ASA

Annie Searle & Associates LLC

Research Note

Simpler Internal Controls

By Annie Searle

Applicable Sectors: **Banking and Finance, Information Technology, Communications, Energy**

Well-known management expert Rosabeth Moss Kanter has a new publication called "Simplicity: The Next Big Thing," [i] in which she weighs in on streamlined design, fewer products and less-complex processes for one's customers. Some companies have already adapted a Six Sigma disciplined approach, originally derived from cleaning up and "leaning out" manufacturing processes. Here, we'll take a quick look at how operational risk controls can be strengthened by working across operations or platforms that are silos, to effectively streamline and simplify the environment.

A hard look at IT platforms, policies or procedures usually finds a significant amount of layering over time. Rather than tweak the technology platform architecture when an application is added to the environment, the new application often sits inconsistently in the

production environment. In the IT world in particular, this can create a nearly unmanageable environment when the applications do not play well with one another, or use “customized” controls to allow for idiosyncrasies in the environment.

A good example of an unstreamlined environment can be seen in the disparity between the uniformity and tightness of mainframe controls and the level of controls variation on distributed systems platforms. To adequately protect consumers and customers who shop or bank on the Internet is a true controls challenge because data passes through both the mainframe and the distributed systems platform, where design must be well engineered to both protect against and anticipate threats from Internet fraudsters that have not yet materialized.

Often an audit or regulatory "finding" is a result of a disconnect. It may be related to a company's formal governance process (including policies and standards and reporting around internal controls) or it may be in how certain types of work are performed (operational processes and procedures and reporting). Sometimes a disconnect is unintentional, perhaps the result of a lack of staff training. And sometimes the control itself is so manual that it is easy to deliberately

ignore it, especially if employees are impatient with the right way to do things.

In the operational risk arena, **key internal controls** as identified by the Federal Financial Institutions Examination Council (FFIEC) include:

- Creation and safe storage of records
- Adequate segregation of duties among those responsible for the control
- Reliable MIS data with complete auditable cycles
- Efficient and effective operating procedures
- Procedures for business continuity
- Identification and monitoring of high risks with reports to executives
- Adherence to management standards and policies, applicable laws and regulations, regulatory policies and guidelines

Though this guidance is written specifically for the banking and finance sector, these areas of control are applicable to most other regulated sectors as well, such as IT, communications, and energy. As seen from the recent financial crisis, to manage risk effectively means looking at the big picture, not just narrowly at individual controls. Though he was

writing specifically about market and credit risk, the six errors identified by Rene M. Stultz in a March 2009 Harvard Business Review article[ii] are applicable to operational risk as well. All of these errors are a result of looking too narrowly at operational risk, especially if there is not a coherent and streamlined controls design at the enterprise level that looks across all of the silos to aggregate the risk(s).

Here are the six errors that Stultz identifies:

- Relying upon historical data
- Focusing on narrow measures
- Overlooking knowable risks
- Overlooking concealed risks
- Failing to communicate
- Not managing in real time

A first step that every institution can take is to examine the incongruities and unnecessary complexities in its existing control structure; and to ensure that there is a specific senior group assigned to handle enterprise risk management inside the company.

---

[i] Rosabeth Moss Kanter, "Cut Your Company's Complexity," Harvard Business Management Tip of the Day, July 7, 2009.

[ii] Rene M. Stultz, "Six Ways Companies Mismanage Risk," Harvard Business Review (Boston: March 2009) Volume 87, Number 3.