AuditOne LLC

Risk-Managed Internal Audit and Credit Review Expertise

NEWS

AuditOne Compliance Advisory: Model Validations and Related Exercises

AuditOne, LLC April 21, 2017

AuditOne Advisory

From Bud Genovese, Chairman

Model validations to meet model risk management and governance requirements are clarified in this reprint of WIB's April 2017 Compliance Digest article written by Jeremy Taylor, Co-CEO, AuditOne LLC. Please feel free to forward it to the appropriate people in your financial institution. Thank you. -Bud

Model Validations and Related Exercises

Jeremy Taylor, Co-CEO, AuditOne LLC
The last 2 – 3 years have seen a burst of emphasis on ensuring a disciplined process for financial institutions' (FIs') management of model risk, in accordance with OCC Bulletin 2011-12 (which superseded 2000-16) and FRB SR 11-07. Neither the FDIC nor the NCUA have issued similar formal guidance, but they have signaled their concurrence in other documents (e.g., the Winter 2005 issue of the FDIC's *Supervisory Insights*). This emphasis has come, not surprisingly, in response to FIs' growing reliance on models, whether purchased or developed in-house, for a wide range of risk management and other purposes. While community banks are typically less model-reliant, there are still expectations that they adopt appropriate governance and controls for their models, examples of which are cited below.

While the OCC and FRB documents address all the required elements of model governance, what has become evident is some confusion among model users over terminology and over the particular requirements for verifying satisfactory model performance. Specifically, we see frequent failure to distinguish clearly between what each of the following is intended to do and when/where it may be needed:

- Validation
- Certification
- Audit

- Independent review
- Service Organization Controls report (SOC 1/SSAE 16 and/or SOC 2)

This blurring in terminology can in turn translate into either gaps in required documenting or, perhaps, overkill. The resulting confusion can easily carry over into an FI's dialogue with its regulators and auditors as well.

The OCC and FRB guidance clearly states that: "All model components, including input, processing, and reporting, should be subject to validation." But who is to do this and how? For purchased models, it is critical to recognize that the structure, features and core functionality are common to all users; it therefore makes sense for the model vendor to arrange for a validation report to be prepared independently (e.g., by a consulting firm with specialized expertise in that area), to be made available to all users. This makes more sense than every user going out and independently commissioning such a report. Its purpose is essentially to answer the question, "Does the model do what it says it does?" Such a report will attest to those validation concerns relevant to all users, which takes in a model's logical structure; the underlying math, finance, statistics, etc.; their translation into algorithms and coding; the reliability of those calculations; the reporting options available; alternative/competing models and approaches; etc.

So why, then, the need for audit? Because it is important to recognize that this list of validation concerns is only a partial list. There is another, quite different, set of concerns that an off-the-shelf validation report will not touch: the user-specific concerns. Is the model appropriate for the user and has it been set up properly? This is where an auditor will focus, taking the validation report as a starting point (including verification that any issues identified in the report have been following up on by the user). The audit will then address such critical issues as:

- Is the model appropriate for the FI's needs?
- Have the data feeds been set up correctly?
- Are there controls to ensure continuing data input integrity?
- Are the assumptions reasonable and properly supported?
- Is the model producing results that make sense, verified by back-test?

Unfortunately, the audit exercise described above is often referred to as a "validation." It also sometimes gets called (e.g., in the 1996 *Joint Policy Statement on Interest Rate Risk*) an "independent review." Let's call just call it an *audit*, and the first exercise discussed above a *certification*. Again, this distinction only becomes necessary for purchased models; in-house models won't have the same bifurcation.
For most of the vendor models that our firm encounters – such as for IRR simulations, AML suspicious activity monitoring, ALLL general reserve requirements – independent model certifications are indeed typically available. To throw in another wrinkle, there are situations where an outside vendor may also need to consider obtaining and making

available a Service Organization Controls (SOC) 1 and/or SOC 2 report. This will come into play where the vendor is not just offering usage of a model but also an outsourced service to take its client's (e.g., a bank's) data, run it through the model, and produce reporting to send to the user. In those cases, the vendor's internal controls relevant to defined principles – security, availability, processing integrity, confidentiality and privacy – become a separate concern that a model certification report may address only in part.

A SOC 1 is performed in accordance with Statement on Standards for Attestation Engagements (SSAE) 16 and is needed when the output relates directly to the financial statements of a client; the ALLL is a good example. A SOC 2 is broader in its assessment of controls and does not have the financial statement focus. It was created in response to technology entities such as data centers and cloud-based systems to create an audit that would assess the effectiveness of their controls according to the defined principles listed above, applied across all functional areas and not just those related to financial reporting. For this reason, some service organizations have both a SOC 1/SSAE 16 and a SOC 2 performed to satisfy different audiences. The clients of the service provider may need the SOC 1/SSAE 16 for their financial accountants while providing the SOC 2 to the information security officer of the client firm.

Whatever label we apply to these different types of exercise with their different goals and audiences, what is clear is regulators' growing focus on ensuring a systematic and comprehensive approach to addressing the relevant concerns.

Published in Western Independent Bankers Association's Compliance Digest, Issue 23 – April 2017.

AuditOne has been audited for compliance with the QAR requirements of the Institute for Internal Auditors (IIA).

AuditOne, LLC | LinkedIn

Address:
6131 Orangethorpe Avenue, Suite 470
Buena Park, CA 90620

Phone: 562.802.3581