

## **On Compliance: Holistic Vendor Risk Management**

***Your credit union will reap benefits from considering third-party oversight, business continuity and information security risks at the same time.***

By Kris Buckley

*May 28, 2009*

*CUES' Credit Union Management's Web-only "On Compliance" column runs the fourth Thursday of every month.*

A serious dilemma for credit unions is how to streamline the myriad questions, risk assessments, monitoring and documentation required under federal regulations for third-party vendor oversight.

Taking a holistic approach, actionable on a daily basis, is the optimal way to manage existing and future regulatory requirements and follow industry best practices. When we work with a credit union, we consider together third-party vendor oversight, business continuity, and information security. Working on each area of compliance at the same time as the others means you can sometimes find efficiencies in your efforts to secure member data and mitigate technological risks to your credit union's business.

Streamlining vendor management programs will eliminate duplication when considering each of the three areas. A credit union needs to create a change control process that requires staff to do risk assessments when it adds a new vendor, starts offering a new product, renews a vendor contract, or upgrades or revises a product. While CUs are required to do an annual review of all their vendors, doing so provides minimal protection from the ever-changing technological and economic risks it faces. Doing a risk assessment on each of the key events listed above keeps the credit union up to date.

The initial challenge for credit unions is performing an initial risk assessment to create a baseline of vendors and all of their associated business processes. The number of processes a credit union will have depends on its size and complexity. The credit union's existing business continuity or disaster recovery plans may help create a partial list of business processes. To ensure a complete list of business processes is generated, both managers and employees involved in daily operations must be included in the effort to create the list. By identifying all the business processes, the credit union avoids the frequent trend whereby management stops doing third-party risk assessments after assessing the most critical business processes and does an incomplete risk assessment. For example, when looking at the credit union's data processor, the primary system risks may be included in SAS70, a statement on accounting standard maintained by the American Institute of Certified Public Accountants, but such business processes as statement processing and credit bureau reporting may be missing and have associated risks.

Before a business process list is complete, each business process and its potential risk must be evaluated under three initial risk categories: the level of nonpublic information shared, impact on the credit union if the service is lost or interrupted, and the financial risk posed by the process. These three categories of risk are by no means the sole areas of consideration, but provide a means for rating each vendor on how critical it is to the credit union's ongoing operations. The credit union will assign a risk rating of high, medium or low for each of the three initial risk categories regarding the level of nonpublic information shared, impact on the credit union if the service is lost or interrupted, and the financial risk posed by the process. If the credit union assigns the risk rating as a medium or high, a comprehensive product risk assessment for each related business process should be considered. Such an assessment includes a series of questions-such as what new servers might be required to support a product-that pertain specifically to the controls over member data.

It is the credit union's responsibility to define the parameters for the risk ratings of high, medium and low. An example of such a parameter may include defining vendors with business processes involving any level of membership data with a high non-public information risk rating due to the current risks surrounding a security breach and/or loss of membership data.

Following the assignment of the risk rating for the three initial risk categories, the vendor's initial risk rating of high, medium or low can be assigned. The assignment of the preliminary oversight criticality rating will consider the three initial risk ratings and other considerations unique to the vendor, such as accounting, lending, security or staffing concerns.

The credit union's next step is to prepare to perform further comprehensive risk assessments. The risk assessment questionnaire is provided in [NCUA 08-CU-09](#). A credit union should review each question to determine its applicability to a specific vendor relationship. Upon completion of the vendor risk assessments, the credit union has a comprehensive list of vendors, their associated oversight criticality, and related business processes.

The defined triggers for doing a risk assessment (e.g. new product, new vendor, etc.) provide management with an effective change control process that encompasses vendor oversight, business continuity and information security. During the initial risk assessment process, the credit union collects critical information on the vendors and related business processes. This information can be incorporated into the existing business continuity and information security programs. In addition, upon any of the five defined triggers, the credit union can review the three programs at the vendor and business process levels using the risk assessment process. The change control process must clearly define each employee's responsibilities under the vendor oversight program for submitting, reviewing and approving the vendor risk assessments under each of the five defined triggers.

The implementation of this methodology requires management's commitment and the allocation of resources for the initial and ongoing development of the program. Long term, implementation of this methodology ensures the credit union has an effective means to plan, monitor, react and revise related policies and procedures-such as disaster recovery-effectively and efficiently across the credit union. It ensures the credit union is prepared to respond to a vendor or member incident, natural disaster or security risk on any given day, not just at the time of annual review.

**[Kris Buckley](#)** is president of [Buckley Technology Group](#), Norwell, Mass., which offers professional services and software products for business continuity, information security and vendor management. Reach Kris at 781.258.0618.