NextGen 360° Advanced Business Continuity™ White Paper

Infusing Pragmatism for Real World DR/BC

Part 1 – The Risk Analysis

How can company after company work for decades to establish their disaster recovery program and still never test their critical applications end-to-end? And how can it take years to create departmental business continuity plans that simply document work procedures that are performed every single day?

Clearly, it can't be for a lack of procedure. There are hundreds of proprietary DR/BC methodologies out there. In fact, every practitioner and consulting organization has their own methodology du jour. There are also at least a dozen "Certifying Bodies", who for a price will bestow "expert" designations relative to their own benchmarks. And most recently, there has been a constantly-increasing number of published "Standards" issued by various international- or industry-specific organizations all of whom are vying for their standard to become THE standard.

Some of these methodologies and standards are reasonably mature. Others are clearly first attempts. Some are far-reaching. Others are very narrowly focused. Some are overly easy to implement. Others can take years

However, one shortfall that they all share is a disconnect with day-to-day reality…particularly in large organizations. While all of these methodologies/standards attempt to address DR/BC needs as they perceive them, none attempt to integrate real-world pragmatism into their model. The perceived theoretical or philosophical need of the subject matter is their universal goal. The practicality of achieving that goal in the real world is seldom even an afterthought. We attribute the DR/BC industry's befuddling acceptance of never-ending program development to an industry-wide surplus of practice and a severe shortage of pragmatism.

Real day-to-day constraints can reduce even the best philosophical methodology to a meaningless pile of never-ending, contradictory tasks. Sometimes the methodological flaw is deceivingly minor, but overtime it poisons the entire program by undermining confidence and diluting management support. Looking back, you often cannot even point to the source of the poison…all that you know is that you've worked for years and still haven't reach your goal. Other times, the problem is so large and obvious that it can be career threatening.

But when the process is looked at for decades through the multi-dimensional lens of hundreds of different organizations…large and small, public and private, for profit and not for profit…we believe that there are six major elements that all of the methodologies and/or standards attempt to address with their own proprietary methods.

- The Risk Analysis
- The Business Impact Analysis
- The Architectural Solution
- The Development of Recovery Plans
- The Testing of the Program
- The Maintenance of the Program

We believe that across all of the methodologies, these six elements need a major dose of pragmatism to work in the real world. In this series, we offer specific recommendations for each element to ensure development of a pragmatic, real-world recovery capability that can grow with the organization and which can be maintained without an army of dedicated practitioners.

The first common program element is the Risk Analysis.

If, as statistics indicate, more than 80% of business disasters are caused by preventable or avoidable events, the importance of mitigating risks is obvious. Still, most risk assessments fail to elicit

the mitigation necessary to actually reduce risk.

We believe that an infusion of pragmatism in the following areas will dramatically improve the effectiveness of the Risk Analysis and increase the likelihood of gaining support for mitigating efforts.

Differentiate Risk Management (RM) and Risk Assessment (RA).

The fundamental difference between Risk Management and Risk Assessment is that RM tends to use probability (when low) as a rationale for acceptability. RA, for DR/BC purposes, should use probability simply to prioritize mitigation efforts. The difference is that while RM might define a low probability, crippling event as an acceptable risk given the organization's overall risk appetite, a RA for business continuity purposes would be require an acceptable level of recoverability despite the low probability. Infuse pragmatism into the RA by limiting its scope to "PIP" (Physical Exposures, Facility Infrastructure Exposures, and IT Policies and Procedure Exposures). By focusing only on risks that can interrupt business processes, the RA's scope can be pragmatically contained by disregarding (for DR/BC purposes) operational risk management such as credit risk, accidents, safety, legal liabilities, etc. that cannot interrupt business processes.

Physical Exposures unique to the exact geography must be fully evaluated in terms of: Risk, Vulnerability, Impact, Target Importance and Weighted Significance.

Too often, physical exposures are evaluated too broadly (in a geographical sense) with the result being an understatement of actual exposure. A geographical difference of 100 feet can have a huge effect on exposure. For example, a data center in direct line with the exit ramp of the highway is much more at risk than if it were 100 feet further up the street, out of the direct line of traffic. At the same time, physical exposures are often evaluated too narrowly in terms of the range of possible exposures. The pragmatic approach here is to evaluate each facility individually to develop its own, detailed exposure profile. To avoid arbitrary metrics, rate each facility relative to "a typical company in a typical location". This simplifying approach is easily understood by all participants and eliminates bias that results from different individual perspectives. Also, unless your analysis address at least 100 unique exposures, the exposure analysis is probably too narrowly focused. Finally, both non-forensic and forensic methods should be employed. We use the term non-forensic to describe an interview-based process where the findings are taken at face value and their veracity is not questioned (other than ensuring in-line consistency from one question to another). In contrast, we use the term forensic to indicate a research-based process where the findings are distilled from creditable, independent third-party data. The two approaches are more than just complementary, they are required if participant bias is to be pragmatically avoided or eliminated.

Explicitly assess the exposures resulting from each facility's unique infrastructure.

Fully 23% of business disasters are related in some way to failure of facility infrastructure and if facility location is taken into account the number increases to a staggering 54%. Still, this statistic is not unusual when you consider how few facilities where chosen with proactive business continuity requirements in the forefront of the selection process. While mitigating major facility shortcomings retroactively may not be practical in many cases, a comprehensive infrastructure assessment is critical if there is to be any hope for Proactive Continuity (e.g. the long-term

integration of business continuity objectives into the daily fabric of the organization). To define the term "comprehensive" pragmatically, the following topics must be addressed, and experience dictates that more than 500 individual questions are required in order to address all of the necessary nuances of the topics.

Information Technology's ubiquitous presence requires that IT policies and procedures receive an explicit focus in the risk assessment.

As the enabler of most business processes today, IT is clearly one of the most significant potential harbingers of risk. In fact, hardware failure has always been, and still is today, the single most common cause of business disasters. As such, IT demands a significant focus within the Risk Assessment. However, the breadth and depth of the IT arena can completely overshadow the entire Risk Assessment unless its scope is effectively contained. Experience dictates that the most pragmatic way to contain IT scope for DR/BC purposes is to focus only on IT Process and Procedure. Proper assessment of IT Process and Procedure as defined by the following categories will systematically cull the disaster-causing exposures from non-disaster causing aspects of IT and pragmatically simplify the assessment. Nevertheless, to adequately evaluate the component elements of all of these categories requires well over 500 distinct questions.

In any Risk Assessment, the completeness and effectiveness of the DR/BC program's ability to mitigate risks must be independently evaluated across multiple benchmarks to ensure impartiality and to avoid "blind spots" within individual benchmarks.

As mentioned above, the specific *raison d'être* of each standard, their built-in biases, their maturity level (or lack thereof) and their unique "blind spots" combine to make evaluation against a single standard problematic. However, choosing the best standards against which to benchmark a program is also problematic. The solution is to choose complementary standards that offer a balance of detail and simplicity, business continuity and disaster recovery and traditional practice with current thinking. Today, most practitioners would agree that a combination of BSI25999, ISO22301, NFPA1600 and DRII Professional Practices meet these criteria. However, individual assessment of every component against all four of these standards would quickly try the patience of even the most cooperative assesse. The pragmatic solution then is to distill each of the standard's elements down to their underlying intent so that in many cases, the same question/answer can apply to all three standards, albeit with more or less completeness. As such, the following program elements must be evaluated. Even with the aforementioned distillation, nearly 1,000 individual elements must be considered.

Programmatic objectivity of the assessment process should be required of the assessment methodology.

One of the most effective ways to use assessments is to gauge improvement over time. As such, year-over-year repeatability is a critical factor in the process. The process must ensure that any differences in the assessment are differences of fact, not simply differences of opinion. If two assessors conduct the assessment, their personal viewpoints and biases must not enter into the equation—both should produce the exact same assessment results. Similarly, changing business priorities, differing

management emphasis or any other external factor must not be reflected the assessment results. The most pragmatic way to accomplish this objectivity is programmatically. The assessment should employ a tool that that "enforces" the possible answers, the weighting scales, the report results and all other aspects of the assessment. The objective programmatic assessment can then be combined with subjective recommendations from the assessor to enjoy the best of both worlds.

Not all organizations are the same; therefore, the assessment must be customizable to the specific situation.

If in fact an objective tool is used to conduct the assessments, that tool must be customizable to ensure that its built-in assumptions match the needs of the organization…particularly if year over year assessments are anticipated. Assumptions for question and section weight, tags to indicate which questions resolve to which reports, best practice tags, standards tags, etc. all need to be easily modifiable to ensure compatibility with the organization's needs. Pragmatically, even once the underpinnings of the tool have been customized, the tool itself should be "intelligent" enough to automatically customize itself for different assessments with the organization. For example, if one building has card key entry controls, then its assessment must address card key controls. If the next building does not, the card key control questions should automatically be eliminated from the assessment. With this approach, the length of the assessment is always optimal for the target audience and they feel it clearly reflects their environment.

A pragmatic Risk Assessment can dramatically change management's perception of the viability of the assessment, and once the results of the assessment are accepted, the likelihood of gaining support for mitigating activities increases proportionately. By minimizing the interpretation of theoretical probability and focusing on understandable, real-world impact, the Risk Assessment can become valuable tool in the DR/BC lifecycle.

The William Travis Group is a dedicated disaster recovery, business continuity and all-risk incident management consulting firm that has been in business for over 25 years. The founder of WTG has been in the disaster recovery industry since its inception and developed many of the technologies and methodologies that represent the standard in the industry and the baseline for today's practitioner certification. Today, WTG's NextGen 360^0 ABC™ methodology offers a holistic All-Risk Incident Management approach that combines best practices in disaster recovery and business recovery planning with leading edge all-risk initiatives such as management succession planning, supply chain continuity, pandemic operations, manufacturing resource planning, production line continuity and other advanced continuity solution. WTG works with across all industries with organizations of all sizes, both public and private and guarantees its clients 100% satisfaction.

The William Travis Group can be contacted at 1827 Walden Office Square, Suite 220, Schaumburg, Il 60173 ■ Phone 847-303-0055 ■ fax 847-303-0378 ■ www.williamtravisgroup.com ■