BCM Regulatory Soup

DO YOU LIKE ALPHABET SOUP?

As a kid, I remember my mom making alphabet soup for lunch. I would try and try to spell words and make sentences – a tireless game as all of the letters would eventually swirl around and become confused all over again. It was great eating, but frustrating all the same.

So, what does alphabet soup have to do with Business Continuity Management (BCM) or Information Technology Disaster Recovery (DR)?

SO MANY REGULATIONS - SO LITTLE TIME

In case you haven't noticed, we BC/DR folks live in a world of regulatory alphabet soup. There are well over 100 regulations, methodologies, maturity models, guidelines and laws – what I'll call, "authoritative sources" that have something to say about how to implement or manage BC and/or DR. These authoritative sources can be regional, country-specific, industry-specific, topic-specific, offer practical advice, supply best practices and much more. Just thinking about it is enough to make your head spin, let alone trying to comply with them.

I'm not making light of these sources in any way as they serve their own purposes and some excellent thought and preparation has gone into them, but for the sake of an example, let's take a look at my current bowl of alphabet soup – ISO22301 … BS25999 … HB292 … NFPA1600 …. ITIL … NIST… Z1600, etc. So, my quandary as a business is how do I determine which of these sources to comply with? Which of them actually apply to my business? How can there be so many varied sources, and are they really that different? Do they all say the same things and how do I coordinate them all?

A LITTLE HELP FROM OUR FRIENDS

Industry experts, including our friends at Disaster Recovery Journal, have done a great job compiling and coordinating these sources for our reference (for example, see http://www.drj.com/tools/tools/dr-rules-and-regulations.html). But this information still leaves you asking the following questions:

- Which sources do I comply with and why?
- And once I've figured that out, how do I handle conflicts between the sources?
- How do I prioritize them?
- Further to that point, how do I institute these requirements into my existing program?
- And if I do, will these authoritative sources provide me with good guidance or are they just a checklist of requirements?
- What if I'm audited -- how do I prove my program is compliant?
- Finally, how do I explain and justify this to executives and business partners?

These questions are being asked in BC/DR programs of all levels of maturity. It can be daunting to weed through the morass and put together a coordinated program that you can actually manage. Here, we strive to give some practical guidance on how to do just that.

ELIMINATE WHAT DOESN'T APPLY TO YOU

The first step is to understand enough about the authoritative sources that you can begin eliminating the ones that don't apply to your organization. Once you are comfortable with the list of regulations, methodologies, maturity models and laws you can begin reducing the list. Here are some ways to do that.

- Laws and Regulations – If a law or regulation applies to your business – follow it. If you have questions or need advice, discuss your requirements with your legal department.
- Your Industry – Many of these sources apply to specific industries, such as the FFIEC for the financial services industry. Eliminate those that don't apply to your industry. Although some of these may have great ideas, chances are they are replicated in another source.
- Where You Do Business – This might be obvious, but include those authoritative sources that apply to the part of the world where your company does business. If the Australian Commonwealth Criminal Code (1994) doesn't apply to where you do business, remove it from your list.
- Good Practices – This speaks mostly to the methodologies and best practices out there, such as the Carnegie Mellon Resilience Management Model. These models strive to represent best practices or give you a roadmap on how to mature your program. Implement what works for your company today – it could be the best practices out there, or maybe it's just the practice that's best for you.
- BC/DR Program Maturity Level – Something to consider, especially when you're determining which best practices or methodologies to adopt, is the maturity of your BC/DR program. Do not eat the elephant all at once. Instead, adopt those methodologies that coincide with the maturity level of your program and it will give you good practical advice and steps to help you continue to develop your program in a way that doesn't outstep your company's ability to progress along with you.

Simplify Your Soup

Evaluate your requirements based on:

- Applicable laws and regulations
- Your industry
- Where you do business
- Good or best practices
- Program maturity level

Get Organized

- Prioritize your compliance requirements
- Coordinate and consolidate your sources
- Make use of internal and industry resources
- Measure and evaluate your progress
- Be prepared for your audit
- Things change. Don't get left behind

Once you've determined the list of sources in which your company needs to comply, you should evaluate:

- What's the priority order of the sources that apply to my organization?
- How do I ensure I coordinate compliance across the sources without duplicating or missing something?
- How will I prove compliance if my program is audited?

NOW GET ORGANIZED

You have nailed down your sources and are now ready to move your program forward. It's important to get organized before diving in.

- Prioritize First – Of the sources you've selected, you'll now want to prioritize what requirements are most important to comply within your organization. Come up with a prioritization approach that makes sense for your company. Laws and regulations are typically pretty important, so consider these first. Then you may want to look at industry guidance, then regional guidance, and finally methodologies or best practices that make sense for your business.
- Coordinate the Sources – This can be a real challenge as it requires an organized effort to match up the sources you're going to comply with to see where they overlap or differ. Put a comprehensive list together to help you match up those duplicate requirements and consolidate them. Once you have a good list of requirements spanning all your authoritative sources, take it a step further and prioritize the requirements so you can start with what's most important to your organization.
- Use Your Resources – Chances are that there are others within your company that are exploring these issues as well. Work to coordinate your plans with other departments that may have a similar interest in the program – specifically legal, compliance and audit departments. Let them know your intentions and approach and leverage what they've done or are doing. If your company uses automated methods, such as a tool suite to manage governance, risk or compliance, leverage that too. In addition, leverage local BC/DR industry groups to ask questions and share best practices.
- Measure and Evaluate – Remember, everything we do in the business world – even compliance – is a cost/benefit decision. More and more, BC/DR is not only becoming an executive strategic imperative but also a discipline that must show proven results – quantitative and qualitative. Therefore, it's important to set goals, measure your progress, self-evaluate and report your results. Be proactive and vocal. We practitioners know BC/DR is an invaluable discipline, but to the executive or business partner that has many priorities, it's often just another item on the list. You must prove how critical BC/DR is to your organization and that your team is ultimately reducing the company's risk. A tool suite can be a great way to track your plan, measure your results, evaluate progress and report progress to executive management.

- A Word About Audits – Now, I don't speak for all auditors out there, but having been one for 15 years, here's my perspective. There are always those audits (or auditors) that will evaluate each and every requirement of the audit subject to the 'T'. If this type of authoritative source, or others like it, is a requirement for your program, make sure you build it into your compliance approach. Additionally, I have performed audits across many companies, industries, organizations and topics and I always appreciated the group that had a logical, well-organized, justifiable, documented plan and program. Be organized, show and prove what you've done and why. This will go a long way with your auditor. All program elements may not be perfect or prevent any and all findings, but insight and feedback is always good.
- Keep Your Eyes Open – In today's global business world, one thing is for certain and that's change. Be aware of changes in the authoritative sources you follow, as well as new sources that emerge and their implications on your business and program. Also be aware of changes to your business, such as acquisitions (that may require additional authoritative sources), divestitures (that may reduce sources you have to comply with), or other business changes that may have downstream effects on your program.

IN CONCLUSION

So, back to that bowl of soup – is it looking more manageable now? Hopefully this approach will give you some food for thought to help you organize your soup into something that makes sense to your organization. Remember, another great source is your BC/DR colleagues in your industry or location. Our industry is filled with good people that are a wealth of knowledge and experience. In fact, you can discuss BC and DR challenges and questions with professionals within the RSA Archer Community. I am also interested in your feedback and input. Good luck and bon appétit!

Patrick Potter is a RiskSight Principal at RSA, responsible for the Business Continuity Management and Operations solution. He is a CBCP with over 20 years in BC/DR practice and consulting, and has worked with organizations around the world. You can follow Mr. Potter on LinkedIn.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, **CONTACT** your local representative or authorized reseller—or visit us at www.EMC.com/rsa.