

Controls Over Complex Financial Models: Common Deficiencies

By Richard Pace

In a recent Sarbanes-Oxley webcast hosted by PwC in October 2006, almost 30 percent of industry participants indicated that complex financial models represented the highest risk of material weakness to their companies. Although three years have passed since the implementation of Sarbanes-Oxley (SOX), it is clear that control challenges still remain for companies employing complex financial models in financial reporting. In this article, we examine some of the more common control challenges in this area and offer some practical tips to improve control efficiency. In a subsequent article, we will focus more strategically on the use of a centralized model risk management program as a company-level control and offer some insights into features that can enhance the effectiveness of such programs.

Common model control deficiencies and suggested improvements

In many cases, the key controls associated with a complex financial model are not based on an effective model risk assessment

To design controls for a particular model-based financial estimate effectively, one needs an accurate understanding of all key model-related risks. However, based on our observations, this is an area where companies still have opportunities to enhance processes and improve efficiencies.

- In some cases, companies perform these risk assessments by simply applying a generic set of model risks to all models (for example, those contained in the Office of the Comptroller of the Currency's (OCC's) 2000-16 Risk Bulletin on Model Validation).

- In many cases, the risk assessments are limited to just the "black box" model and not the supporting operational processes surrounding the "black box."

Alternatively, a more effective evaluation of model risk is one that is customized to the inherent risks of each model and one that is broad enough to incorporate all supporting key model processes. To perform a customized model risk assessment, it is necessary to understand, in detail, the overall model structure, its degree of complexity and all key model processes. Accurate model documentation and associated process flows are critical to this exercise. Once one obtains this detailed level of understanding, the risk assessment should reflect the following dimensions of model-related risk.

- For some accounting purposes, numerous models may interact within a complex structure to generate the required financial estimates. The sheer number of these models, along with their interactions within the financial estimation process, increases the complexity of potential model error.
- Models based on the application of statistically-derived relationships (such as prepayment models) present a different set of risks than those that simply apply an objective formula in computing financial values (such as a discounted cash flow formula).
- Internally developed models have a different risk profile than vendor-supplied models.
- Models implemented via end-user computing applications typically have greater operational risks than models implemented via a centralized software platform.

Clearly, the risks – and, therefore, the needed controls – can vary significantly across these dimensions.

From an operational perspective, the model risk assessment needs to cover more than just the "black box"; ideally, it would cover all three of the following key model operational stages.

- Data pre-processing stage – In this stage, there is likely both manual data collection as well as

automated data extraction from internal and external data sources. Raw data is then combined, converted and reformatted into model-specific variables that feed the “black box.” The data pre-processing stage is likely operationalized through one or more SAS programs, Access databases, SQL queries or other software applications.

- Model processing stage – In this stage, the model “black box” processes the data from the previous stage-along with other assumptions/inputs-and produces the model output.
- Data post-processing stage – In this stage, there is likely automated data processing of the “black box” model output that is operationalized through one or more SAS programs, Access databases, Excel workbooks or other software applications. The final financial estimates are then output to a specific file format or uploaded to a data warehouse for use by the company’s finance/accounting function.

Once again, the complexity of these operational stages will differ across models and, therefore, will contribute to the unique risk profile of each model. Furthermore, in our experience, critical errors are just as likely to occur in the data pre-processing and post-processing stages as they are to occur in the “black box” itself. However, given the primary focus that is typically placed on the “black box,” these errors may go undetected for extended periods due to insufficient controls in these ancillary stages.

Companies may be exposed to significant key person risk and, potentially, fraud risk due to insufficient controls associated with model documentation

While many companies have policies requiring model documentation, most of these policies lack specificity or specific standards to ensure their effectiveness. As a result:

- Departures of key employees can significantly compromise the company’s ability to execute its critical financial models, effectively maintain these models and train new employees on these models.
- There may be no official standard to which one can compare existing model specifications in order to

determine whether errors or unauthorized model changes have been made.

- There frequently is a lack of transparency – particularly to the finance/accounting function – associated with the underlying theory and approach behind the model estimates.

Companies may improve the effectiveness of this control by reviewing their model documentation policies to ensure there are specific requirements/standards and there is specific accountability for maintaining the documentation in a complete, accurate and secure manner. Some features model documentation policies include are:

- A nontechnical, management-level overview of the model theory and approach
- Key features of the model development process and the model production application that are required to be documented
- Important model limitations and considerations
- Key model sensitivities
- Requirements to document the operational processes associated with the model production application
- Requirements to clearly document computer code, spreadsheets, Access databases and other model-related software
- Requirements to document all data inputs used by the model – including the source of each input, its format, how to interpret its values (if it is coded), how it is calculated and any data scrubbing rules applied

Insufficient control procedures associated with desktop application-based models – such as Excel and Access – may expose the company to model risk due to manual processing errors

Based on our observations, reliance on desktop applications to implement complex financial models creates significant operational risks and associated control costs due to the following:

- The numerous manual processing steps and data hand-offs – such as manual query executions (Access), the need to manually update hard-coded

cell references (Excel), the use of pivot tables (Excel) and the frequent copying and pasting of data between applications:

- In Excel, the potential lack of computational integrity if the same formula is not completely and accurately copied and pasted to the correct range of cells, as well as the lack of transparency associated with the underlying calculations.
- In Access, the lack of any automated error detection processing, such as a processing “log file” that indicates the number of records processed and any errors or other anomalies encountered during model processing.

Companies may wish to consider enhancing the effectiveness of their model controls by implementing a “sunset” policy for all material financial models that rely on desktop applications. Such models could be migrated to a more robust platform that is automated and subject to centralized IT general controls – including security access, change management and version controls. While such a migration is not required, companies may find that such a policy yields significant mitigation to the operational risks noted above – as well as a significant reduction in control costs.

Insufficient model change management controls may also lead to model risk

Regardless of whether a model is implemented via desktop applications or via a centralized software platform, we continue to observe control deficiencies related to the following areas:

- Disclosure and tracking of all model changes
- Sufficient pre-implementation testing of approved model changes – such as user acceptance testing and regression testing
- Consistent quantification of financial impacts of model changes
- Affirmative evidence that no unauthorized changes have occurred to model applications (particularly models implemented via desktop applications such as Excel and Access)

- Segregation of development and production versions of model applications

In addition to strengthening the IT general controls environment surrounding key financial models, companies can leverage certain technology tools to enhance model change management controls by:

- Creating a suite of test cases with known results that can be run through a model prior to the official production run as an affirmative test of the integrity of the model code and calculations.
- Using certain software utilities that can detect and show changes to computer files. For example:
 - A file comparison utility can be used to detect changes to computer program source code since the previous production run. These changes can then be reconciled to the company’s model change management log to detect unauthorized changes.
 - A file comparison utility, such as an MD5 checksum program, can be used to generate digital fingerprints of computer files at regular time intervals (such as monthly or quarterly). These digital fingerprints can then be compared between time intervals to determine whether any changes have occurred to critical files.

While significant progress has been made in this area by many companies, there still exists a great opportunity to enhance model control structures, reduce risk and generate efficiencies. From a more strategic perspective, a formal enterprise-wide model risk management function can provide additional benefits, and we will explore this topic further in a subsequent article.

For more information on controls over complex financial models, please contact:

Richard R. Pace
ric.pace@us.pwc.com
703-918-1385

This document is provided by PricewaterhouseCoopers LLP for general guidance only, and does not constitute the provision of legal advice, accounting services, investment advice, written tax advice under Circular 230 or professional advice of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisers. Before making any decision or taking any action, you should consult with a professional adviser who has been provided with all pertinent facts relevant to your particular situation. The information is provided “as is” with no assurance or guarantee of completeness, accuracy, or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties or performance, merchantability, and fitness for a particular purpose.