

On Compliance: From a Business Continuity ‘Heretic’
January 2011 – Vol: 34 No. 1
by Kenneth Schroeder, CBCP

What does your credit union really need to get started?

January 27, 2011

Credit Union Management magazine’s Web-only “On Compliance” column runs the fourth Thursday of each month.

Here’s my confession: I’m a business continuity heretic. I’m apt to be burned at the stake. But before I go up in smoke, I want to give you my message: “Business continuity is easy.”

That’s it? Yup! Here’s why that statement brands me as the heretic. We in the credit union industry get mired in the minutia—and the National Credit Union Administration or state examiners only complicate the issue by focusing on the minutia. Using Federal Financial Institutions Examination Council [guidelines](#) to inspect your credit union’s business continuity plan, they find all sorts of requirements to use to beat you up. We in the business continuity profession get in the way as well, insisting that all the procedures, tools, and processes must be in place to have a viable plan. That list includes:

- risk assessment,
- business impact analysis,
- planning strategies,
- documentation,
- gap analysis,
- testing and
- business continuity lifecycle.

So where does the heretic angle come into play? I’m branded as the heretic, because I say that entire list can wait. I’ll go against all the professional standards in the business continuity industry. I’ll stand up to the FFIEC guidelines. Yes, I’ll even confront your examiners. You see, I think we can clarify the process by asking, “What does that credit union *really* need to put in place to get started?” Here’s my recommendation:

Begin by asking yourself, “What’s more important: getting started with some degree of survivability, or filling all the squares to pass the exam?” I say, “Let your survival instincts prevail. We’ll get the rest later.” (See, I told you so! Heresy!) So, let’s take a couple of minutes and apply some old-fashioned common sense to the issue.

From my experience, in the typical small credit union of fewer than 50 employees, business continuity probably evolves from a short blurb in a planning meeting where someone (usually the CEO) says, “Well, who’s in charge of our business continuity plan?” following which, everyone gives the infamous two-shoulder shrug, following which the CEO delegates the task to either the junior IT person or the compliance person, and they all move on to the next topic. Right or wrong, it happens, and we have to live with the reality of it.

Our stalwart, dedicated hero scurries to an industry Web site for help and, finding none, picks up the latest copy of *Disaster Recovery Journal* magazine, reads some article that applies second order differential equations to a risk assessment model, throws up his hands in disgust, makes sure that IT makes back-up tapes, and calls it a day.

My mantra is: “Business continuity planning is simple!” When all is said and done, you can build a basic foundation by considering your mission statement and my two lists of three items each.

Is this an oversimplification? Absolutely. But that’s the point. As your grandfather admonished you, “Always remember the KISS principle!” (Keep it simple, stupid.) A typical small credit union doesn’t have the assets, resources or time to throw at building the business continuity program the way the business continuity industry and your examiners demand, but that doesn’t mean it’s hopeless. My two lists of three are a great starting point—right *after* a look at your mission statement.

If your mission statement says something like “Our mission is to serve our members,” go back to the drawing board. My heretic viewpoint says your mission statement should be something like “Our mission is to safeguard our members’ money, and give it to them when they need it.” That’s right. Your *first priority* is to get members their cash in a crisis. Cash is King! Everything else is secondary! Nobody in your organization should ever forget this precept.

Now we can begin to look at my lists:

List 1: Risk Assessment Process

1. What threats face us?
2. What risks do those threats impose on us?
3. What can we do to minimize (or virtually eliminate) those risks?

This first list covers the threat/risk assessment portion of planning. Our hero doesn’t need to struggle with all the differentiation he reads about. (Why, for example, does he need a separate risk analysis for “Blizzard and “Ice Storm” when “Winter Storm” might suffice; or, to note the difference between a disgruntled employee and a disgruntled customer, when “someone going postal” might suffice?)

Keep it simple. Focus on the risk, not the threat: Computer systems go down! Work interruption occurs! The building incurs damage! Staff are unavailable! Pay attention to the closely related risks. That makes it easy—the mitigations are the same, regardless of the threats that impose the risk. In fact, what advantage is there in listing 20 threats that all impose the same risk, except to make the list look longer to keep the auditors and examiners busy? (Although some would naturally argue that there is some merit to that logic!)

Of course, the real reason for this analysis is to see what mitigations you currently have in place (or planned), and to measure (read “guess”) just how effective they really are. If you determine they aren’t effective, you take it to the board, which has a simple choice: 1. Accept the risk as is; or, 2. Cough up resources to add more or better mitigation.

With the risks mitigated, we can move on to my second list which covers the planning process.

List 2: The Planning Process. Ensure back-ups for:

1. People (Who backs up whom?)
2. Places (Where can they work if we lose our facility?)
3. Processes (How can they operate if the primary process is unavailable?)

Every business function depends on three critical elements: people, places and processes. You have to provide back-ups for each of them. It's like the proverbial farmer hand-milking the cow. He sits on a three-legged stool. If a leg breaks, he falls over into unpleasantness and the entire process comes to a halt. Our job is to prevent that from happening by using back-ups to shore up all three legs of the credit union milking stool: people, places and processes.

Every person or team in the organization needs a back-up. Maybe they aren't fully proficient, but trained and exercised well enough to continue a minimum level of service for the duration of the crisis. (And *no*, reorganizing the names from the primary team doesn't create a new team!)

Publish the names in your plan. Don't let it be enough for HR to bury an entry in the personnel folder that says Smitty can double as a teller. That information is lost if the records are destroyed in the disaster.

By the way, if you don't have a back-up, say so. Don't try to cover it up. Admitting a shortfall is the first step in correcting it. Just like in our threat-risk analysis, your business continuity plan is a mitigation. Identifying a mitigation shortcoming is OK. It shows you where you need work.

Similarly, every workplace needs a back-up. For whatever reason the facility becomes unavailable, staff need to know where they go to work (and members need to know where to find them)—and that location needs to be ready to go. It doesn't matter if the cause was flood, earthquake, hurricane, fire or riots, the result is the same—staff must go somewhere else to work.

Every process needs a back-up too. Keep the KISS principle at the fore here as well. Just because a primary process has a complex IT supporting process doesn't necessarily mean that the backup must be IT-based! For example, following Katrina, sister credit unions using printed trial balance reports dispensed cash from black garbage sacks stored in the trunks of cars using folding tables set up in parking lots. The transactions were recorded on old-fashioned ledgers until IT systems were restored. Was it elegant? No! Did it work? *Absolutely!*

With back-ups for people, places and processes identified and published, our intrepid small credit union is miles ahead of its competition (No, not other credit unions, but the neighborhood banks!), ready to face any adversity that might befall it. Has the CU developed a BIA, done a gap analysis, determined annualized losses in its risk assessment, or built an exercise schedule? Have it met all the requirements of the FFIEC guidelines, auditing standards or examination requirements, or even the business continuity professional standards? Absolutely not! There's plenty of work left to do.

However, the CU now has the foundations of a business continuity plan, and it can take care of these other details later. The CU is off to a great start, even if it used the rantings of this heretic to get there!

More importantly, the CU has the foundation for a business continuity program that will give it a leg up for continuing operations following a disaster. And, after all, that is what we in the business continuity and credit union industries want all CUs to have, and what their members should expect.

Kenneth Schroeder, CBCP, is VP/business continuity for \$3.3 billion Southeast Corporate Federal Credit Union, Tallahassee, Fla., which provides consulting support to member credit unions.

Several CUES members have contributed "immediate disaster response plans" to CUES Members Share. To access them, log in with your CUES member password, go [here](#) then type "immediate" into the search field.

© 2010 - CUES

Reprinted with permission of CUES