

Executive intelligence on credit union exams, enforcement and risk management

Should CAMEL Ratings Stay Secret?

It is an article of faith and law: CAMEL ratings, and the examination reports that underlie them, are strictly confidential. They're for the eyes of regulators and the regulated only. NCUA rules explicitly prohibit the release of the information to the public. And the agency takes the mandate seriously. Witness the internal investigation NCUA chairman Debbie Matz ordered up earlier this month into who leaked CAMEL and other confidential information about a CU headed by NCUA board nominee Carla Decker.

Yet, at a time when private ratings organizations do a decent job of mimicking CAMEL ratings, and when there is growing pressure on institutions to be more transparent with their customers and owners,

a case can be made that the secrecy that shrouds the ratings is starting to outlive its usefulness and may even be counterproductive.

State Employees Credit Union (\$23.4 billion), Raleigh, N.C., for one, is trying to make that case. It recently got approval from the North Carolina Credit Union Division to begin publishing the CAMEL rating it receives from its state regulator. Officials see the disclosure as a step in the direction of greater accountability to its members and enhanced corporate governance, not to mention a neat marketing trick.

"We feel the more the public knows about us, and hopefully about others, the better," says Jim Blaine, president and CEO of SECU, the nation's second-largest CU, in an interview.

As an FISCU, which is also exam-

(Continued on p. 2)

OIG Criticizes NCUA Data Security

The NCUA has been holding credit unions' collective feet to the fire when it comes to enhancing information security, on the Internet and otherwise. But a recent report by its inspector general suggests that the agency's own security management efforts leave something to be desired.

The November 10 report examines the NCUA information systems and security program and controls for compliance with the Federal Information Security Management Act, a 2002 law that lays out a framework

(Continued on p. 6)

How Should CROs Function at Smaller Financial Institutions?

Risk management, we all know, should be tailored to the size and complexity of your business. But how much risk management is enough? Who should be responsible – and responsible to whom? At a growing institution, that can be more art than science. It can also be expensive: Chief risk officers are valuable and costly commodities.

Banks and CUs should also view risk management and structure as an

active and evolving process, experts say. Certainly, with regulators expecting you to stay on top of an ever growing array of risks – not the least of which are regulators' own expectations and enforcement actions – you ignore this area at your peril.

As a kind of road map, Eric Holmquist, president of Holmquist Advisory LLC, Spring House, Pa., offers up distinct risk-management models for small and large organizations. Each has a Chief Risk Officer, and

each helps design a risk-management structure for the organization. But that is where the similarities end.

CROs in smaller organizations will be much more hands-on, Holmquist says. They conduct risk assessments, and act in an advisory capacity on risk to business units. They typically are part of the management team and report to the CEO.

The role of the CRO becomes more formalized and removed from daily

(Continued on p. 4)

(Secret, continued from p. 1)

ined by the NCUA, State Employees is still prohibited from publicizing the CAMEL rating it receives from federal examiners, even if it is the same as the grade from the state.

This summer, the NCUA instituted a new policy of sharing its CAMEL ratings with state-chartered institutions that it examines, although the non-disclosure requirement remains. Blaine says he thinks both the state and federal ratings should be made public – although signals from the NCUA are such that he should not hold his breath. “I don’t think they are too happy with me,” he says.

CAMEL ratings have been under wraps ever since the five-pronged ratings system was adopted by financial regulators in the 1970s. Officially, they are the property of the NCUA or the FDIC, shared with CUs and banks, on the condition that they remain confidential between the parties. The acronym stands for the five components on which institutions are judged: capital adequacy, asset quality, management capability, the quality and level of earnings and adequacy of liquidity. The banking agencies added an “S” in 1996 for “sensitivity to market risk.”

Courts have also long held NCUA examination reports exempt from release under the Freedom of Information Act to protect the security of financial institutions and to promote cooperation and communication between agency employees and examiners. Everyone from insurers looking to underwrite risks to private investors has sought versions of the ratings over the years to no avail.

To outsiders, the ratings have become a yardstick for measuring financial strength, although regulators say they are really an internal tool for examiners and managers to determine what kind of remedial actions a bank

or CU needs. The higher the score, the higher the regulatory scrutiny becomes.

SECU, Blaine says, got a “2” from its state regulator. “We have always been a ‘2,’” he says, adding that a “1” would require the CU to add more capital, at the expense of members’ pocketbooks. “We feel we are safe enough,” he says.

Under the current system, the thinking goes, under-performing institutions get a chance to work out their problems without the glare of publicity. Even since the advent of deposit insurance, there remains concern that unauthorized disclosures of bank or CU examination reports could spur a run on deposits and de-stabilize an institution earnestly trying to put its house in order.

“Any release of a credit union’s examination results could compromise the credit union’s safety and soundness, which is why such release is illegal,” says NCUA spokesman David Small, adding that plenty of financial data about individual CUs is available to the public on the NCUA web site.

Blaine says the lack of disclosure is at odds with growing demands from the likes of the Consumer Protection Financial Board, which wants to make financial institutions more transparent and consumer friendly. Suppressing information seems out of touch in an age of Wiki Leaks. His view: Put the truth out there, get over it, and move on.

The proliferation of private ratings organizations is also a factor. “There are ... businesses that guess at these kinds of ratings. We thought instead of having anybody guessing, why not just release it,” he says.

Perhaps most important is the cooperative structure of CUs, which he says is anathema to the lack of disclosure. “Why aren’t you going to tell a member of a member-owned cooperative

what the score is?” he says. “It is different than a bank. Each member of a credit union is an individual owner.”

The reaction to its ground-breaking move has so far been muted. Most members have been doing business with the CU for years, and have deposits within the federal insurance limit. “They are local. They know us,” he says. “They don’t care if we are a ‘1’ or ‘2’ or ‘3’ or ‘10.’”

Beyond the transcendent goals, he acknowledges, the disclosures could also be good for business. “If everybody could make a logical and fair and reasoned comparison, and it is not all warm and fuzzy for us, we think people would come here to do business with us,” he says.

While federal regulators are staunchly opposed, state-chartered institutions like SECU may become a laboratory for CAMEL disclosures.

State laws governing such disclosures are more flexible than those at the federal level. Blaine says he has heard from a number of others who are interested in following his lead.

“We have heard from a couple of West Coast and a couple from Middle America,” Blaine says, some with even higher ratings. (“I did not get any calls from ‘5’s,” he says.)

Among the defenders of the status quo are the ratings agencies which have developed a lucrative niche business around publishing their own private ratings.

Disclosing the information, they say, could make bankers and CU managers more sensitive to changes in ratings and make the examination process less open to forthright sharing of information and thus less productive.

Keeping the information nonpublic, they say, improves the odds that a troubled institution will recover.

“They can disclose issues without fear of the public becoming aware of things that probably management can fix given an opportunity. If that is shared before there is a chance to act that would undermine the very thing they are trying to do.” says Gene Kirsch, senior banking analyst, Weiss Ratings, Jupiter, Fla.

Even if CAMEL ratings were to be made public, Kirsch says he thinks there would still be a market and need for private ratings as an independent check. “I would think that the public would want another opinion independent of the government ... in light of what has happened over the last three years,” he says.

Blaine argues that releasing CAMEL information could have a disciplining effect on risk taking. CU managers might take regulatory advice more seriously, he says, if they knew information about their exploits and activities were to become public. But he acknowledges some drawback with such a system. If all the healthy CUs were disclosing their ratings, it would back troubled institutions into a corner.

The sometimes fickle and unpredictable nature of the examination process may also militate against disclosure. Regulators have sought to be more consistent in how they evaluate the safety and soundness of banks and CUs in recent years. But the ratings are still viewed among many observers as highly subjective, and potentially misleading.

In a report earlier this year, the NCUA was scored by its inspector general for giving high ratings to 74 failing CUs that were closed or merged from 2008 to 2010. If published, those overly rosy outlooks could have had the perverse effect of luring new depositors and customers to institutions just as they were about to fold.

“It feels like public information to me. But it feels like dangerous public information to me,” Dave Sidon, principal with The Navis Group, Gloucester, Mass., says of the CAMEL debate. “It is so subjective and so much is in the eye of the beholder.”

He recalls the case of a two-bank holding company client being examined for Y2K preparedness. The banks had the same documentation, but one was examined by the OCC, the other by the FDIC.

“One regulatory body came in and said, ‘You guys are doing a Cracker Jack job. Can we have copies to make templates for other banks? Keep up the great work,’” Sidon recalls. “The other regulatory body came in, and said, ‘This is horrible. We are going to put you under a memorandum of understanding. You just don’t get it, do you?’”

“Frankly, neither of them was right,” Sidon says.

The debate over disclosing CAMEL ratings was fueled by a recent report in *Credit Union Times* that the credit union that Decker headed, District Government Employees FCU (\$45 million), Washington, D.C., received a CAMEL rating of “3” and was considered a “high strategic risk.” The *CU Times* article was based on examination reports and other documents the publication had obtained.

In the wake of the disclosure, NCUA Chairman Matz asked the NCUA inspector general to investigate and determine the source of the leak. She implied in a statement that she believed it came from the credit union’s board or management.

Decker’s credit union, which has 10,900 members, reported a profit of \$71,762, in the first nine months of 2011, following four years of losses

(Continued on p. 4)

MISSION:

The *Safety & Soundness Report*, the independent eyes and ears of the credit-union movement, provides executive intelligence on CU exams, enforcement and risk management.

EDITORIAL:

Need us to investigate a topic? Want to express your opinion? Please call or e-mail us.

Editor:

Aaron Steinberg
800-929-4824 ext 2471
asteinberg@cusafety.com

Group Publisher:

Hugh Kennedy
800-929-4824 ext 2213
hkennedy@ucg.com

SUBSCRIPTIONS:

Direct questions about newsletter delivery and account status to

Tel. 1-866-236-6228;
Fax 301-287-2945;
or send an **e-mail** to
Customer@cusafety.com.

EDITORIAL CONCERNS:

Our goal is to provide you with the most accurate and balanced information available anywhere. If you ever feel we’re not living up to this standard, I want to know about it. Please call me, Hugh Kennedy, Group Publisher, direct at 1-800-929-4824 ext. 2213.

DON'T WAIT!

Register today for the 35th Annual National Directors’ Convention – July 31-August 3, 2012, in Las Vegas!

Go to www.cudirectors.com or call 866-620-5937 to guarantee your seats.

ADDRESS:

The Safety & Soundness Report
Two Washingtonian Center
9737 Washingtonian Blvd., Ste. 100
Gaithersburg, MD 20878-7364

(Secret, continued from p. 3)

dating to 2007. At Sept. 30, it was considered well-capitalized, with a net worth ratio of 10.48%

According to *CU Times*, the examination report noted that the credit union had un-reconciled ATM and ACH accounts going back to 2002 totaling \$734,235, and said the CU would have to write off the accounts if they were not recovered by the first

quarter of 2011.

Last December, the NCUA and the credit union signed a letter of understanding and agreement setting certain goals for return on average assets for 2011 and mandating certain reductions in operating expenses and other management and financial changes, *CU Times* reported.

The document also required the

credit union's board to send monthly progress reports to the NCUA that include board minutes, monthly financial statements, a summary of delinquent loans by category and the methodology sheet for calculating allowance for loan and lease losses. The credit union exceeded the targeted return on average assets for the first three quarters of 2011, *CU Times* reported. ▲

(CROs, continued from p. 1)

program management as organizations grow. At the largest institutions – those with, say, more than \$30 billion in assets -- the CRO assumes a more corporate role with risk managers embedded within business units. He becomes independent of management and reports to a board-level risk committee.

Most banks and CUs do not fit neatly into either scenario, Holmquist acknowledges. “There is an infinite number of permutations and each organization will need to decide how best to design their risk governance structure,” he says.

There is lots of pressure, too, especially from regulators.

“Certainly the expectations are increasing with every month that goes by,” says Marcus Faust, senior vice president, RP Financial, Arlington. “(Regulators) are increasingly expecting smaller and smaller companies to do something around enterprise risk.”

Newly proposed guidelines requiring small banks to conduct capital stress testing, he says, pre-suppose an understanding of enterprise risk. “There is no question that the size threshold for the expectations is decreasing,” Faust says.

“Everyone is struggling with these questions,” says Dave Sidon, principal of The Navis Group, Gloucester,

Mass. “What is the evolution of the delegation of the functions from the CEO to a hierarchy as the bank or CU grows?”

Dozens of regulator-driven policies and procedures are driving demand for more risk analysis, and financial institutions are finding it harder and harder to keep up.

“I have seen more and more banks over the last couple of years that are just plain missing things,” he says. “I think it is getting harder and harder for bank presidents and boards to make sure they have captured the totality” of what regulators want.

Risk management in a small bank or CU is obviously much different than in a giant institution. The smallest CUs and banks probably do not have a designated CRO. Those duties are absorbed de facto by the CEO or by some other top executive.

Many managers understand the basic concepts of enterprise risk management and perhaps even the benefits of thinking holistically. But they don't have the luxury of a budget to afford a qualified and experienced CRO. Others struggle where to start.

But the trend towards more is undeniable. “It used to be only the biggest international and national financial institutions that were doing

much in the way of true enterprise risk level management activity and really had the systematic processes in place,” says Tony Ferris, an ERM consultant and partner with The Rochdale, Group, Overland Park, Kan. “Now, I would say there is very little cause for any financial institution to not have some sort of organizational risk management and have those capabilities in place.”

Smaller institutions, he says, may be among the most vulnerable and have the most to lose. “Their opportunity for error is even smaller than some bigger organizations,” he says. “They do not have the capital levels and the management breadth to spend time on those activities.”

“It is a work in progress,” he says. “It depends on the skill sets they have been able to acquire. The CRO types are pretty far and few between.” Automated support tools may offer a fairly low-cost solution for smaller institutions to facilitate the process, he adds.

A frequent solution, assigning risk-management duties to someone who retains operational responsibilities, can also be a problematic one, Holmquist and other experts say.

Conflict of interest issues inevitably arise when duties are split. You lose credibility as a risk expert in the eyes of senior management or board members.

“You cannot serve two masters. If you are the CFO and the CRO are you going to blow the whistle if there is financial risk in your world?” Holmquist asks. “Are you a steward for the risk program or a day-to-day manager?”

The problem often arises in institutions with assets of between \$500 million and \$1 billion who recognize the need for better risk management but who are also constrained by budgetary or personnel issues. It is unusual for such sized institutions to have a designated CRO that is not wearing multiple hats, such as that of the internal auditor or chief credit officer.

Both approaches are problematic, Faust says. Vesting an auditor with risk-management duties, especially one without broader banking experience or a track record as a strategic thinker, “tends to drive the focus of the whole enterprise risk management into a type of internal control exercise,” he says. “Enterprise risk is intended to be more forward looking, at a strategic level.”

Similarly, a chief credit officer put in charge of risk-management will tend to focus on credit-related risks because that is within his comfort zone. Better to give him a lieutenant or two who focuses solely on the credit side to free up time to take a broader of organizational risk. In that scenario, “Credit becomes just one of all the risk areas he has to manage,” Faust says. “He has to come out of the trees to look at the forest.”

For someone steeped in an area other than risk analysis, that new role can also be a cultural challenge. Sidon knows a former police officer who is now a financial institution CRO and who analogizes his new job to the cop on the beat who is re-assigned to run internal affairs. “You have to disavow all of your friendships and cut yourself off,” Sidon says the former

cope observed. “You could be investigating whistleblowers or calling people on the carpet who used to be your partners or friends.” While ending relationships is extreme and probably unnecessary for most bank or CU risk officers, the idea of independence is a worthwhile ideal, he says.

The CRO can also have too much influence, which is a problem. A common pitfall is that the CRO becomes the ultimate decision-maker on whether to proceed with a product or service or new venture because he has analyzed the risk.

Smaller institutions, he says, may be among the most vulnerable and have the most to lose.

CRO-prepared risk reports certainly can be powerful tools if circulated widely within management. But the ultimate decisions should remain with the business unit managers.

You do not want a risk expert making the final call on a lending program or a new mobile banking gizmo. Indeed, some high-risk opportunities may be well worth pursuing, while some less-risky ones may not be worth the trouble.

“The decision on whether the risk is acceptable or not, that has to stay with the business side. The CRO can be a voice in the conversation but the business areas must own the risk,” Holmquist says. “You have to be very careful they retain that advisory role.”

“The purpose of it is for decisions to be made understanding full well what the entire scope of risk is. It


is not to be risk free or risk averse,” says Jeannie DeCarlo, senior vice president, operations, and chief risk officer, USE Credit Union (\$724 million), San Diego, Calif.

USE could be a model of sorts for the enlightened, mid-sized, risk-conscious CU. DeCarlo is part of the senior management team and reports to the CEO. She also makes periodic risk presentations to the board.

A hands-on manager, she does risk analysis for new products and services the CU is proposing to roll out. But credit risk is owned by the lending unit and reputation risk is the bastion of retail and marketing.

Lately, the CU has been examining new participation lending programs as a way of generating revenue. DeCarlo did her typical comprehensive risk analysis, and then sent the findings to her lending group for review. “That overall risk assessment becomes part of the process,” she says. “It does not mean if it is high risk we don’t do it. It means that we know it.” One program was rejected because its prospective partner did not have a long enough track record, which made it difficult to measure potential losses.

The current structure, she says, serves the CU well. The idea of having a board-level committee strikes her as overkill and potentially counterproductive.

“It sounds like a structure where the board wants to watchdog the executive team. I don’t see us going into that direction,” she says. “The board hires the executive team to have the right processes and procedures and structures in place to carry out the desire of the board. The watchdog is your yearly financial statement audit. The watchdog is your internal audit people. If you need more watch-dogging than that I wonder why you have your executive team in the first place.” 

(Security, continued from p. 1)

for annual information technology security reviews for federal agencies.

The report by the NCUA internal watchdog says the agency has made progress. But it also scores the agency for a half-dozen problems, including “deficiencies” that have persisted for more than a year.

Among the findings:

- NCUA only requires one-factor authentication for remote access to its network, putting its systems at risk of unauthorized exposure that could threaten its reputation and pose “a serious adverse effect on organizational operations, assets or individuals,” the report said.


- NCUA needs to improve its continuous monitoring program.

“Specifically, the agency does not have documented continuous monitoring policies and procedures and has not fully integrated the various components of its information security program into a strategy that facilitates near real time monitoring and risk management,” the report found.

- NCUA needs to improve its security authorizations. The report said the security plan for the agency’s Asset Management and Assistance Center does not address each of the minimum security controls for the system’s security categorizations. The report also said that the agency needs to improve its contingency planning for the AMAC system, which has not been tested in a year.

- NCUA needs to improve its in-

trusion detection policies and procedures. The agency has implemented in-house intrusion detection and developed intrusion detection policies and procedures. But the report found that its policies and procedures “do not include response times for addressing vulnerabilities,” and that the agency “does not have a means to monitor the remediation of vulnerabilities through completion.”

NCUA officials, in response, said they were working on addressing the concerns. The agency said it had delayed transitioning from a single-factor authentication for remote network access because of logistical and financial concerns. But it said it would implement two-factor authentication at the national conference. 

Concentration Risk: A Guide for Directors

**This is a must-have guide for
all credit union board members!**

ORDER TODAY! www.cusafety.com • 866-236-6228

The **Safety & Soundness Report** is published weekly (48 times a year). Copyright 2011. Price \$595/yr. To receive photocopying or electronic distribution permission, call 866-236-6228 and ask about our copyright waiver programs. Or e-mail asteinberg@ucg.com. WARNING: copyright violations will be prosecuted. The **Safety & Soundness Report** shares 10 percent of net proceeds of settlement of jury award with individuals who provide essential evidence of illegal photocopying or electronic distribution. To report violations, contact: Roger Klein, Esq., Howery LLP, 1299 Pennsylvania Ave., NW, Washington, DC 20004-2402. Confidential Line: 202-383-6846.