

Mom and Pop need Business Continuity, too

And it doesn't need to break the bank

John Glenn, MBCI

Enterprise Risk Management Practitioner

Part 2

This is not a plan and is not intended as a plan; it only lists suggestions on how a plan can be created with minimal expenditure.

Creating the plan

Creating an Enterprise Risk Management (ERM) plan actually is simple, but it cannot be rushed.

Gathering information

The first step is to determine exactly why the business is in business. What is the profit center?

Once the profit center – e.g., motel rooms or repair bay – is identified, we can start looking at things that might impact the profit center. (In a Big Company plan, processes performed by the profit center are identified first, and then risks to each process are hunted down.)

What threats or risks can keep the motel room or repair bay empty.

At this point, I suggest that one person act as discussion leader and another as the amanuensis, a fancy name for note taker, a truly critical person. I also suggest that the amanuensis set up a spreadsheet graph similar to the one below. The computer spreadsheet makes adding rows and later sorting them easier.

Risk/Threat (Name)	Means to Avoid/Mitigate (Eliminate, Reduce Risk)	Probability (1 to 5)	Impact (1 to 5)	Rating (1 to 5)

Make as many rows as needed.

A Risk/Threat may have several avoidance/mitigation options. Which option is best based on need and cost will be determined later.

The Rating column identifies which risk/threat should be addressed first. The Rating is assigned after all risks are identified.

List, without any particular order, risks as they are discovered.

Once most of the risks are listed – no list ever is complete – go back to the top and start to list means to avoid (usually expensive) or mitigate (normally less expensive) the risks. (This is one time a computer spreadsheet is handy since each risk may have several avoidance and mitigation options.)

Fortunately for the budget, some risk avoidance or mitigation options can be applied to multiple risks.

To help you decide which risks are the greatest threat to the business, rate each risk by probability and impact. Use “1” as least probable/least impact, and “5” as most probable/greatest impact. Don't worry that the Probability and Impact columns don't agree with the order of risks as they were recorded.

Now, it's time to see which risks deserve your attention first.

Look at each risk's Probability and Impact columns. In the Rating column, put a “middle” number.

If Probability = 5 Impact = 1 then Rating = 3

If Probability = 5 Impact = 5 then Rating = 5

If Probability = 1 Impact = 1 then Rating = 1

This quickly prioritizes which, as determined by the planners – and that's “all hands” - what risks need the greatest attention.

Bottom line time

Sooner or later everything comes down to “the bottom line.”

Let's say you have a 5-5-5 risk; it's rating gives it a Top Priority for attention.

There is an avoidance option that costs \$50,000 to buy and install, and it has a \$1,200-a-month maintenance fee.

There is a mitigation option that costs \$5,000 and has zero maintenance fee. But, the mitigation option only reduces the maximum anticipated damage and reduces the amount of time to return to business as usual. On the other hand, you'll have to spend more to recover (than if the risk had been avoided).

Determining the bottom line, both in "today's currency" and in the anticipated value tomorrow may require help from outsiders. Moreover, some things may not be worth saving; technology rapidly advances and prices decline; it may be more cost effective to insure some things for "replacement value" but to "absorb" another risk. (It could be that even insurance for a technology item – a computer, for example – simply is not worth the money.)

How much money is available to deal with the really critical risks, and if a little money is saved on a 5-5-5 threat, how much money will be left for lesser threats?

This is a management decision, but smart management knows it needs input from all resources, both internal (employees, board) and external (vendors, government).

By the way, insurance is a form of disaster recovery; having a back-up computer also is part of "disaster recovery;" there is no true mitigation involved.

How soon; the time line

Once the decisions are made what to implement and a budget is set up to this, the implementation time line needs to be fixed in concrete. Anything more than 6 months out should be ignored in the response planning.

Why? Experience shows that unless something is sufficiently critical to rate immediate attention, something else always comes up that will have a higher priority.

When all else fails

Some risks simply cannot be avoided or totally mitigated. The most obvious are weather-related: hurricanes, tornados, earthquakes, nor'easters, floods.

Before, the focus was on risks or threats.

Now the focus moves to impact. We have done everything financially and reasonably possible to avoid or mitigate the risk; now it's time to assume the worst – the risk occurs and we have to recover from it as expeditiously, economically, and efficiently as possible (else our competitors will take away our customers).

Start with the proverbial "worst case" scenario. You come to work (assuming you don't actually live where you work) and there is nothing there. Why this

scenario? Because it includes all lesser scenarios. (Don't like "scenario?" Try "event" instead. Consultants – which is what I am – need to be flexible.)

"Everything is gone" is a big chunk to chew, so break it down into manageable bites.

Let's say you have your accounting on the computer and the computer is useless.

You need to replace the computer with a compatible one (that is, one that runs the same software and has the same type connectors), and you need to reload (or have loaded) your applications that you carefully stored off site or at least in a data safe (possibly buried under tons of debris – you KNEW you should have taken everything to the bank vault). Then you need to restore information (data) from the back-up media – tape, CD, external hard drive.

Here's an "unadvertised" benefit of creating response plans. You see now what should be done, rather than later and what should have been done. Hindsight in advance – an oxymoron, but it works for me.

OK, the computer issue is resolved. Move on to the next issue.

How about the facility?

Unless your business IS a facility (e.g., lodging, catering hall) where can you go to keep doing what you do? You need to look for something as close as possible to your present - "former"? - location so people can find you.

While looking for a new facility, think about duration. Planning to rebuild on the damaged site (is it worth it?); how long will it take to rebuild (or restore). Should you ink a short-term (90 day) lease and anticipate a move to "somewhere" at the end of the lease or should you go for a longer term?

Take each process – including communications: telephone, email, courier, etc. - and isolate it to determine what it takes to restore the process.

While doing that, consider who will be restoring the processes. Be careful not to overload anyone. Going all out for more than a little while will cause burn-outs with slow recovery. Time off is important even when recovering from a disaster event.

If the Mom-and-Pop has employees, management needs to consider policies and procedures to cover disaster events. Will staff be paid, how much, how will they get their pay, for how long if work cannot be resumed quickly? What about insurance, benefits? Just because the income goes away doesn't mean payments stop.

Back to the lists.

This time, make a list (the spreadsheet software is good for this, too) of all the processes that can be impacted. You can start from "everything is gone" or from the other end, one process is gone.

Once again, this exercise is best performed with a group so nothing is missed.

Process	Dependencies	Action to restore
Process name or brief description	(What's needed? Documents, media, hardware, software, pencil sharpener?)	In general; restoration will be documented later step-by-step so that a novice can do it

As the list is populated, make sure to include ALL necessary resources, even if some are listed for several processes. All resources for a truly high priority process need to be restored before resources for lower priority processes, unless of course the processes share the resource(s).

Document, document, document

Each process to be restored needs to be completely documented. Never assume something is obvious (e.g., plug in and then turn on the system).

Keep the documentation simple; use the KIS(S) process: *Keep It Simple (Stupid)* the last word of course is optional.

List each step in order. I like tables, others prefer by-the-numbers text. Use whatever method works for you and the people who may have the recovery function, remembering that these people may NOT be the people who do the job day in and day out and that the recovery process may be different than the day-to-day operation.

As a former tech writer, I encourage you to have each restoration process validated by someone who is NOT familiar with the process and who has only the documentation to use.

Exercise the plan

No plan is perfect the first time out. If it is, it is flawed.

In more than a Baker's Dozen years, I never have seen a plan 100% on the first exercise. That's one of the reasons to have the exercises.

Start off simple – gather the troops and “walk-through” the documentation. Was anything missed? Is a process out of order? Are all processes complete? Are there any proven-to-work shortcuts? This is a two-part exercise. Part 1 is to review the total documentation. Part 2, with the group, is to share with the

documents author any necessary changes – clearing up ambiguities, for example - and to review the processes to assure completeness.

Maintain the plan

Maintaining the plan, keeping it up to date, may be the hardest part of the whole process.

The plan needs to be updated each time there are personnel, procedure, process, product, provider (vendor), and other changes to the operation. It's a nasty job, but someone's got to do it. The best person to do it, and assure the job is done right, is Mom or Pop.

Planning on a budget

Creating and maintaining a viable Enterprise Risk Management plan need not be a budget breaker nor need it become a full-time job for someone with “better” things to do.

On the other hand, it does require some budgeting of money and time.

Developing a plan, playing the “what if” games and challenging each other to make certain all the Is and dotted and the Ts crossed can be both challenging and fun.

The end results can mean surviving a disaster event or going out of business (and taking employees and possibly vendors under with the business).

John Glenn, MBCI, has been helping organizations of all types avoid or mitigate risks to their operations since 1994. Comments about this article, or others at <http://JohnGlennMBCI.com/> may be sent to Planner@JohnGlennMBCI.com