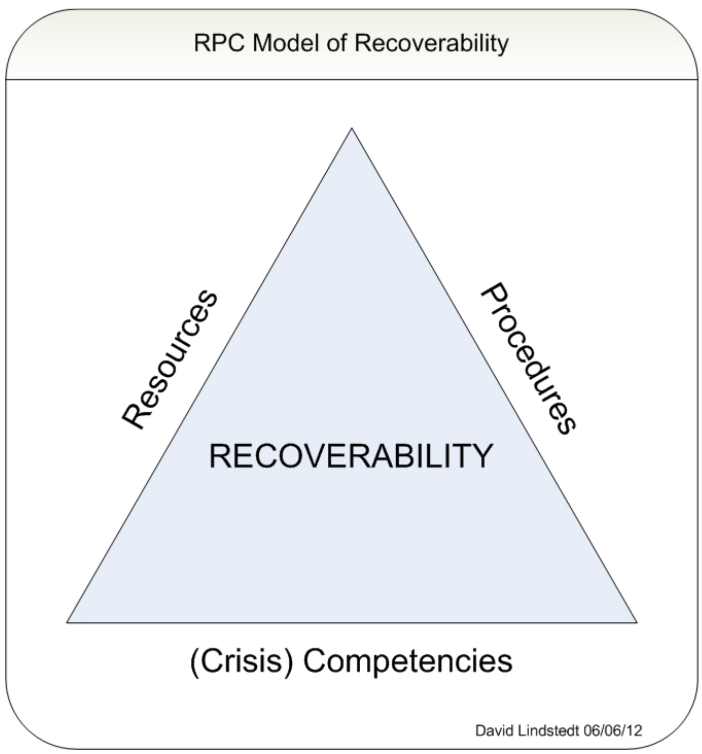
Measuring Preparedness and Predicting Recoverability

David Lindstedt, PhD, PMP, CBCP

With input from John Smith, ABCP



Version 1.0, Revision 3 – August, 2012

Creative Commons License

I hope that this model will benefit the resilience community as a whole and that it can be improved with additional usage, dialogue, and research.

[1] https://creativecommons.org/share-your-work/licensing-types-examples/, viewed 08/13/19.

Table of Contents

Abstract

Preparedness to recover from disaster can be measured. The likelihood of recovery can also be predicted, though only an approximate formula is possible with current data.

Recoverability consists of: Resources, procedures, and competencies (RPC). The state of preparedness for recoverability can be ascertained by measuring these three factors.

For proper measurement, the scope must be properly narrowed to exclude prevention activities, focus on physical or staffing losses, and factor in both time and degree of post-incident functionality. Recovery preparedness is not the same as readiness, resilience, survivability, or any other all-embracing concept.

All individual factors of resources, procedures, and competencies that are not ready-at-hand within necessary timeframes become post-incident costs. These costs can also be identified and classified in terms of: Brand, money, (eliminated) services, and/or time.

This model for measuring preparedness and predicting recoverability:

- Is applicable to small businesses and large organizations alike
- Enables apples-to-apples comparisons within and between organizations
- Is compatible with existing standards, practices, and methodologies
- Removes the current focus on documentation
- Provides an ongoing measure of progress for work done on preparedness planning
- Allows for additional research, reliability, testing, and improvement

Surprisingly, however, preparedness is not equivalent to recoverability. This is due to the fact that individual RPC factors do not act in silos; they interact with each other. Gaps in one RPC factor influence the other two RPC factors so that problems are compounded.

There is not enough research to provide an accurate formula for predicting recoverability, but a first approximation is:

Recoverability = R x P x C

where R is resources, P is procedures, and C is competencies.

This formula captures the multiplicative nature of the three factors and shows that improving (or neglecting) any one factor will have an influence on the other two as well as recoverability as a whole. It also means that an organization's measure of preparedness will be much higher than its predicted recoverability.

This formula is a working hypothesis in the truest sense of the term. It should serve as a starting point against which to predict recoverability and measure actual results.

Introduction

Can we predict the likelihood that an organization will recover from a disaster before a disaster ever happens?

Organizations are increasingly focused on preparations to recover critical services following a disaster. But are these preparations effective?

Organizations need to know which preparation efforts will improve their odds of recovering. Stakeholders should know when preparations are adequate and when gaps exist.

In a similar vein, measuring the efficacy of any particular plan or planning effort remains a significant challenge to continuity planners. Measurements that focus on documentation (whether all the boxes have been checked, the fields filled in, and the last time they were updated) do not provide an accurate assessment of the real preparedness and recoverability of a unit.

This paper addresses the following critical questions:

1. What are the factors that determine recoverability?
2. Can preparedness be measured?
3. What is the relationship between preparedness and recoverability?
4. Is it possible to predict recoverability?

These questions ought to be of fundamental importance to the profession of recoverability planning, and to the leaders of any organization wishing to dedicate time, money, and effort to prepare for potential, adverse conditions. It is clear that not only executives, but policymakers, the public, and "jurisdictions at every level across the country are asking 'What are we getting for our money?'"[2] If practitioners are to avoid a wasteful, scattershot approach to preparedness, thereby providing the most value for the money, the answers to these questions are indispensable. Hopefully this model will help anyone engaged in improving the overall resilience of their organization.

The paper attempts to shed light on the essential elements of preparedness and recoverability by presenting a conceptual model of recoverability. It focuses briefly on the scope and definition of recoverability then provides answers to the four questions above. It concludes with a presentation of issues that arise as a consequence of this model.

---

[2] Jensen, Jessica, Ph.D., "Preparedness: A Principled Approach to Return on Investment," International Association of Emergency Managers, August 11, 2011.

Section One: The Proper Scope

One challenge of preparedness and recoverability discussions is that key terms in this industry are still somewhat unclear or undefined. Terms such as resilience, continuity planning, sustainability, disaster recovery, survivability, risk management and others are often equated or conflated.

This paper focuses on "recoverability" and whether it can be measured and predicted. It begins by defining "recoverability" through five core principles and delineating its scope to avoid possible confusion with other industry terms and concepts.

To begin with, recoverability must be differentiated from "prevention."[3] No matter how much a unit has worked to mitigate risks in an attempt to prevent an incident, it may be forced to recover from loss. A building may have the finest environmental alarms, fire suppression systems, closed circuit monitors, security systems, vehicle blockades, and blast-glass windows, but it may still succumb to disaster.

Preventing potential threats is only useful up to the point of an actual loss, no matter how unlikely. After the loss, the unit is forced to recover. At that time, the unit must rely on the work it has done to prepare to recover.

The focus of prevention is avoiding a loss; the focus of recoverability is recovering from a loss and efficiently returning to "new normal". [4] This point is often lost, confused, or conflated, so it is stated here as a clear principle:

1. *Preparing for recoverability is not prevention.*

Secondly, it is important to posit that:

2. *Recoverability is not survivability [or resilience].*

The purpose of preparedness is often believed to be as follows: Improve the <u>survivability</u> of an organization. There are two fundamental problems with this belief.

[3] "Recoverability" can also likely be differentiated from "mitigation," but the utilization of the term "mitigation" in existing standards makes it unclear. NPFA 1600 defines mitigation as "activities taken to reduce the impacts from hazards" (3.3.15). ASIS SPC.1-2009 defines it similarly. These definitions might, or might not, include recovery preparedness activities depending upon interpretation. I suspect that mitigation is too broadly defined in most existing standards which means that myriad planning activities are incorporated under the current definition.

[4] This paper purposely avoids the term "recovery planning" as it typically connotes planning solely for information technology; the terms "recovery preparedness" and "recoverability" are at once meant to capture a broader scope than IT disaster recovery planning, a different scope than prevention, and a stricter scope than survivability or resilience.

The first problem is the almost innumerable variables that contribute to an organization's survivability. Listing all the critical components of a successful organization operating under all conceivable circumstances with all the different disciplines that play their role would soon exceed the course listing of every MBA program. Unpacking all the requirements of survivability (or resilience) would far outstrip the proper domain of preparedness.

The purpose of continuity planning is sometimes given as: Improve the survivability of an organization.

But such thinking is flawed.

The term survivability covers too much ground, first because there are so many variables that contribute to an organization's survivability, and second because what it means for an organization to "survive" is nebulous.

The second problem is that what it means for an organization to "survive" is nebulous. Particularly within the context of a disaster, speakers often focus simply on whether the organization "survived" the event. But, surely, there are better and worse conditions under which an organization stays in business. Was the organization forced to cut staff, reduce services, and expend capital? Did it lose market share? What are its prospects for the next few years? Survivability, as well as recovery, cannot be an all-or-nothing prospect.

At least for the purposes of this paper, recoverability must not be expanded to include readiness, resilience, survivability, sustainability, or any other all-embracing concept.

Next, as recoverability implies that the organization is recovering from something, FROM what is it preparing to recover? In this case, the scope is concerned only with recovering from a *physical* loss or a loss of *staffing*. While the two previous distinctions allowed us to differentiate recovery preparedness from prevention and survivability, this third distinction allows us to differentiate recovery preparedness from issue management and crisis / reputation management. While we will not argue for a particular definition of each, in general we see:

- Issue management as the lifecycle to monitor and respond to emerging threats[5]
- Crisis / reputation management as the response to incidents which primarily threaten an organization's brand or reputation

Whereas recovery preparedness and prevention have little to no overlap, recovery preparedness does overlap to some degree with issue management and crisis / reputation management. The paper does not need to detail the degree of difference, only to properly focus the model as such:

[5] See, for example, Issue Management Council, Public Service White Paper: "Issue Management: Tool for Crisis Recovery and Mitigation," 2001.

3. *Recoverability concerns recovery from a physical and/or staffing loss.*

Naturally, the term recoverability also implies that the organization is recovering something. WHAT is it recovering? The simple answer is that it is recovering its services as it establishes a "new normal." The organization will likely not look the same as it was before the disaster, but will recover some level, perhaps even an improved level, of services pursuant to its core mission.

The literature uses many terms to describe this "what" of continuity and recoverability, particularly these expressions: processes, functions, systems, operations, and services. For the purposes of this paper, the term "services" is used. This allows for the inclusion of any process, function, operation, or service that must be resumed to support the core mission of the unit, area, or organization.

It is also important to note that services might need to be recovered individually as well as in an organic whole. Each level of the organization, from the unit up to the entire organization, has a collection of services that must operate together. Therefore, a fourth principle can be introduced, namely that:

4. *Recoverability concerns the reestablishment of services, either individually or as an organic whole.*

This leads to the final principle of recoverability:

5. *Recovery is always a matter of degree.*

This principle can be partially deduced from the above discussions on "survivability" and "service." There are better and worse conditions under which an organization stays in business (or, for that matter, goes out of business). Similarly, recovery is not an all-or-nothing prospect. Leaders of organizations, areas, units, and even services may elect (before or after an incident) to recover all, some, or none of their existing functionality within a designated period of time.

If we aim to measure preparedness, we must move beyond simple black and white notions of survivability and get to a real understanding of the different possible degrees of recoverability. Further, if we aim to predict recoverability itself, we must be able to say what kind of recoverability we have in mind. Section Three below will unpack this principle in further detail.

At last, based on the principles established in this section, a definition and proper scope of recoverability can be formulated as such:

Recoverability: The ability to recover services, individually and/or holistically, within the targets of time and degree following a physical loss and/or a loss of staffing.

Having laid the foundation for the model with these five principles and a definition, let us turn to the larger question: What are the factors that determine recoverability?

Section Two: The Factors of Recoverability

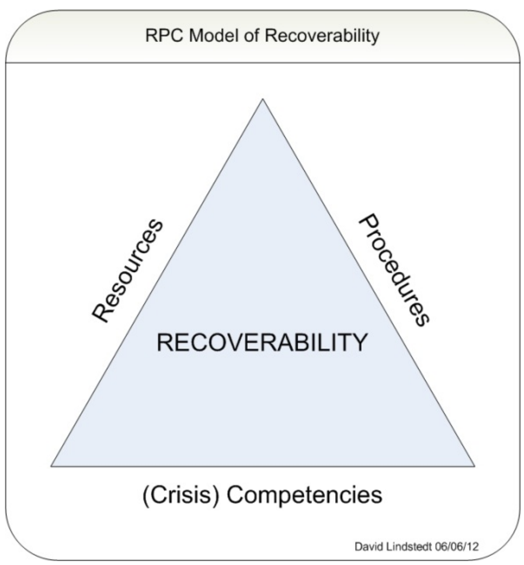
Naturally, there are many factors that come into play when considering the ability of a unit or organization to recover from a disaster. This, in part, explains the wide variety of planning standards, best practice guides, and maturity measures across the discipline of business continuity and risk management. Nonetheless, it is possible to synthesize and categorize the variables that factor into recoverability.

After a disaster, a unit or organization must rely upon the following to recover (some portion of) its operations:

- Resources: Physical assets required to provide services[6]
- Procedures: Methods, practices, and instructions for taking action to recover services[7]
- Competencies: Characteristics allowing individuals to function throughout recovery.[8]

One might think of this as the "what," the "how," and the "way" a unit can continue services.

Thus, a high-level model looks like this:



By way of example, consider the following brief scenarios:

[6] ISO 22301 definition of resources: "all assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objective", 2012, Section 3.47.
[7] ISO 22301 definition of procedure: "specified way to carry out an activity or a process", 2012, Section 3.39.
[8] [8] ISO 22301 definition of competence: "ability to apply knowledge and skills to achieve intended results", 2012, Section 3.9.

- A small manufacturing company is without power for many days. While they know how [procedures] they would restore each of their production lines, with leaders ready to take charge [competencies] and workers trained for tasks [competencies], there is no other manufacturing equipment available [resources], and they are forced to suspend production.
- A training department loses their building. For the first several days, they suspend all classes. But within two weeks, they collaborate [competencies] to identify and obtain teaching space [resources], figure out [competencies] how to make do [procedures] without the usual materials, and resume most classroom instruction.
- A data center is destroyed by fire, but they have experienced staff [competencies] to utilize a host of practiced procedures [procedures] to restore services within one hour at a fully redundant hot site [resources].

Any identifiable factor of recoverability fits somewhere within one of the three RPC categories. But what types of items fit within each of these factors? What are the further levels of categorization?

Such categorization is going to be a topic of much debate, and properly so. The paper's conclusion will say more on this. However, it is important to note that the model should be able to incorporate any item of preparedness into one of these three categories. While the details will be up for debate, for now let us offer some guidance.

With regard to resources, these will be whatever the unit needs at-hand at time of disaster to provide services and aid in recovery. The list of specific, required resources will vary widely depending on the unit, ranging from pencils and paper to sphygmomanometers and NMRIs. This is the "what" is needed to recover. A high-level categorization for resources might be as follows:

- Equipment (including workstations)
- Hardware (especially if recovering IT)
- Software / Applications
- Space / Locations (including HVAC, network access, telecom access, and utilities)
- Staffing[9]
- Supplies
- Vital Records (including contact information, documents, and spreadsheets)[10]

With regard to procedures, this is "how" the unit will recover. Naturally, the specific procedures needed to recover will vary widely depending on the unit. This is particularly so when it comes to restoring specific services. There are a variety of ways these specific procedures might be categorized. Yet, a categorization of these procedures is possible by:

---

[9] It is important to note that staffing does NOT include what might be termed "human capital" such as education, training, knowledge, and skill sets; these must be categorized within procedures and competencies.
[10] The importance of capital cannot be underestimated. Yet, as this capital must be expended and transformed into actual resources at time of disaster, it ought not to be listed as a resource in itself.

analyzing typical activities in the hours following an incident, synthesizing existing industry standards and best practices, and acknowledging the uniqueness of specific service recovery and continuity procedures. The following categorization can classify the many different types of possible procedures:

- Assess
- Communicate
- Coordinate
- Establish Locations
- Mobilize
- Prioritize
- Reestablish Services

Finally, competencies are the "way" in which the unit will recover. This factor often gets overlooked in preparedness planning but is vitally important. A unit or organization that does not have the proper experience, performance, crisis exposure, preparedness planning, leadership, and training is going to be far less prepared to recover regardless of the resources and procedures that might be in place. In fact, some writers in the profession have even argued that competencies are the only important factors in preparedness and recoverability.[11]

Arguably one of the best studies on organizational readiness is Paul C. Light's "Predicting Organizational Crisis Readiness: Perspectives and Practices toward a Pathway to Preparedness."[12] While Light's paper is devoted to "crisis readiness," *per se*, clearly his focus on preparedness is instructive to the topic at hand.

Light argues that "…crisis readiness is a function not just of crisis readiness activities but also of the organization's characteristics" (p. 21). In the language of the RPC model of recoverability, Light's statement might be translated as: preparedness is a function not just of procedures but also of competencies. Light proposes a categorization scheme for those characteristics of an organization that are likely to be statistically significant measures of crisis readiness.[13] Summarizing Light's conclusions, he identifies the following significant characteristics of preparedness; those qualities marked with an asterisk indicate the most significant indicators:

The organization:

---

[11] See, for example, Stagl, John, "DRII, ASIS, NFPA? They're all missing the point," *Continuity Insights*, Vol. 6, No. 5, p. 20.

[12] Light, Paul C., "Predicting Organizational Crisis Readiness: Perspectives and Practices toward a Pathway to Preparedness," The Center for Catastrophe Preparedness and Response, New York University, Public Entity Risk Institute, year?

[13] Light identifies a list of 23 significant "predictors of crisis readiness;" interestingly, he concludes that there are five predictors that are the most significant: high-performing, experience with external crises, shared vision of mission, preparedness planning, and preparedness training (p. 52).

- Engages in preparedness planning, training, and exercises*
- Has clear chains of command with leaders who share a vision of mission* and encourage teamwork
- Has high-performing,* competent, competitive, results-driven, and innovative employees
- Is vulnerable to, threatened by, or has experienced external crises*
- Regularly surveys clients and customers and actively monitors threats
- Spends time and money on continuous improvement of crisis readiness

I have taken and synthesized Light's 23 significant predictors for competencies, making alterations which I hope will simplify the list and make it more intuitive. The ideal characteristics for those responding to an incident and recovering services are:

- Crisis Fortitude
- Leadership
- Performance
- Shared Vision
- Teamwork

The degree to which these competencies exist *before* the incident will dramatically influence the effectiveness and efficiency of the response *after* the incident.

These qualities must ultimately manifest themselves to some degree in any successful recovery effort. Employees must achieve at least at a high enough level of performance to work together to reestablish services. Individuals must have at least enough fortitude to weather the crisis and assist in recovery. Someone or some group must take charge of coordination, make decisions, and provide leadership. And all must have enough of a shared vision of mission to unite and agree upon what must be done. Ideally, the organization would have: high performing team(s), trained to recover services, coordinated by strong leaders who share a vision of mission.

What is important in all this is this: The degree to which these competencies exist before the incident will dramatically influence the effectiveness and efficiency of the response. As Light notes, "Readiness is certainly possible in organizations with lower levels of [competencies]… but it is almost certainly easier to achieve if these and other conditions are met."[14]

Returning again to conceptualizing the three factors of preparedness, it may be helpful to think of them by way of analogy, as seen in the following table.

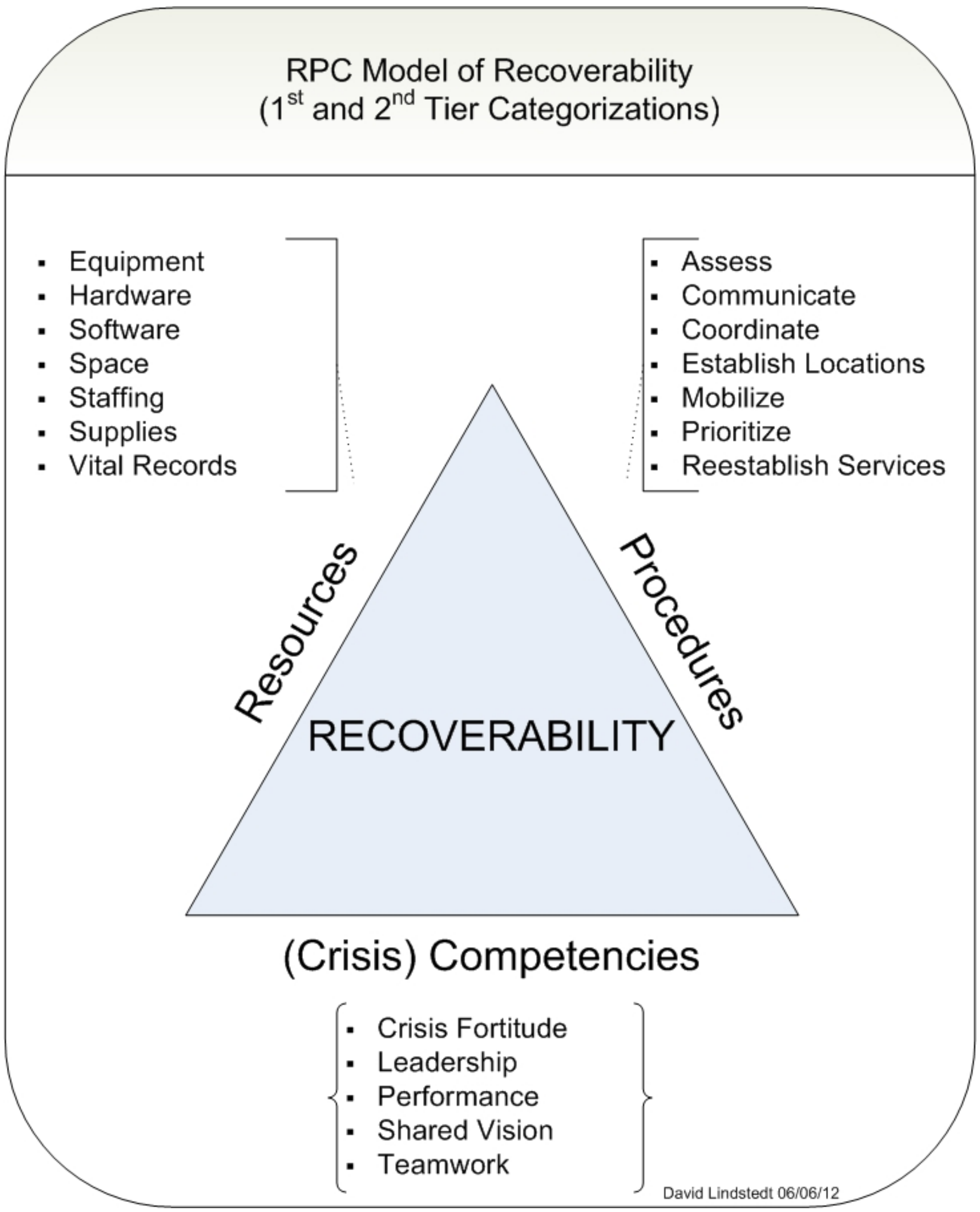
Resources	Procedures	Competencies
"What"	"How"	"Way"
Nouns	Verbs	Descriptors
Stuff	Actions	Characteristics
Things	Activities	Qualities

[14] Light, *ibid*, p. 53.

Availability of physical resources	Knowledge of what to do	Abilities to perform throughout a crisis

Doubtless there are additional ways and levels to categorize RPCs. It is not the purpose of this paper to try and flesh out the entire skeleton at this point, but rather to establish the initial framework for proper discussion, research, and debate.

Thus, the final model can be presented rather simply, with both the primary and secondary categorizations displayed, in the following diagram.



Why is such a model important and what does the discipline gain from this categorization? Isn't this just introducing one more planning guide?

This framework is critical for the following reasons:

1. It provides the only existing model to measure preparedness and predict recoverability. Other guidelines, standards, and best practices recommend how to implement a program and even measure its maturity. They are wide-ranging in scope. They focus on many aspects of resilience including life safety, IT disaster recovery, continuity planning, crisis management, and risk mitigation. None of them, however, provide a method to measure the work done specifically to prepare to recover services from a physical or staffing loss.[15]

2. It focuses on recoverability, not on plans and documents. Too often practitioners and stakeholders get caught up in documentation and counting the number of plans created for an organization. As Jensen notes for the field of emergency management, "knowledge of the numbers of emergency operations plans in existences tells us very little."[16] Some measure preparedness by the last time their plans were updated. While proper documentation is a key element of preparedness, it is clearly not the only factor. Along these lines, the discipline must move away from vague questions such as, "Do you have a plan?"[17] to "What is your estimated measure of preparedness and prediction for recoverability?"

3. It both narrows the scope and provides a common language. There is much confusion in the industry on the part of practitioners, stakeholders, and customers alike as to what types of readiness activities fall under which broad categories. This framework allows us to narrow the scope of future discussion, research, and debate surrounding recoverability (only) to: The ability to recover services, individually and/or holistically, within the targets of time and degree following a physical loss and/or a loss of staffing. As such, it can be utilized as a measure within and between other methodologies and standards without impacting their specific adoption.

---

[15] For a longer discussion and more information on this topic, see Appendix A below.
[16] Jensen, *ibid*, p. 10.
[17] See: Flach, Joe, "Why I Hate The Word 'Plan'", *Continuity Insights,* http://www.continuityinsights.com/blog/post/why-i-hate-the-word-plan, viewed 10/27/11.

4. It simplifies and focuses conversations with stakeholders and customers. With a narrow scope and three measures, it is much easier to talk with those who are footing the bill for recovery preparedness and ask critical questions such as:
   - Is it important for our organization to recover from a disaster?
   - How much of our organization and how quickly?
   - How prepared do you think we are now?
   - How much more prepared ought we to be (and is the cost justifiable)?

5. It enables apples-to-apples comparisons within and between organizations. Practitioners can compare the preparedness of non-like services and units within an organization. Stakeholders can get a good sense of the level of preparedness for all aspects of the organization, accounting for differences in targets of degree and timeframe, and despite the fact that the types of services are disparate. Further, analysts outside of any single organization can compare and assess multiple organizations within a single industry or that constitute a single community.

6. It is universal and scalable. Whether we are talking about the recovery of a single service, a unit, an area, or an entire organization, we can reduce preparedness to a simple model. Each level allows for its own measurement and requires its own work to ensure the existence of proper RPCs prior to the time of disaster. Moreover, it can be applied to small businesses and large corporations alike; any organization from mom-and-pop shops to Fortune 500 companies can adopt and adapt the model.

7. It allows for appropriate degrees of precision. Many organizations and their executives may be satisfied with a rough estimate of preparedness and recoverability. They may need only to look at a high-level measure that focuses on the first or second tier of the RPC model of recoverability. Other organizations may desire a much higher level of precision in their measurements. The RPC model allows for such precision, moving into third and fourth tiers of analysis and prediction.

8. It suggests a proper way to set up a recoverability program. Organizations often struggle with the best way to establish, organize, and govern a resilience program. There are many standards and best practices available, and the RPC model of recoverability does not conflict with their adoption. However, this model does suggest a way to structure a program or sub-program focused exclusively on recoverability. This model implies that each section within a resilience program must have its own proper scope and body of knowledge. It also suggests that the recoverability section (or program) itself operate in such a way that it properly prepares the organization to recover its designated services within the targets of time and degree.

Having presented a conceptual model and having discussed several immediate advantages,[18] the paper now turns its attention to a deeper analysis of measuring preparedness.

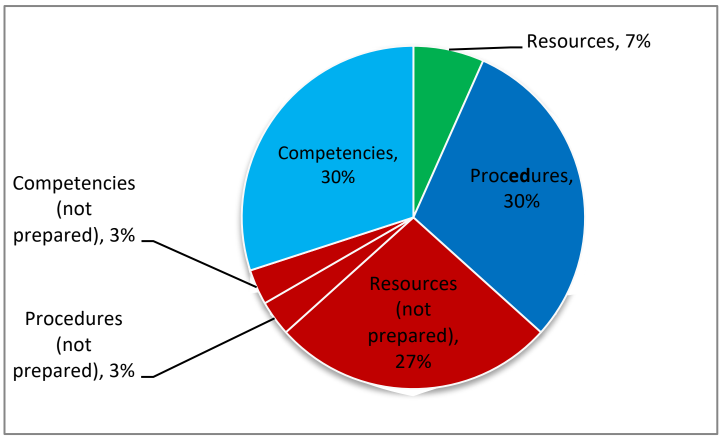
[18] There are two additional reasons this framework is so critical, but these must wait until the full discussion of recoverability later in the paper. In short, the model also allows for the identification and categorization of costs, and a predictor of recoverability.

Section Three: Measuring Preparedness

Measuring a unit's degree of preparedness seems simple in principle: identify the resources, procedures, and competencies (RPCs) that need to be in place then compare them to those RPCs that are actually in place. If a unit has 75% of everything it needs to recover, then it stands to reason that it is 75% prepared for recovery. Adding together and then averaging the RPCs for a unit provides a measure of preparedness that can be mathematically expressed as:

Recovery Preparedness = (R + P + C) / 3

Consider the manufacturing example from earlier on where the organization had no alternate equipment available to them during an extended power outage. Before the disaster one might judge that they have only 20% of the resources they need (since they do not have another manufacturing site to use) but perhaps as high as 90% of the procedures and 90% of the competencies they require. Looking to analyze this in terms of the whole, preparedness might be most easily visualized like this:



In this case, one might say they are 66.6% prepared, as (20% + 90% + 90%) / 3 = 66.6%.

While this approach seems simple enough, it presents an immediate problem: how can one account for differences in the degree and timeframe of what the unit wants to recover?

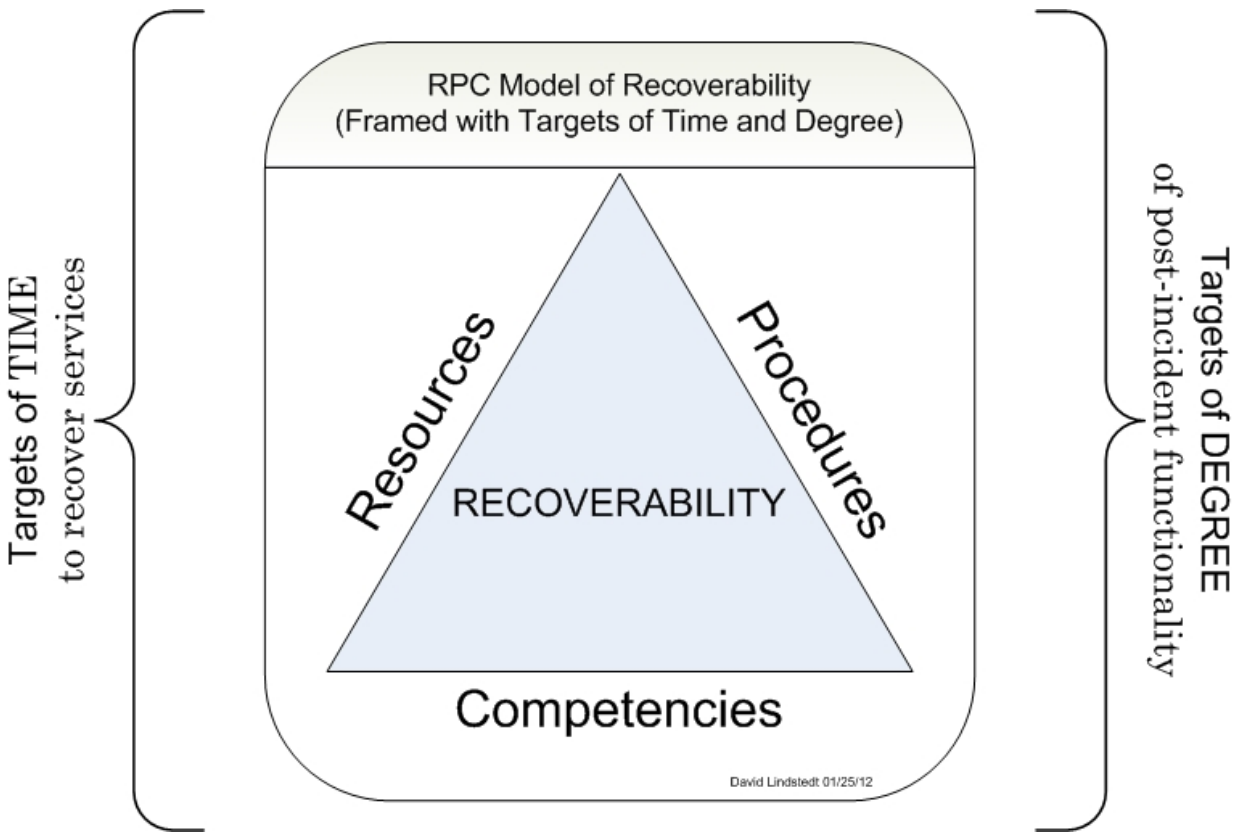
This question is difficult to answer in both theory and practice, but a proper approach can be determined.

The targets a unit sets for what and how quickly it will recover from a disaster are not necessarily the same as the current operation. A unit may plan on resuming only 50% of its current services and plan on taking a month to do so. Another unit may need to resume 90% of its operations within a matter of hours.

Hence, what it takes to be prepared to resume 50% of a unit's functionality in a month is likely going to be much less than what is needed to resume 90% of its operations within a matter of hours.[19] This provides further detail to the earlier principle that *recovery is always a matter of degree,* and leads to another principle of sorts:

(Recovery) preparedness must frame measurements within established recovery targets of degree and time.

This concept might be depicted as follows:

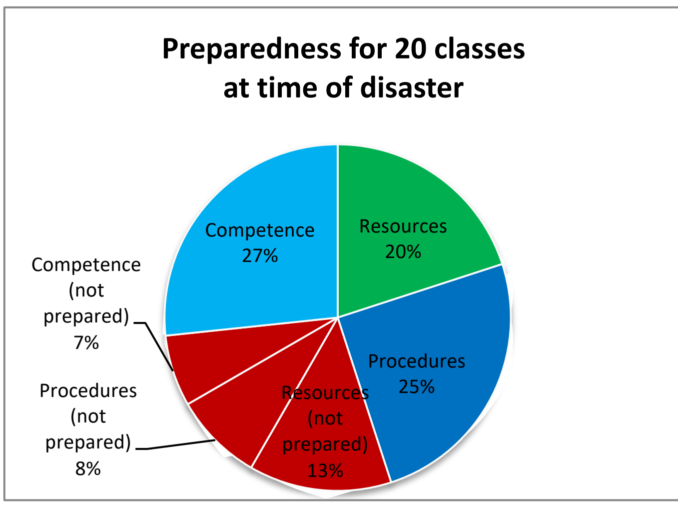


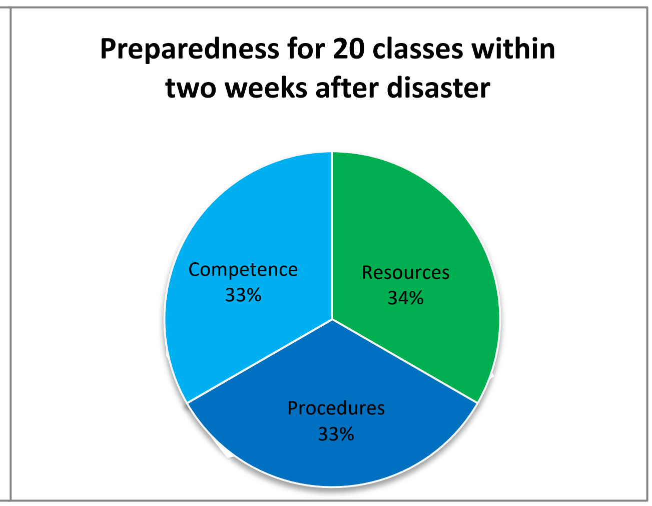
[19] As Brian A. Jackson succinctly puts it, "questions of speed, scope, and scale are critical…" Jackson, Brian A., "The Problem of Measuring Emergency Preparedness: The Need for Assessing 'Response Reliability' as part of Homeland Security Planning," Rand Corporation, 2008, p.4

In order to incorporate this principle into the model, one must be sure to measure against these targets of degree and time. For example, there is no need to measure preparedness of the entire organization at the exact time of disaster if management has already declared its objective of recovering only a few critical functions within the first 48 hours.

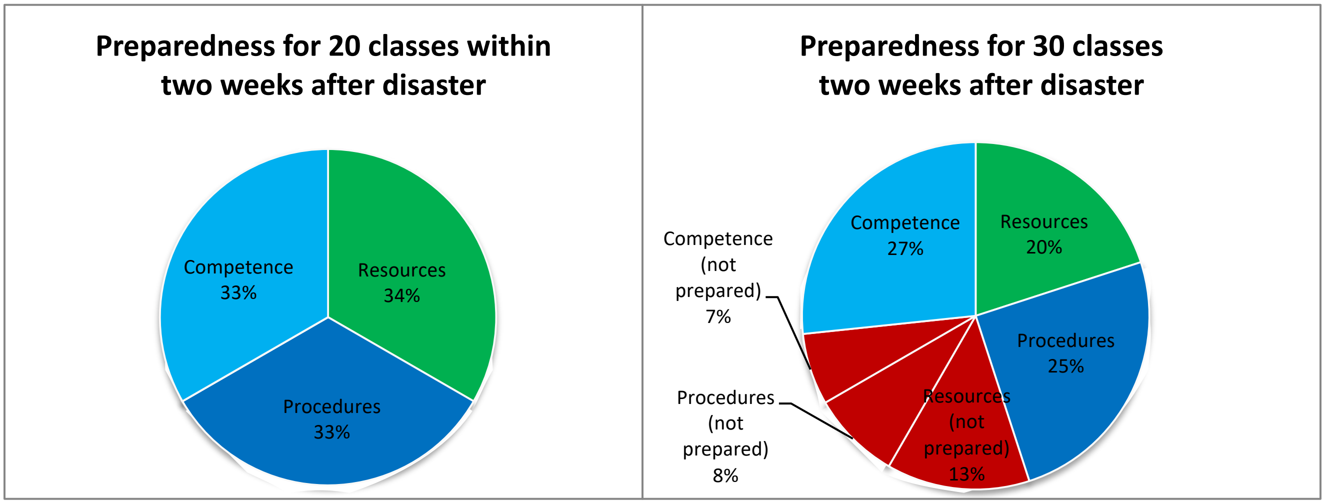
Thinking back to the example of the training department whose building was destroyed, the group was not able to recover classes right away; it took them two weeks before they could offer a majority of their classes. Suppose they recovered 20 of their 30 existing training classes within two weeks. One might say that they had only 25% of the resources (particularly classroom space), 25% of the procedures, and 50% of the competencies prepared to recover right away. Thus one might judge them to have been 33.3% prepared to recover 20 classes [measure of degree] at time of disaster [measure of time].

After a while, however, the instructional group was able to secure additional resources, create procedures, and build competencies to offer most of their classes. Thus, in two weeks [time], they might have 100%, 100%, and 100% of their RPCs respectively, and thus be 100% prepared to offer 20 classes [degree]. The measures might look like this:





Note that the measurement kept degree fixed and changed the point in time for the two measurements. This could have been reversed, fixing the time and asking the question, "How prepared are they to recover 20 classes in two weeks and also 30 classes in two weeks?" The resulting two measures might look like the following charts:



Alternately, the measurement could have changed both the degree and the time. Stakeholders may want to measure different degree and time targets for different types of scenarios.

Naturally, such measurement is going to be easier depending on the complexity of the subject, the degree of functionality to be recovered, and the number of time intervals. As such:

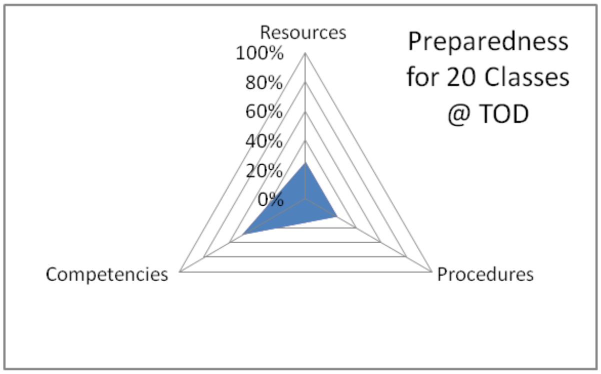
- Measuring an individual service will be easier than an entire organization.
- Measuring a quantifiable degree of functionality will be easier than non-quantifiable (e.g., 20 specific classes versus "educational excellence").
- Measuring for fewer intervals of time will be easier than many intervals of time (e.g., at one week and two weeks versus daily for three months).

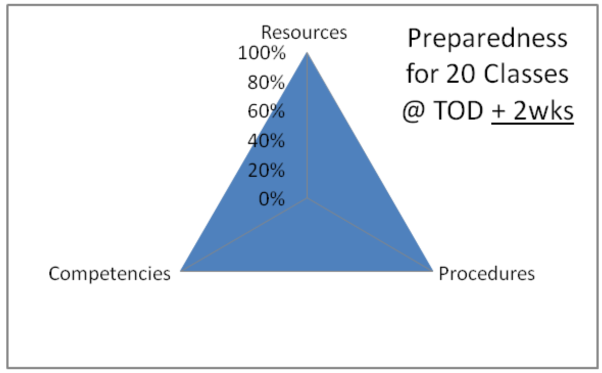
However, while measurements may be easier or harder depending on the complexity involved, they are indeed possible in both theory and practice.

For ease of explanation, the examples above were presented in pie charts. However, perhaps now is a good time to show that they are best presented within the volume of a triangle associated with the model.[20] To preserve the flow of the paper, the triangle diagrams will simply be presented here without annotation; for an annotated presentation, see Appendix B.

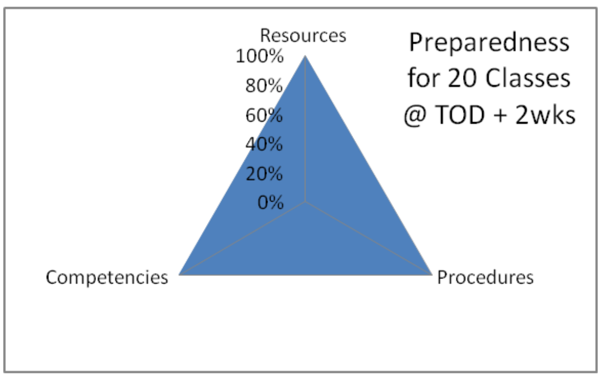
[20] One change – necessary to properly reflect the "volume" of each RPC factor within the full triangle – is that the factors have to be rotated and presented on the points instead of the sides of the triangles. Hopefully this small change does not prove a stumbling block.

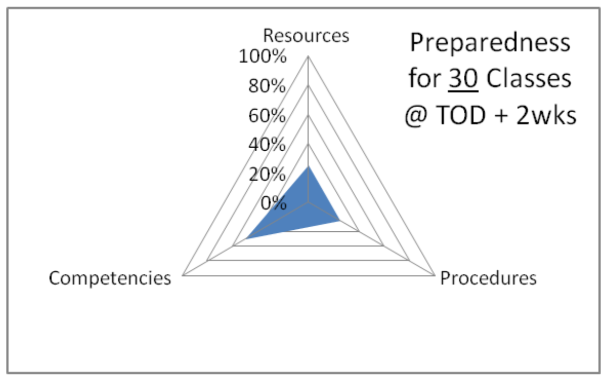
"Volume" Diagrams: Preparedness measurements with fixed degree and <u>different</u> time targets.





"Volume" Diagrams: Preparedness measurements with fixed time and <u>different</u> degree targets.





The math is not meant to be imposing and can be used to a degree of precision that is appropriate to the organization. It would be rather easy to use this model to quickly summarize a unit's level of recovery preparedness: "We estimate the unit has about half of the resources, half of the procedures, and most of the competencies needed to recover 75% of our operations within a week." Yet these equations are robust enough to provide critical measures of preparedness at any level of detail.

It would certainly be possible to identify the critical services within an organization, estimate the preparedness for each service given its targeted recovery degree and timeframe, and calculate all measures together for a combined measure of preparedness. A quick hotel example[21] at a high level might look like:

Reservations	R =	25%	**AP / AR**	R =	80%
(manage all reservations	P =	25%	(resume all AP / AR funct.	P =	60%
within 4 hours)	C =	65%	within 72 hours)	C =	90%
Catering	R =	75%	**Check In / Check Out**	R =	25%
(boxed lunches only	P =	75%	(manage all guests	P =	25%
within 24 hours)	C =	90%	within 4 hours)	C =	65%
Kitchen	R =	85%	**Valet**	R =	95%
(cold food only	P =	95%	(fully operational	P =	80%
within 24 hours)	C =	90%	within 2 weeks)	C =	80%
Laundry	R =	50%			
(turn 55 rooms	P =	50%	**Total Estimated Preparedness**		
within 24 hours)	C =	75%	**within degree and time targets:**		**67%**

These rather simple measurements could easily form the basis of important conversations with critical stakeholders.[22]

These measurements help explain another intuition held by many in the profession, namely that the act of planning (and exercising) is more important than having a physical plan.[23] This is due to the fact that procedures and competencies in particular will be vastly improved if more people spend time thinking about them. Procedures will be more fully developed and more accurately reflect what needs to happen if more subject matter experts are involved. Moreover, these procedures need to be known and internalized at time of incident; it will not do to have them pulled from a binder for the first time by the person needing to use them. A group is better able to identify a more complete set of required resources and will be more motivated to procure them ahead of time. And competencies can best be enhanced through actual experience and training to improve leadership, enhance performance, encourage teamwork, and increase crisis fortitude. Competencies are the least likely to benefit from a focus on documentation.

---

[21] One might object that, if the entire hotel was rendered unavailable, no services would need to be resumed. This is not the case under several circumstances, especially if the loss is temporary or the hotel is part of a chain. Further, under any circumstances, guest-related and business office services must be continued.

[22] For additional details and annotated modeling diagram, see Appendix A.

[23] As Jackson expresses it, “while two areas may both have a preparedness plan, there is a major difference between a high-quality plan that was carefully assembled and one that was produced merely to satisfy a requirement that has not been looked at since it was written.” Jackson, *ibid*, pp. 7-8.

The model can explain this intuition mathematically. One person working independently to create a plan might yield known and viable procedures something on the order of, say, 50% with no aid to existing competencies. Thus the measure of preparedness might be something like (50% + 50% + 50%) / 3 = 50%. But if a group of people brainstorm together, they are much more likely to identify and procure additional resources, create and learn better procedures, and improve their general post-disaster competencies, especially with a comprehensive exercise and additional training. Thus the final measure might be something like (75% + 80% + 70%) / 3 = 75%.

At the targeted time of recovery, an organization needs to have available resources, internalized procedures, and ingrained competencies.

The model helps explain the intuition that planning is more important than the physical plan.

Procedures and competencies will be vastly improved if more people spend more time thinking about them.

Procedures need to be known and internalized at time of incident; it will not do to have them pulled from a binder the first time a person needs to use them.

Competencies must be ingrained in individuals; they must solidly established before the crisis in order to bolster recovery efforts.

Section Four: The Relationship between Preparedness and Recoverability

We are not preparing to prepare; we are preparing to *recover*. This is critical because it leads us to the final, consequential questions of the paper: what is the relationship between preparedness and recoverability, and, can we predict recoverability based on preparedness?

One might be tempted to equate preparedness and recoverability, thinking that if a unit is 75% prepared to recover (within the targeted frame of degree and time), they are 75% recoverable. Or, put another way, it seems logical to guess that a unit which is 75% prepared to recover has a 75% chance of recovering.

Surprisingly, this is not so.

The problem comes with the realization that each of the factors of recoverability *interact* with the other two. Resources, procedures, and competencies are not silos and do not function independently of each other.

> *Each factor of recoverability <u>influences</u> the others. Resources, procedures, and competencies are not silos and do not function independently of each other.*

This can most easily be seen in extreme cases. For example, suppose a unit knows how it will do everything to recover and has the most competent staff imaginable. Yet they lose everything in a fire and have no additional capital. So, they score a 0% for resources and 100% for procedures and competencies. They average out to 66.6% preparedness, as (0% + 100% + 100%) / 3 = 66.6%. But, judging ahead of time, one would have said that they have no chance to recover from a total physical loss.

The measure of preparedness must not be the same as the predictor of recoverability.

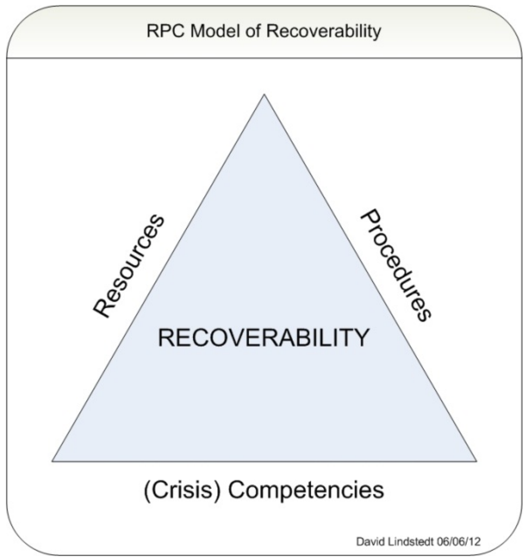
Take a more subtle example of a unit which has prepared, say, 75% of the necessary RPCs. The RPCs in this case might not "match up" to one another. Some existing procedures might need equipment that is part of the 25% of missing resources. Or the existing procedures might play on training and past experience (competencies) that is lacking. Or the majority of resources might be ready to go, but no one knows how to use them (procedures) or the people are too emotionally affected by the disaster to be of any help (competencies). The what, how, and way that a unit needs to recover all influence each other.

This brings us to another principle:

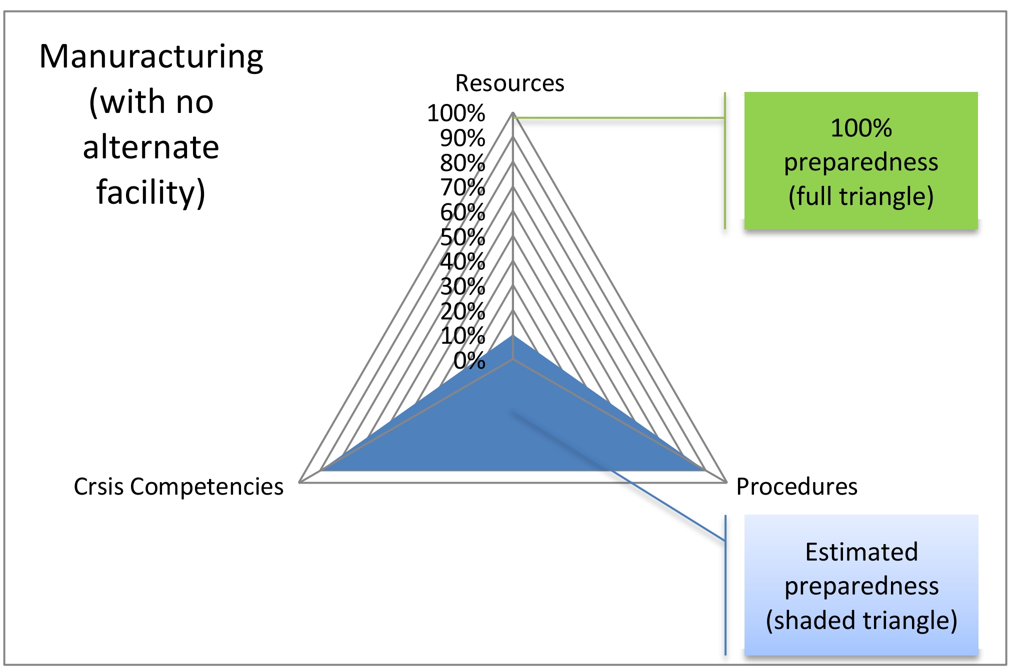
The factors of resources, procedures, and competencies influence one another.

But clearly there must be some relationship between (recovery) preparedness and recoverability? If there were not, then there would be no point in preparing to recover in the first place.

Perhaps the best way to visualize this is to return to our original model of recoverability:



Here is an extreme example, where only 10% of resources exist in comparison to 90% of both procedures and competencies. The area of recoverability might be depicted like this:



The area of recoverability is very small. Yet the measure of total preparedness is 63.3%. This small area of recoverability should match our intuition that a unit which has only 10% of the resources it needs to recover (including capital) is not likely to recover any time soon, if at all. We would predict that anything like full recoverability for this department is improbable.

Thus, at least the following deduction is possible:

A measure of preparedness does not equate to a prediction of recoverability.

A prediction of recoverability is impossible without the measure of preparedness.

It is important to note that such a prediction of recoverability is impossible without the measure of preparedness. Just because preparedness is not the same as recoverability does not mean that measuring preparedness becomes dispensable or inconsequential; it is essential to a prediction of recoverability.

The diagram above introduces yet another crucial point with the question: What is the area outside of actual recoverability yet inside the original dimensions of our triangle? The answer is <u>cost</u>.

If a unit wants to go from one degree of functionality at a given time to a higher degree of functionality at another time (before or after a disaster), it is going to cost:

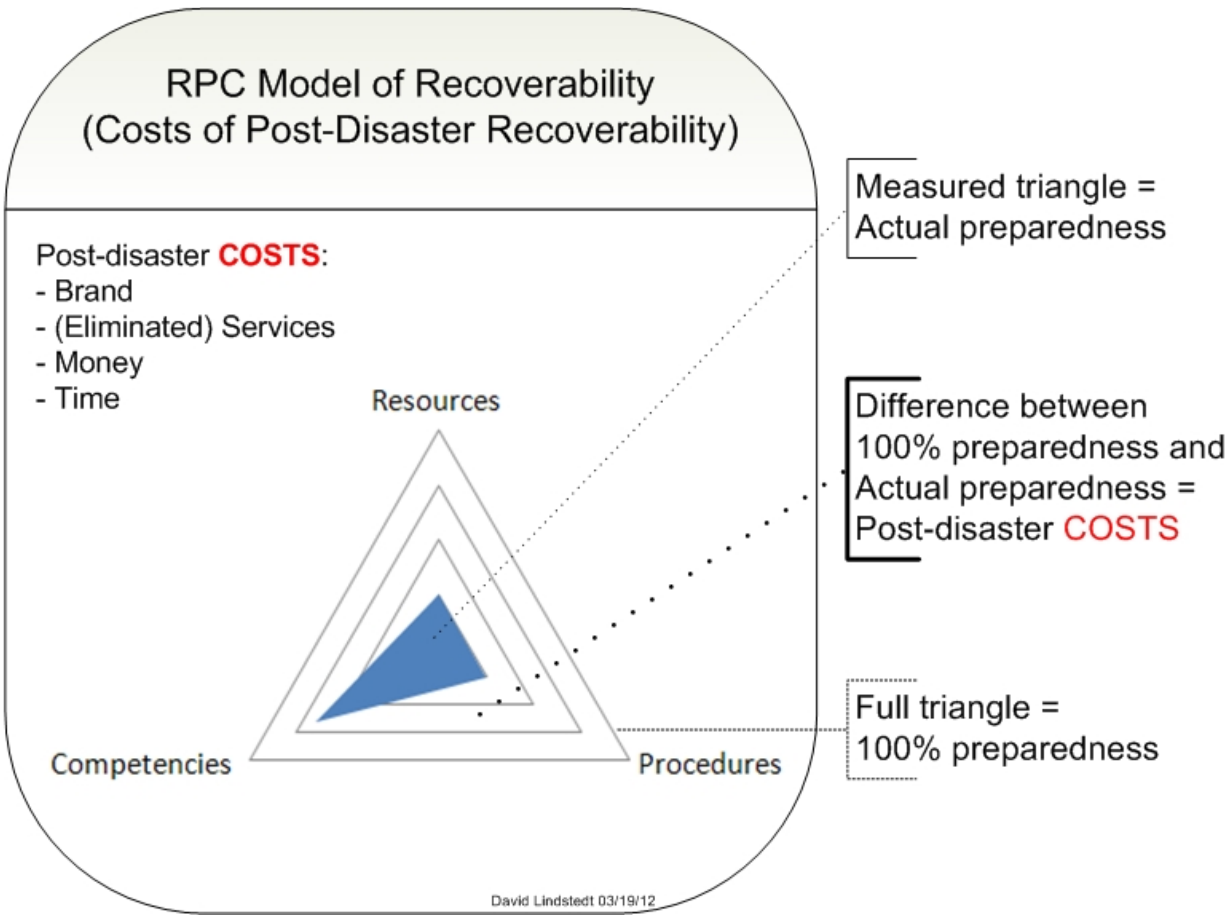
- Brand,
- (Eliminated) services,
- Money, and / or
- Time

Some examples:

- One week following the disaster, the manufacturing company is barely offering any services. Luckily, it finds a generous donor and a location to build again, though not to the size it once was; it will not be able to manufacture any item over one ton. In five months [time] and with a lot of donor investments [money], they are able to offer many, but not all, of their previous services [services]. Their reputation [brand] has suffered, and they are dropped by several of their customers.

- Two days following the disaster, the training department is not training anyone. It takes them several days [time] just to figure out the appropriate policies and procedures, not to mention identifying temporary classroom space. The organization will have to rebuild permanent space [money]. In addition, it is determined that 10 of their pre-existing courses will have to be cut [services], as either the proper equipment cannot be replaced or there is not enough available space. Enrollment for their department is down 17% the following year as many within the organization begin to question the need for any training courses [brand].

Costs within the framework diagram model might be depicted in this manner:



Thus, another principle is:

Moving to a higher degree of post-disaster recoverability will require costs in terms of brand, (eliminated) services, money, and/or time.

It seems likely that these costs increase over time. Consider the following simple examples:

Prior to Incident	Post Incident
– Maintaining a successful brand – Preparing service recovery strategies – Accumulating recovery equipment – Training staff to handle disasters	– Repairing a damaged brand – Cobbling together work-around tactics for minimal service – Procuring scarce recovery equipment – Motivating staff to recover services

There is not enough analysis specific to these recovery costs to plot a proper data curve. Some costs naturally increase sharply following a disaster then peak and return to previous levels. Other costs, such as brand, may increase linearly or exponentially with no hope of peaking and decreasing. At least it seems safe to say that the costs of preparedness will be significantly less than the costs of an unprepared recovery.

Section Five: Predicting Recoverability

Based on the model, can recoverability be predicted? With the type and amount of data currently available, a precise equation is impossible at this point in time. However, it is possible to propose a hypothesis for initial use and further study.

This paper proposes that there is a direct, mathematical relationship between the RPC factors. As an initial proposal, assume that each RPC factor influences each other with equal weight, which can then be expressed as such:

Recoverability = R x P x C

Let us consider some examples and begin with an extreme one. Imagine the theoretical case above where a unit has no resources (including capital) but all possible procedures and competencies. As noted, they average out to 66.6% preparedness yet one would have said that they have NO chance to recover from a total loss disaster. Instincts are right in this case, as the equation confirms that 0% x 100% x 100% = 0%. They had a 0% chance of recovering.

Take the manufacturing example, where they have 20% of the resources they need but perhaps as high as 90% of the procedures and 90% of the competencies they require. This gives them a measure of 66.6% preparedness, but it is easy to realize that having 20% of the necessary resources puts them at a great disadvantage. Indeed, 20% x 90% x 90% is only 16%. Perhaps anyone would have predicted that the company would be able to recover only roughly one-fifth of its former operations immediately following a disaster, and this rings true.[24]

Here is one final example. It is often stated in one way or another that 80% of businesses that undergo a major disaster never recover.[25] Let us take this to be true for now.[26] How can one explain the mere 20% recoverability rate? Assume that any given organization has roughly 50% of the resources, 50% of the procedures, and 75% of the competencies required to recover. This gives us 50% x 50% x 75% = 18.7% recoverability, very close to the stated 20% recoverability rate, especially accounting for the real costs of recovery over a

---

[24] This 16% may include payroll, HR, business office, sales, and other functions that can continue despite the cessation of manufacturing *per se*.

[25] See, for example: http://www.edwardsinformation.com/content/ImpactofDisaster.pdf, p. 4, viewed 10/05/11.

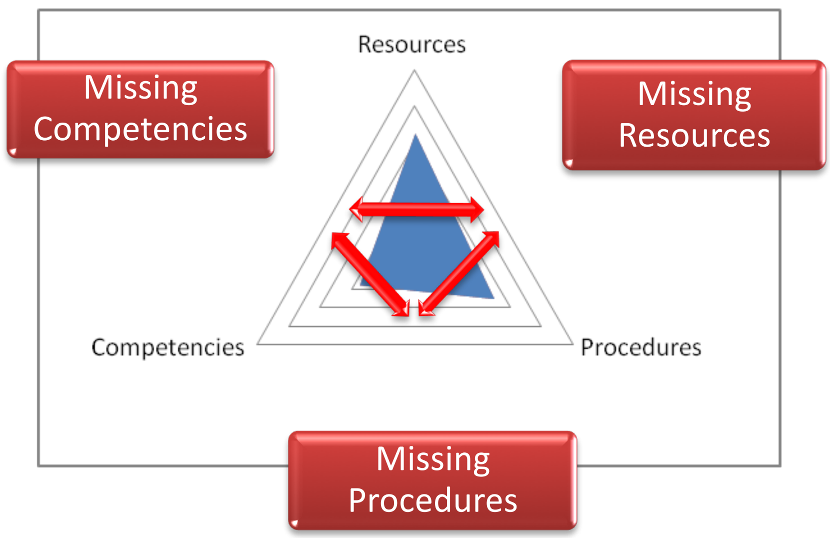
[26] It should be noted, however, that there does not appear to be any empirical evidence for this claim. See: Hiles, Andrew and Gosling, Mel, "SMEs – Stop the Preaching," www.rothstein.com/blog/smes-%e2%80%93-stop-the-preaching/, 2008, viewed 10/05/11, and "Business Continuity Statistics: Where myth meets fact," *Continuity Central*, April, 2009, www.continuitycentral.com/feature0660.html, viewed September, 2009. It is interesting to note signs that these potentially high estimates are coming down; the Red Cross, for example, recently cited the Insurance Information Institute, 2000, saying, "15-40 percent of businesses fail following a natural or manmade disaster." See: www.readyrating.org/Businesses/ReasonstoPrepare.aspx, viewed 10/05/11.

timeframe of several years. While analysts may well haggle over better and worse general estimates, this model's predictor of recoverability seems to fall in line with our intuitions.

Thus, the equation reflects the fact that the percentages of missing RPC factors each interact with each other, such that missing factors in one category compound the missing factors in another. This can be stated as:

Each factor of recoverability (R, P, and C) multiplies those factors which are not available at the targeted time of recovery.

The equation indicates the multiplicative nature of the three factors, and that improving (or neglecting) any one factor will have an influence on the other two as well as recoverability as a whole. Available RPCs might not "match up" to one another. A critical resource needed as the dependency of a procedure may be unavailable. The what, how, and way that a unit needs to recover all influence each other. A simple representation of the interactions might look like this.



Or it could be depicted in a dependency table:

Required Resource	Required Procedure	Required Competency	Outcome
✓	✓	✓	✓
✓	✓	X	X
X	✓	✓	X
✓	X	✓	X
✓	X	X	X
X	✓	X	X
X	X	✓	X

Naturally, however, the *Recoverability = R x P x C* equation may well prove to be too simple. It seems likely that each factor has its own influence and level of importance involved in the outcome of recovery. It may turn out that resources and competencies are more critical than procedures; thus future study may provide an improved equation that properly expresses each factor's criticality on recoverability, such as: *1.7R x 0.7P x 1.2C*. Consider this at the second level of the RPC model of recoverability, where a proper predictor could weight each of the causative factors. In this case, each sub-competency, for example, should have its own weight, resulting in a weighting of culture, experience, external relations, internal structure, leadership, and training.

It is time for some caveats and clarifications specifically regarding predicting recoverability.

The formula Recoverability = R x P x C is a working hypothesis in the truest sense of the term. It should serve as a starting point against which to predict recoverability and measure actual results. Occam's razor suggests that the formula should be kept simple from the beginning, though observed results will likely require developing a more complex formula. Empirical evidence over time will be necessary before a proper and more accurate equation can be developed. In this way, it is a matter of real discovery based on real events affecting real organizations.

An accurate predictor of organizational recoverability, applicable to every layer within an organization, should be a major goal of the continuity profession. With wide participation, it could be achieved within a decade. Should measurements become increasingly adopted throughout the discipline, a wide number and variety of real figures would be in place. As disasters befell organizations, data would be available to practitioners and researchers to examine, running parallel with the organization's actual recovery efforts over time.

Finally, while the model presents a way to predict the likelihood of an organization's recoverability from disaster, it does not inform us as to *whether* it should.

This important topic will perhaps serve as a fitting last note of context. All decisions about recovering a service, unit, or organization must naturally occur within a framework of strategic planning, business acumen, and common sense. The RPC model of organizational recoverability may be conceptual in nature, but it ought not to be divorced from a larger reality. As John Stagl shrewdly comments:

> One of the common fallacies in business continuity planning is the assumption that the duplication of an existing process or segment of an organization in and

> of itself reestablishes its inherent value to the organization. This assumption ignores the value projected to that organization by its clients and customers… An operation is "mission critical" only if it is instrumental in the accomplishment of organizational goals... After a disaster, it is possible that the competition in the market, local or global economics, customer values, and employee availability (just to name a few) have all changed. Any of these factors will redefine "mission critical" for a company's holistic operation.[27]

As was pointed out near the start of this paper, there are better and worse conditions under which an organization stays in business. Survivability, as well as recovery, cannot be an all-or-nothing prospect. In this way, executive leadership must apply their measures of preparedness and predictors of recoverability to the landscape in which they find themselves following a disaster.

[27] From John Stagl's 12/05/11 comments on an earlier draft of this paper (with my many thanks). It is important to note that Stagl is very skeptical of any model claiming to accurately predict recoverability. Not only does he strongly emphasize the role that management and ingenuity play in recovery, but he envisions all recovery efforts taking place within an environment so dynamic predictions are impossible. Stagl's cautions are an important context for discussions on recoverability; naturally, however, Stagl and I disagree on derived conclusions.

Section Six: Conclusions and Recommendations

While this conceptual model of recoverability is a critical first step, it is important to note that there is still much work to be done to flesh it out properly. The model establishes a framework for discussion and make improvements; it does not mean the work will be easy. Jackson states it nicely: "The reason most current efforts focus on things that can be counted is because that counting is comparatively easy – and assessment that goes beyond such input measures will be more difficult almost by definition."[28]

The type of analysis and investigation needed to further refine the model and its associated measurements might best be divided into four broad categories: [29]

1. Application: How can the model best be applied to any particular organization?
2. Conception: Are there improvements to be made to the conceptual framework of the model itself?
3. Discovery: What are the factors that most influence recoverability?
4. Technique: What are the best techniques to achieve the most appropriate measurements?

The remainder of this paper will briefly suggest some considerations in these categories. These considerations are not meant as an exhaustive list by any means but as a starting point for discussion and next steps.

Application

- Create effective ways to capture and share the results of measurements
- Develop a thorough questionnaire to measure preparedness for the first three tiers of RPC factors
- Develop overview and training materials to help stakeholders (at any level necessary) understand the importance and benefits of the model and its measurements and predict recoverability
- Develop specific templates and tools to aid in the application of the model and associated measurements
- Develop ways to transform the results of measurements into a gap analysis with specific recommendations for preparedness improvements

[28] Jackson, *ibid*, p. 21.

[29] While it is certain that critical discussions will, and should, revolve around the question of how best to *improve* recoverability, and while this paper suggests some answers to that question, it is not specifically within the immediate scope of this paper.

- Suggest ways to address the potential psychological impact of relatively high preparedness numbers leading to relatively low recoverability estimates (due to the multiplicative nature of the way RPC factors interact)

Conception

- Create collaborative initiatives, websites, conferences, and other methods by which members of the industry can invest their (limited) time investigating, discussing, and considering the model
- Determine whether the "dedication" of an individual[30] is properly accounted for in Light's conceptual model (and, thereby, within the factors of capabilities)
- Determine the most appropriate ways to account for both the weakness and strengths that "human systems" play in factoring into recoverability,[31] and whether that has an impact on the identified factors of competencies
- Determine the proper role of life safety, if any, within the model
- Fully elucidate the role that *capital* plays as a resource, given that it by itself is not a proper resource under this model (because such capital cannot immediately be utilized as a necessary resource in direct support of service recovery)
- Identify points of overlap and commonalities between this model and issue management as well as crisis / reputation management, including whether the model could be applied to cyber security incidents
- Consider any issues in applying the model to sub-disciplines of continuity planning such as supply chain preparedness and workforce continuity
- Conduct a literature review to identify additional supporting or conflicting research

Discovery

- Begin to measure RPCs before and after disasters in an effort to refine calculations and offer an accurate predictor of an organization's ability to recover from disaster
- Begin to determine the proper weighting of all sub-factors in the RPC recoverability equation; refine and test the improved equation
- Identify all existing RPC factors in third level categorizations
- Identify exceptions to RPC factors, if any
- Identify those elements of preparedness that provide the biggest return ("bang for the buck")
- Perform additional research to plot a proper data curve specific to the identified recovery costs; determine how different costs fluctuate over time (i.e., which costs increase in what ways over time following a disaster)

Technique

[30] I.e., whether the individual will remain at their station to assist the organization during recovery efforts.
[31] Jacson *ibid*, p. 16, paragraph 2.

- Address the critical issue of how to identify what is needed for 100% preparedness (given degree and time), that is, how to know when a service is, in fact, 100% prepared for recoverability
- Determine which situations would benefit from an application of the Delphi method (or other such methods) to assist in measurements
- Determine whether the physical area of disaster affects the measures in the model; in other words, is it necessary to set the scope of disaster to a specific, limited physical area in order to return accurate measurements of preparedness
- Identify nuances involved in measuring preparedness and recoverability at each level of units, areas, and organizations not only in terms of collections of services but also as holistic entities themselves
- In general, begin to refine the best ways to measure the more challenging factors of procedures and competencies
- Suggest ways to address the potential psychological tendency on the part of participants to over-estimate preparedness
- Consider the challenges of applying the model to a loss of staffing scenario, particularly separating out:
    - People as "only" a resource without any assumption of skill sets or abilities
    - Procedures that are not just documented but which must be well understood to those executing them
    - Competencies as capabilities and proficiencies

Future efforts along these lines may allow us one day to accurately predict an organization's ability to recover from disaster. Then perhaps we all could consciously and wisely prepare our communities to face the unexpected.

David Lindstedt is the Program Director for Enterprise Continuity Management at The Ohio State University, the largest university in the United States.

He and his staff partner with over 300 individual workgroups to perform and exercise business continuity planning.

Dr. Lindstedt has presented at numerous conferences and has published several articles in international journals.

He has taught continuity planning for Norwich University and currently serves on the editorial board for the *Journal of Business Continuity and Emergency Management*.

Special Recognition

I would like to express my special thanks to Christine Rueter for editing this paper.

I would also like to express my thanks to the following reviewers who took the time and effort to offer feedback on an earlier draft of this paper. Their responses served to make a stronger final product:

- Michael Carpenter, TOA Technologies
- Nathaniel Forbes, Forbes Calamity Prevention Pte. Ltd.
- Andrew Hiles, Kingswell International Ltd.
- Mike Janko, The Goodyear Tire & Rubber Co.
- Philip Oppenheim, Continuity Information Support Services
- John Orlando, Vertek Corporation
- Howard Pierpont, FEMA
- Peter Power, Visor Consultants (UK) Ltd.
- John Seibert, Nationwide Insurance
- Lisa Skalecki, First Solar, Inc.
- John Stagl, Belfor USA
- John Vargo, Resilient Organisations Research Group at University of Canterbury
- Scott W. Ream, Virtual Corporation, Inc.

--David Lindstedt

Appendix A: A Brief Discussion of Standards

While this paper has attempted to address several anticipated objections and issues, it seems important to address the following concern specifically:

There are already several standards and best practices in place, particularly ANSI / ASIS SPC.1, BS25999, DRII's Professional Practices, NFPA 1600, and Virtual Corporation's BCMM.

Does this introduce "just one more" standard?

The RPC model of recoverability does not attempt to replace these standards. It attempts to fill two important gaps: 1) measuring preparedness and predicting recoverability and 2) suggesting a way to structure a program focused exclusively on organizational recoverability. All existing standards employ a wide-ranging scope that focuses on resilience in broad-brush strokes, including continuity planning, crisis management, crisis communications, emergency operations, IT disaster recovery, life safety, and risk mitigation, among others. They focus on implementing a comprehensive program and auditing whether every component of that program has been established.

None of them focus specifically on the ability to recover services, individually and/or holistically, within the targets of time and degree following a physical or staffing loss. The remainder of this appendix briefly discusses how the RPC model begins to fill these two gaps.

Gap #1: Measuring preparedness and predicting recoverability

Most standards acknowledge the need for measuring preparedness activities. Some notable examples:

- ASIS SPC.1-2009 notes that the standard "provides guidance for organizations to develop their own specific performance criteria" (p. 1) and dictates in section 4.3.3 that "objectives and targets shall be measurable qualitatively and/or quantitatively…"
- BS 25999:2007's Management Review section calls for "techniques, products or procedures, which could be used in the organization to improve the BCMS performance and effectiveness."
- Carnegie Mellon's CERT® Resilience Management Model (V.1.0) SC:SG5:SP1 says to "Develop Testing Program and Standards."
- DRII Professional Practices 2003 Subject Area 8 says to "Verify that the [business continuity] Plans will prove effective by comparison with a suitable standard, and report results in a clear and concise manner." Section 8.B.4.a. says to "Develop [exercise

evaluation] criteria aligned with exercise objectives and scope [that is] (1) Measurable and quantitative."

- NFPA 1600 (2010) section 7.1 says that "The entity shall evaluate program plans, procedures, and capabilities through periodic testing and exercises."
- Section 7 of Virtual Corporation's BCMM looks for "The existence of business recovery plans for all critical business functions across the Enterprise," and several sections require "Test results showing that RTOs and RPOs are attainable."

But standards are lean on providing suggestions as to how these measurements might be achieved. As Brian A. Jackson of the Rand Corporation notes about NFPA 1600 and other standards:

> Although many of these standards lay out accepted criteria and frameworks for planning processes, in general, they do not include detailed guidance to fully evaluate the results of those planning efforts and to assess whether or not an area is prepared. They have also been characterized as "qualitative" and focusing on predominantly on written plans…[32]

Put into the position of calling for measurements but simultaneously being unable to offer ways to provide such measures, these standards are then forced to fall back on testing and exercising as the sole measure of preparedness and improvement. Quoting Jackson again: "The limits of many of the means of assessing preparedness have led to interest in the use of exercises… As a result, whether or not a plan has been exercised is frequently used as a proxy measure for assessing its preparedness value."[33]

> Exercises are done not to measure preparedness, but to improve it.

Yet, if business continuity exercises are actually conducted, few are reliable measures of recoverability.[34] Existing quantitative and qualitative measures of exercises are most often subjective and, like planning documents, usually measure the date of the last exercise, the number of participants, and its perceived value on behalf of the participants. Typically, exercises should be run not to measure preparedness but to improve it. If done well, exercises enhance competencies, lead to a stronger commitment to shared objectives, stress and help internalize procedures, and identify missing resources. As NFPA 1600 declares: "The fundamental purpose [of an exercise] is to improve implementation procedures."[35] Testing and exercises do not provide the appropriate tools needed for quantitative or qualitative measurement of preparedness.

[32] Jackson, *ibid*, p. 6.
[33] Jackson, *ibid*, p. 9.
[34] One notable exception would likely be: Full-scale IT DR exercises focusing specifically on IT system recovery.
[35] NFPA 1600, 2010 Edition, Section A.7.2, p. 1600-25.

In sum, most standards require the existence of business continuity plans or strategies but do not provide ways to examine their quality or effectiveness.

Gap #2: Suggesting a way to structure a program focused exclusively on recoverability

Current standards take an all-encompassing approach to plan for resilience and survivability. Yet they provide few recommendations specifically targeted at planning for recoverability as defined in this paper. Standards agree that a risk assessment and business impact analysis are necessary, but then are vague on how to use those results to perform the necessary preparedness planning. For example:

- ASIS SPC.1-2009 section 4.4.7 notes that, “It is the responsibility of the organization to develop (an) incident prevention, preparedness and response procedure(s) that suits its particular needs.” But as to how this should be done, it notes only that the organization should address, “Mitigation and response action(s) to be taken for different types of disruptive incident(s) or emergency situation(s)” (4.4.7.g).
- CERT® Resilience Management Model SC:SG3:SP2 says only to “Develop and Document Service Continuity Plans” with no supporting detail.
- DRII Professional Practices 2003 Subject Area 6, sections 5, 6, and 7, does a better job than most, but ultimately comes down to two suggestions for the practitioner: “recommend alternative ways to conduct when normal resources are available following a disaster” (5.c.1) and “recommend method/procedures to easily transfer business functions…” (5.c.2).
- NFPA 1600 (2010) takes only two sentences to describe Business Continuity and Recovery, the thrust of which is the recommendation to have a plan that identifies “personnel, procedures, and resources that are needed…” and which “provide[s] for restoration of functions , services, resources, facilities, programs, and infrastructure” (6.7.2).
- Virtual Corporation’s BCMM simply audits whether “All Departments/Business Units have implemented stand alone business continuity plans” and the “Existence of individual department business recovery strategy” (section 9).

In general terms, no existing standard explains how to plan for service recovery. In specific terms, no existing standard provides detail on how best to prepare for the ability to recover services, individually and/or holistically, within the targets of time and degree following a physical or staffing loss. The RPC model suggests how to fill this gap by showing ways that an approach could be developed around increasing the availability of the RPC factors, recommending some approaches over others.

Further, the model follows in the tradition of other sub-disciplines within the larger approach to resilience planning. Enterprise risk management, emergency management, IT

DR, cyber security, crisis communications, life safety, crisis management, and many other areas each have their own methodologies and measures. Continuity planning itself arguably has sub-disciplines such as:

- Business Impact Analysis (BIA)
- Supply Chain (Risk) Management
- Workforce Continuity

This model of recoverability follows an established precedent of creating and utilizing sub-disciplines within the field.

Yet it does not dictate implementation requirements. The model does not describe how to create or implement a continuity management program. It does not include important implementation aspects such as executive support, incorporation of lessons learned, or project management techniques. It serves as a model, not a project management guide or program implementation instructional guide.

The model does not need to take the place of any existing standard; its focus is specific and can be used in conjunction with existing (and future) standards.

In conclusion, then, there does not seem to be a particular danger that this model introduces "just one more" standard. It fills a gap in all existing standards. Indeed, from a high level, there is a critical need in the profession to clarify terms, narrow scope, and provide specific tools and measures for continuity practitioners. Additional research is needed to provide a firm foundation for each individual aspect of resilience planning, and service continuity planning in particular is perhaps the least proven. Moreover, there is an increasing demand from stakeholders to be able to answer the questions: "How effective are our preparedness efforts?" and "What is the likelihood we will recover from a disaster?"

Appendix B: Measuring and Predicting using the Hotel Example

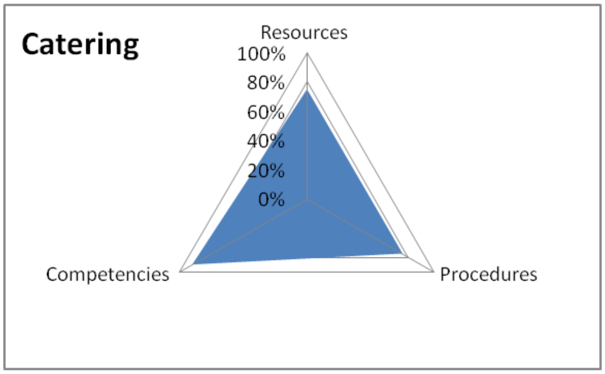
As the model of recoverability has now been fully outlined, it is possible to revisit and re-present the previous hotel example in a fuller context. In the paper, the measurements of preparedness of the hotel's services were charted in pie graph format. This format is acceptable, but perhaps better represented now within the RPC triangle, more clearly depicting each factor of resources, procedures, and competencies.

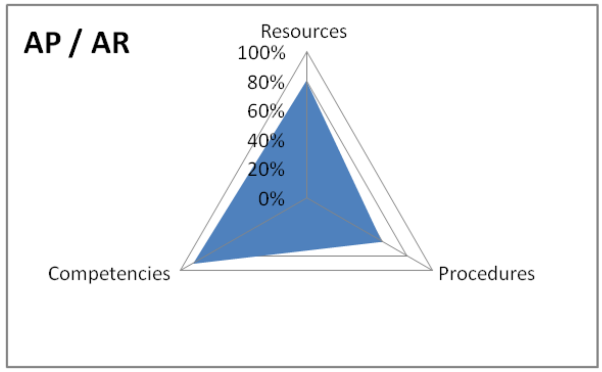
One change – necessary to properly reflect the "volume" of each RPC factor within the full triangle – is that the factors have to be rotated and presented on the points instead of the sides of the triangles. Hopefully this small change does not prove a stumbling block.

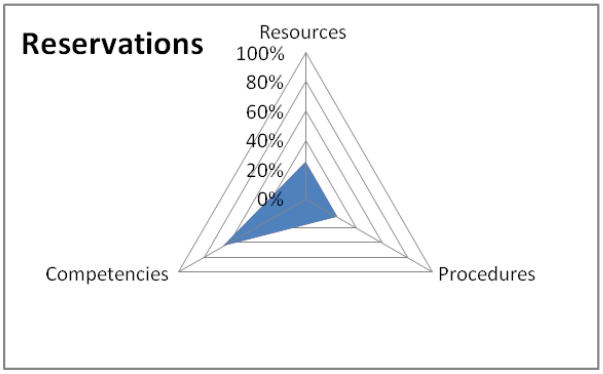
The original (hypothetical) measurement scores for each hotel service are also presented for convenient reference.

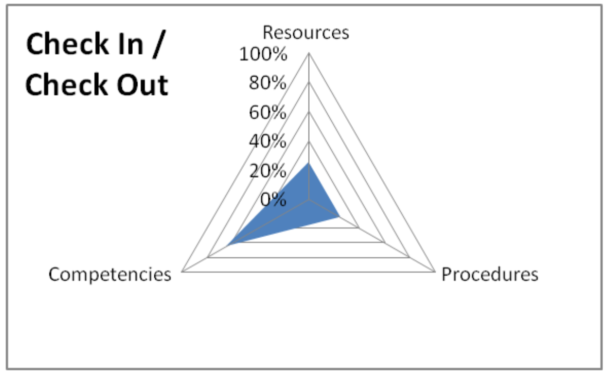
Finally, one "annotated" triangle is also presented by way of further explanation.

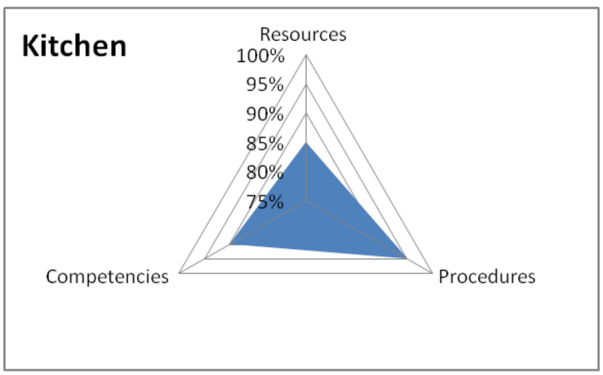
Reservations	R =	25%		**AP / AR**	R =	80%
(manage all reservations	P =	25%		(resume all AP / AR funct.	P =	60%
within 4 hours)	C =	65%		within 72 hours)	C =	90%
Catering	R =	75%		**Check In / Check Out**	R =	25%
(boxed lunches only	P =	75%		(manage all guests	P =	25%
within 24 hours)	C =	90%		within 4 hours)	C =	65%
Kitchen	R =	85%		**Valet**	R =	95%
(cold food only	P =	95%		(fully operational	P =	80%
within 24 hours)	C =	90%		within 2 weeks)	C =	80%
Laundry	R =	50%				
(turn 55 rooms	P =	50%		**Total Estimated Preparedness**		
within 24 hours)	C =	75%		**within degree and time targets:**		**67%**

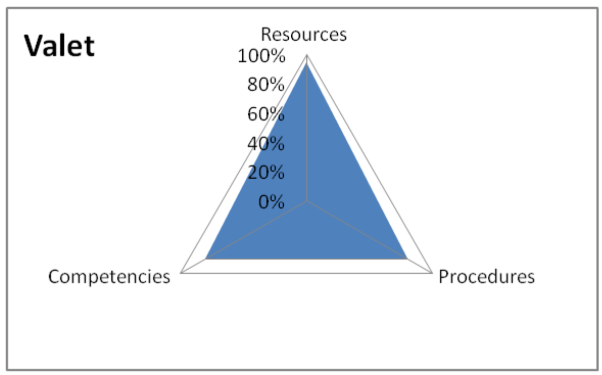


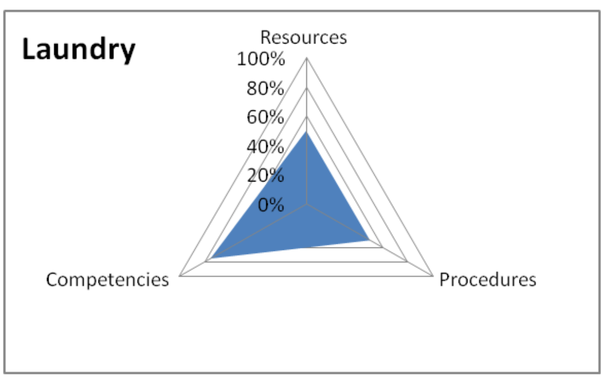


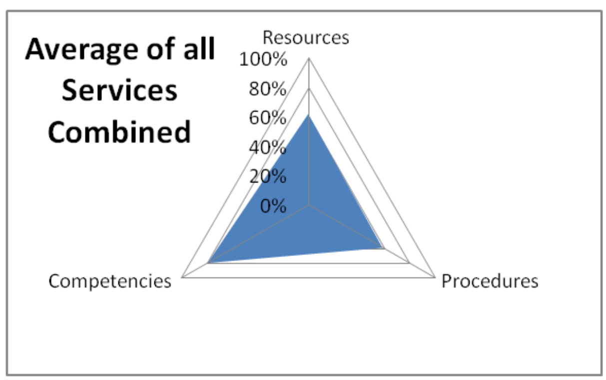












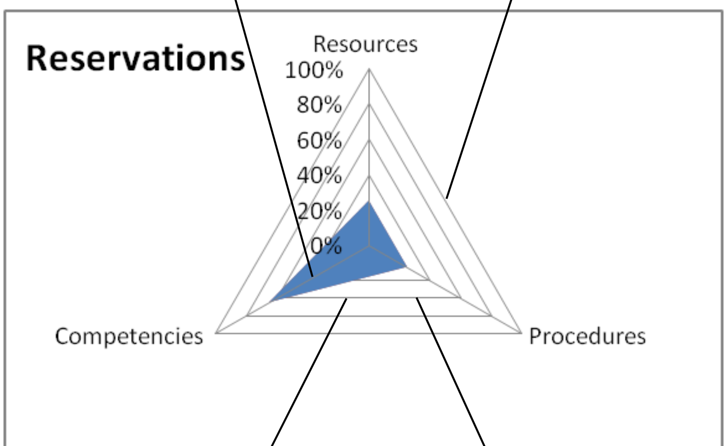
Total Estimated Preparedness	
within degree and time targets:	**67%**

Annotated Example: Measuring a Single Service

The "volume" of the smaller triangle represents the actual preparedness of RPC factors needed to recover the service.

The full triangle represents 100% of RPC factors needed to recover the service.

Time Target = Within 4 Hours



Degree Target = Manage all reservations*

All missing RPC factors interact with a multiplicative effect. Therefore, while (actual) *preparedness* is

(25+25+65) / 3 = 38.3%

(predicted) *recoverability* is

25 x 25 x 65 = 4%

The difference between the "volumes" of the two triangles represents the missing RPC factors required for 100% recoverability and will be borne out in terms of post-disaster costs:

- Brand
- (Eliminated) Services
- Money
- Time

*More detail, not shown here, would be necessary to ascertain the proper measurements of R, P, and C for this service. In short, what does it mean, specifically, to "manage all reservations"?