the starting point for all of our current compliance requirements.

ERM/SOX compliance, done thoughtfully, is a tremendous exercise in analyzing best practices, and should, I suggest, have a goal of uncovering operational improvements in an attempt to more than offset the considerable cost of compliance. The approach to SOX (and “best practices” for mutual banks and credit unions) is most beneficial if it starts with a thorough and diligent identification of every business process and sub-process (functions and tasks as described in some compliance software-assist programs). The creation of the “table of contents” for ERM/SOX compliance then becomes the basis for every other compliance component, a considerable efficiency in the end. But, this is where the “difficultly” part of the oxymoron kicks in – although not rocket science, this takes time and considerable effort.

The creators of the Oxford dictionary sought to control the scope and management of the project by breaking things down into manageable pieces. Their components were somewhat obvious: a,b,c, etc. (A little trivia - Lord of the Rings author, J.R.R. Tolkien served for a while as the "W" sub-editor) The approach to a compliance table of contents is no different, with chapter headings representing the functional areas in an institution (such as Finance, Loan Servicing, Deposit Ops, etc.), and processes and sub-processes filling out the table (exploding the file structure, for you IT-types). The Oxford dictionary first identified almost 500,000 words; a financial institution may likely identify 2,000-3,000 processes and sub-processes. Yes, that's right – a few thousand.

Example, in one SOX project, I have been tasked with identifying the Corporate Governance processes and sub-processes. I am to "CORP" as Tolkien was to "W". Breaking things down into groups of corporate processes such as board functions, policies, reporting, audit, compliance, planning, stock administration, communications, risk management, executive compensation and employee benefits, I have (so far) identified some 47 processes and 225 sub-processes. From this it is easy to extrapolate the myriad of processes attached to functional areas such as branch and back-office operations. Clearly the time element in diligently identifying each process is considerable, but early efforts in the SOX arena have turned up some interesting re-definitions of where risk really lurks. How about the identity security risk posed by the failure to use the blind carbon copy function when sending a bulk e-mail? How about the realization that a major lending risk (a lost note, for example) occurs when the closed loan file moves across town via courier from the originators to the processing department? How about the disgruntled employee risk created by understaffing and overworking our IT groups? Have we created a risk environment where the IT staff could up and quit or, worse yet, stay with a subversive malicious attitude? Welcome to a realization of where your risks really lie.

So ... the message. Take a step back. Create one single table of contents. Consider "everything". As the manager of the "everything" project, demand detail. That's where the ultimate benefits lie.

This article was published in Banker & Tradesman, November 21, 2005.
This article was published by Vitex, Inc., The Alliance Newsletter, May, 2006.

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.