Resilience—A CONCEPT

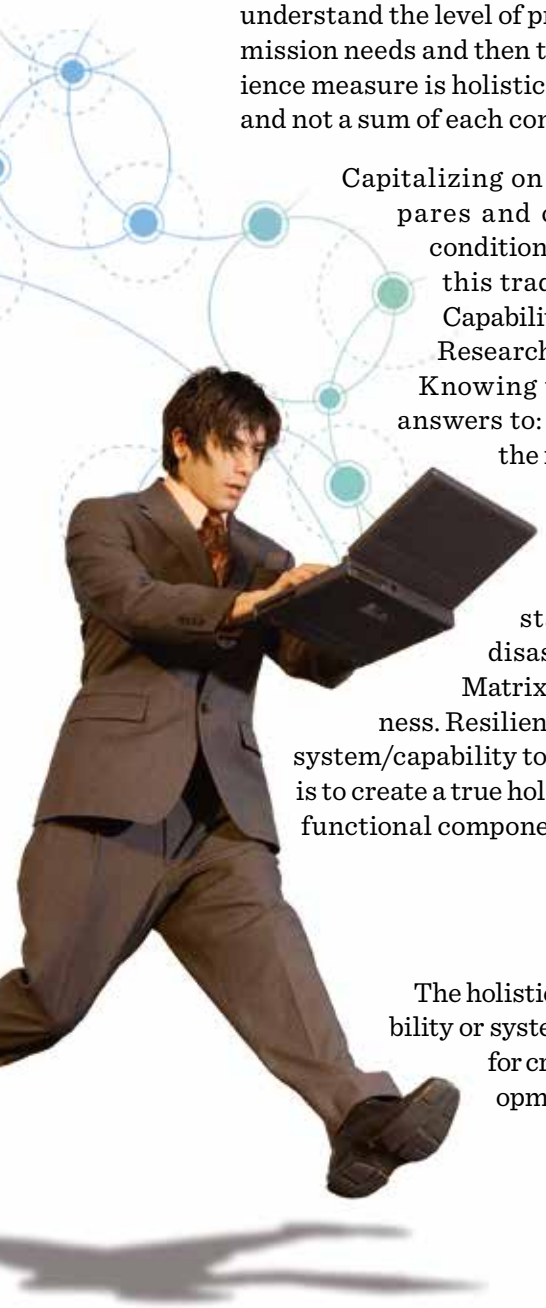
Col Dennis J. Rensel, USAF (Ret.)

Resilience takes on many definitions and ideas depending upon who is speaking. Taking this one step further, consider resiliency as a concept that provides a holistic view of a system or capability, just as biomedical indices provide an indication, a concept of a person's health. This process or concept of assessing one's health can be equated to the assessment of the health of a network or system. The hypothesis is: resiliency is meaningful in the context of holistic assessments of capabilities. At this level, comparisons of capabilities or systems can lead to informed decisions about resources, funding, and tradespaces. This article develops a Resiliency Tier Matrix and illustrates how to obtain a holistic view of resilience for a capability or system.

Keywords: resilience, health, holistic, Resiliency Tier, Resiliency Tier Matrix, State of Resiliency

Image designed by Diane Fleischer

Resilience as a term has as many definitions as people who talk about it. What if resiliency is treated as a concept? How do you measure a concept? In reviewing many definitions, "each [definition] ... rests on one or two essential aspects of resilience: continuity and recovery in the face of change" (Zolli & Healy, 2012, p. 7). A key to the success of any resiliency analysis is to fully understand the level of protection and tolerance that is acceptable to meet mission needs and then to create a strategic plan accordingly. A true resilience measure is holistic, viewing the whole of a robust mission capability and not a sum of each component's capability.



Capitalizing on this holistic view, the resulting analysis compares and contrasts various capabilities with different conditions, requirements, and operations. Working within this tradespace, analysis may lead to critical junctures: Capability vs. Cost, Improvements vs. New Development, or Research and Development Investments vs. Sustainment. Knowing the State of Resiliency of a system will lead to answers to: How can resiliency be improved? Where should the next dollar go? And when has a system reached its end of life? This information can lead to informed decisions and better capabilities.

Effective resiliency planning comes from understanding situational and mission needs before a disastrous event occurs. Developing a Resiliency Tier Matrix would capture this situational and mission awareness. Resiliency Tiers demonstrate acceptable tolerance for the system/capability to meet mission needs. A goal in this entire process is to create a true holistic Resiliency Index that reflects more than each functional component's contribution.

Hypothesis

The holistic analysis of resiliency provides insight into a capability or system's resilient characteristics and provides a means for creating informed decisions regarding funding, development, deployment, and mission accomplishment.

Purpose

This article presents resiliency as a concept that incorporates many other factors and elements and develops a Resiliency Tier Matrix for analysis purposes.

Scope

This article portrays resiliency as an overarching concept that affects capabilities and systems differently depending upon the situation. It develops a Resiliency Tier Matrix to provide a holistic view of what resilience means to that capability or system. The research was limited to recent articles on resiliency and various interpretations of resilience and its effects. The development of the Resiliency Tier Matrix involves the relationships between existing conditions and possible impacts to capabilities and systems. Use of the matrix provides decision makers with knowledge to make informed decisions. This article does not delve into resiliency associated with people or organizations because an abundance of literature already covers the many aspects of these two constructs.

Discussion

The word resiliency has no universally accepted definition. Many organizations have coined more than one definition. One of the more accepted definitions is from the Office of the Secretary of Defense (Policy) (Department of Defense, 2012):

> The ability of an architecture to support the functions necessary for mission success with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats, in spite of hostile action or adverse conditions. Resilience may leverage cross-domain or alternative government, commercial, or international capabilities. (p. 12)

Resilience is an overarching concept or an umbrella, which encompasses many other concepts, characteristics, or parameters. Each may have a major impact at any one time. This leads to the basic question of how the resiliency of a capability can be improved. Many synergies and forces play important roles. Turning to systems, resiliency incorporates many other metrics and

variables. Figure 1 shows the various parameters and techniques associated with resiliency. As a concept, no single metric does resiliency sufficient justice. When defining a specific metric, another aspect of resiliency surfaces. The first metric no longer fits because the emphasis shifted to the next aspect or dimension.

FIGURE 1. RESILIENCY UMBRELLA

Resiliency as a term applies to people, organizations, and items/systems. Information technology networks, ecological systems, social environments, and health conditions use the term. For each of these constructs, risks come from all directions: events, data operations, or even missions. Risks are generally more prevalent during events such as an adversarial attack or natural disaster or even from a series of minor incidents that add up. Preparation to meet these challenges would minimize exposure and provide faster reaction times. One means of minimizing effects would be to understand system vulnerabilities. Many of the ideas and concepts are taken from an IBM

paper on Business Resilience (IBM, 2009, p. 5). Even though the IBM article focuses on business and business management, a variation or derivation of its resiliency framework can be extended to systems and their environment.

The success of any assessment/estimation is situational awareness of all aspects of resiliency. It helps define the level of protection and tolerance that is acceptable. Appendix A describes a Resiliency Black Box and the interactions of the various parameters in Figure 1 under the Resiliency Umbrella. A strategic plan is needed to meet mission resiliency requirements. The implementation of such a plan comes with challenges: (a) assessing risk vs. cost – what level of vulnerability is tolerable? (b) viewing resilience as a strategic enabler, (c) developing a resilience culture, (d) assessing return on investment for resilience strategies (IBM, 2009, p. 7), and (e) linking capabilities to mission requirements. However, done correctly, the implementation could lead to informed decisions about tradespace and alternative actions beyond the technical solution.

Open literature discusses resiliency techniques. These seem to fall into three categories. The first category is human behavioral practices, social and societal impacts (The State of New York, 2013, p. 3), and application to systems-of-systems (Bodeau, Brtis, Graubart, & Salwen, 2013, p. 1). This category is outside the scope of this article. The second category illustrates approaches through case studies on how some communities increased their resilience within their environment. The third category provides an engineering framework for mapping goals to objectives to techniques. Figure 1 depicts many of these techniques, which lead into this Resiliency Tier development. The desired outcome is then to develop innovative measures to enhance resiliency similar to what the communities did in the second category.

In treating resiliency as a multidimensional concept, there needs to be a way to characterize it and still have some quantitative assessment. An analogy would be the status of a person's health, which is multidimensional. Numerous medical indices cover all aspects of health: temperature, weight, disease conditions, muscle tone, aging, etc. But when asked how healthy a person is, a general concept of what all the indices or parameters indicate is the appropriate answer. Resiliency can adopt the same construct. If resiliency of a system equates to the health of a person, then maybe there should be resiliency indices similar to health indices. Just like the health hazards that people experience, systems experience multiple attacks on their configurations. A specific health index addresses a specific health condition or set of related conditions. Depending upon the value and importance of the index, patients will spend their last dollar on a remedy. To obtain a cure,

patients need to learn the overall concept of their health. This is where assessment of the myriad of available health indices is invaluable in determining their state of health. Indeed, the decision may impact where patients choose to spend their health dollars. A similar analytical process can apply to systems or capabilities and their resiliency. The assessment of these various parameters or dimensions can determine a State of Resiliency and would lead to a holistic view of the system. This type of assessment informs budget, development, and/or deployment decisions.

There can be many indices describing resiliency, each emphasizing a different aspect. However, when asked how resilient a system or capability is, the answer should encompass the varied indications from the set of resiliency indices. If done correctly, this Resiliency Index would allow for comparisons of capabilities or systems within a tradespace. For purposes of this discussion, since the relationship between systems and capabilities is close, the rest of the article will concentrate on systems.

> ***As a management tool, the Resiliency Tier Framework offers a way to compare various programs, systems, and capabilities in terms of potential tradespace, cost savings, or capability optimization.***

In reviewing literature, we found many articles that discussed metrics for resiliency. The Defense Science Board Task Force built a notional dashboard-metric collection system (DoD, 2013, p. 13). This system, having maturity levels and designed metrics, supported cyber systems at a very detailed level. In contrast, IBM developed a Resilience Tier Framework (IBM, 2009, p. 14). This framework defines levels of resilience to match business-driven requirements. It spans all business units, services, and technologies. It provides the client a streamlined direction for building a resilient architecture. Ultimately, a true resilience measure is holistic, encompassing the operations, technology, and culture of an organization. In a variation of the IBM model, the Resiliency Tier Matrix in this article has five Resiliency Tiers ranging from Tier I, which is a total disaster, to Tier V, which is the gold standard. In this case, 12 different indices are spread across the five tiers to assess the overall resiliency of a system.

Any military capability encounters numerous hazards or risks from all directions. Examples of sources for these risks are events, system failures, or human error. These risks can be minor or major depending upon

the conditions. To minimize the effects, system users need to be aware of vulnerabilities and have mitigating actions in place. Effective preparations and actions involve a holistic approach with proactive processes and vigilant situational awareness for the unknown (IBM, 2009, p. 5). When system users develop this holistic view, an extensive analysis compares and contrasts various capabilities, different conditions, environments, mission requirements, and operations. Armed with this view, decision makers can make informed decisions regarding better capabilities and their use.

The tool to help determine a system's State of Resiliency is the Resiliency Tier Matrix or Framework, with varying tiers of resiliency. Before proceeding further, an explanation of a Resiliency Tier Matrix or Framework and how it is built is appropriate. Consider the spectrum of resiliency divided into five states. This spectrum ranges from the worst state of resiliency—exposed—through the states of confused, aware, and operational to the best state: capable (Table 1). Appendix B, Table B1, presents further descriptions equating these states to mission accomplishment and operations.

TABLE 1. RESILIENCY STATES VS. MISSION AND OPERATIONS

Exposed	No mission accomplishment	Ceases to function
Confused	Major mission impairment	Highly impeded
Aware	Minimal mission success	Minimal success
Operational	Effective mission success with difficulties	Effective
Capable	Mission success with no difficulties	Highly effective

The question now arises: How is a system placed in one of these states? Measurable criteria (parameters, techniques, or metrics) help in constructing the matrix. The key criteria are those that help define this multidimensional concept. This set of criteria includes system characterization, operator confidence in the system, effectiveness of the security precautions, continuity of operations, and preparedness. Appendix B, Table B2, further explains these criteria. Each of these can further be subdivided depending on the interest and the importance of any parameter in Figure 1, Resiliency Umbrella. The matrix begins to take shape in Table 2.

The intent of this framework is to produce a more complete picture of the system and the forces pulling on resiliency. As mentioned earlier, what may be important one day may not be important the next. This is a way to set up a score card and evaluate the resiliency of a system. The weighting of the criteria would be set according to the priorities of those criteria. In addition this framework also provides a means of analyzing vulnerabilities, evaluating tradespace, and comparing various courses of action. Some benefits (IBM, 2009, p. 11) for constructing such a framework are:

- Aligning capability directly to mission;
- Projecting potential resiliency investments;
- Improving risk mitigation and planning; and
- Enhancing preemptive vs. reactive management.

Some key challenges (IBM, 2009, p. 7) for constructing such a framework are:

- **Viewing resiliency as a strategic enabler.** Resiliency has strategic importance. A resiliency strategy would be a single, integrated plan embraced and executed by all parts of the organization. It would focus on delivering mission capability. It would be the catalyst to higher levels of performance. Drawing together the different components, the overall result would be greater than the parts alone. Senior leadership should be committed to a single resiliency strategy. This strategy aligns with organizational goals to provide a holistic approach over mission-wide systems (McLaren, 2009).
- **Defining the value of mission resiliency.** "Mission resiliency encompasses a proactive approach that systematically prepares for potential disruption as opposed to waiting for a disruptive event to occur" (Peake, Underbrink, & Potter, 2012, p. 31). Understanding resiliency in the mission environment is a significant step in system development and security. A resilient mission system is more capable and more adaptable than the tools used against it. Its value is in less complexity and cost of securing mission systems. "The focus on mission resilience extends the scope of past security practices while simultaneously honing in on mission-critical systems, networks, and processes" (Peake et al., 2012, p. 29).

TABLE 2. INITIAL FRAMEWORK FOR RESILIENCE						
Tiers / Criteria	*Priority Weighting*	V [Capable]	IV [Operational]	III [Aware]	II [Confusion]	I [Exposed]
Scale		1	2	3	4	5
System						
Confidence						
Security						
Continuity of Operations						
Preparedness						

- **Working with advanced technologies.** This provides the opportunity to assist in developing and integrating state-of-the-art solutions to meet time-critical needs. As an added benefit, it provides opportunities for proactive and independent research, analysis, testing, and prototype development to mission requirements.
- **Maintaining continuous availability of mission systems.** This type of system visibility leads to assuring uninterrupted availability of critical mission systems, without need for failover mechanisms or recovery operations.
- **Linking capabilities to mission requirements.** Building resilience into a system from the start requires an understanding of the mission, the environment, and potential risks. These systems are the capabilities that satisfy the mission requirements. Linking the capabilities and mission requirements and evaluating their effectiveness in a hostile environment should be done early in the life cycle of a program.

Using Resiliency Tiers in Defining an Architectural Approach

Resiliency Tiers define levels of resiliency to match mission requirements. Resiliency Tiers span all domains, services, or technologies and provide insight for building a resilient architecture. The intent is that this Resiliency Tier Framework provides an objective scale for the classification of mission requirements. This scale is a set of consistent concepts, measurements, or criteria applied to mission systems or capabilities. This set links technical resiliency requirements to capabilities. Mission resiliency requires an architectural approach spanning the breadth of military and government capabilities. Resiliency Tiers (IBM, 2009, p. 10) help to classify mission requirements by:

- Defining a broad continuum of mission resiliency requirements that apply to all processes, services, development, and missions;
- Linking those requirements to a set of technology criteria that address all capabilities and resources in the mission environment; and

- Providing technical characteristics, criteria, and metrics to measure mission resiliency expectations, and to monitor and manage ongoing operations.

This process develops an effective holistic Resiliency Index. The whole is greater than the sum of each functional component's contribution. This index may also help in identifying how to maximize the architecture and optimize investment.

> ***Mission resiliency requires an architectural approach spanning the breadth of military and government capabilities.***

Benefits of Resiliency Tiers

Defining, developing, and maintaining Resiliency Tiers and associated resilient capabilities have a number of benefits (IBM, 2009, p. 11), such as:

- Better mission-to-technology alignment;
- Clear rationalization of investments in resilient capabilities;
- Greater opportunities for improvements to risk planning, strategy, and architecture;
- More prescriptive management of the mission environment to achieve system-wide resiliency;
- Assistance in gap analysis across mission, service, and technology domains;
- Help in bridging the communications and planning gaps for mission continuity resiliency and planning; and
- Integration of mission requirements with a system-wide approach to achieve greater affordability.

As a management tool, the Resiliency Tier Framework offers a way to compare various programs, systems, and capabilities in terms of potential tradespace, cost savings, or capability optimization.

How Resiliency Tiers Are Used

The Resiliency Tier Framework supports every aspect of the mission system. In an analysis, this framework can address alignment of resiliency strategies with mission needs, can guide the mitigation of adverse actions, and can address all mission and system components.

These tiers are able to help conceptualize and align mission resiliency needs in multiple scenarios. Resiliency Tiers lead to a comprehensive picture of systems and vulnerabilities, and eventually an understanding of specific levels of service. Using this objective and quantitative approach, requirements definition and prioritization ensure that the resiliency objectives and acceptable costs are integral to the overall mission capability.

An organization can also use Resiliency Tiers for guidance to mitigate the potential or existing chaos caused by external forces. These tiers provide a framework for understanding the overall health of the mission area and systems. Similar to the IBM analysis, Resiliency Tiers can help reconcile mission resiliency requirements and guide the infrastructure requirements, architectural design decisions, and major initiatives that will be implemented to achieve the desired future resilient environment (IBM, 2009, p. 12).

Lastly, a tiered resiliency approach enables the warfighter to define a replicable and measurable framework that can address all mission components including weapon systems, force capabilities, and/or government actions (IBM, 2009, p. 13). It can provide a range of resiliency requirements as well as mitigating actions. In addition, the tiered resiliency approach may also apply to a wide range of government actions and resiliency mitigations such as diplomacy, technical redundancy, force structures, and economic measures.

Five Tiers of Resiliency

This framework has five tiers for resiliency estimation (Table 2). Each tier serves as a set of guidelines that specifies the characteristics commensurate with each tier condition for each of five criteria: System, Confidence, Security, Continuity of Operations, and Preparedness. These criteria span the five Resiliency Tiers (defined as *Capable* [V], *Operational* [IV], *Aware* [III], *Confusion* [II], and *Exposed* [I]). When taken as a range, the Resiliency Tiers translate into a conceptual view of the resiliency status of the overall mission system.

The criteria may be any number of parameters or techniques, which are important at the time. Table 3 is a representative example of a populated Table. (Appendix B, Table B3 has more details in developing this matrix.) For instance, Preparedness is one of those criteria. The *Capable* Resiliency Tier defines Preparedness as having a holistic approach to resiliency; whereas the *Operational* Resiliency Tier classifies this as having specific plans in place to address resiliency. Depending on the mission resiliency requirements, either level might provide adequate preparedness; however, the *Capable* Resiliency Tier provides a complete strategy for addressing resiliency. The holistic strategy for the *Capable* Resiliency Tier reduces the effects of outside forces to planned courses of action and continuous vigilance, whereas the *Exposed* Resiliency Tier provides no indication of preparedness for a hostile environment. Again, depending on mission requirements, any level may provide adequate resiliency; however, the *Capable* Resiliency Tier provides for the most complete level of Preparedness for mission-critical functions. A similar analysis is possible with each Criteria or row.

The outcome of this assessment defines a set of immediate actions to improve the resiliency of mission systems. Some actions would result in the development of a longer term, strategic roadmap of major initiatives that would help meet mission expectations for future applications.

Guidance on Scoring

When undertaking a resiliency assessment, the "how good" or "how bad" analysis addresses each criteria individually (National Patient Safety Agency, 2008, p. 14). This is a consequence of the mission environment. Consequence, in this context, means the condition or outcome of a mission capability in reaction to an outside force (National Patient Safety Agency, 2008, p. 4). Clearly, there may be more than one consequence for a single capability.

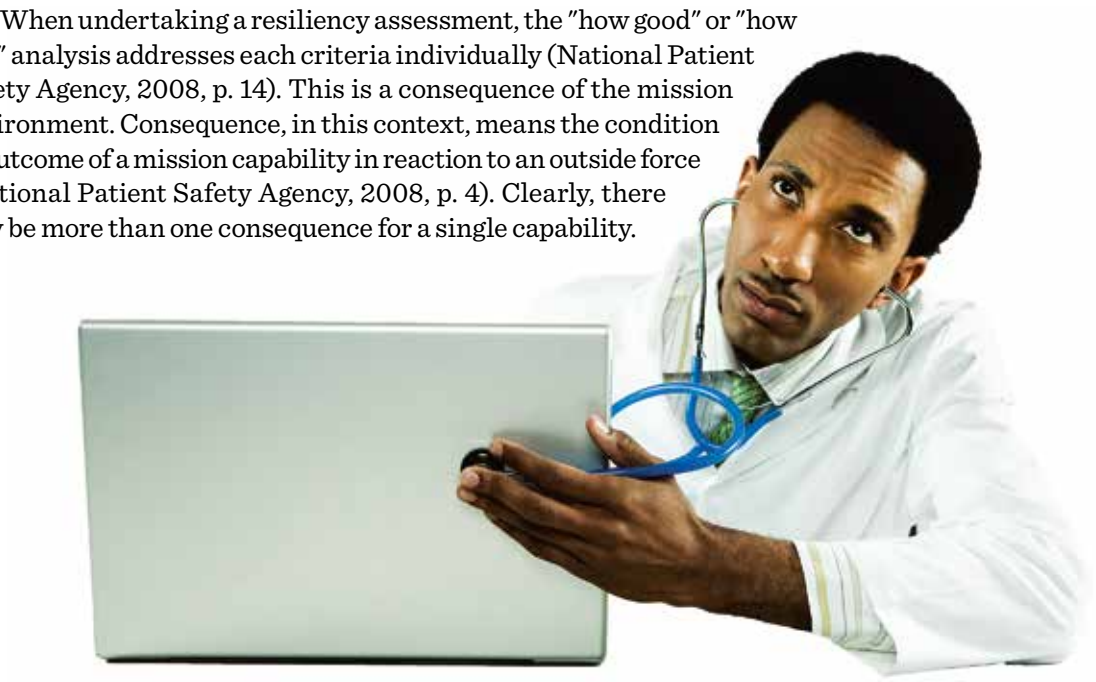


TABLE 3. TABLE OF RESILIENCY TIERS

Criteria \ Tiers		Priority Weighting	V [Capable]	IV [Operational]
Scale			*1*	*2*
SYSTEM	**Overview**		Highly capable	Effective
	Normal Operations		Full capabilities on-line	Maintains normal operations, reached new equilibrium
	Protection		Protected	Protection measures in place
	Corrective Actions		Cohesive actions among all players	Synergy of actions among most actors
	Vulnerabilities		Potential vulnerabilities identified	Know of most vulnerabilities
	Planning		Holistic resilience strategy	Resiliency measures
	Mitigations		Attacks have little or no effect on operations	Successful in mitigating or avoiding most attacks
	Vigilance		Method to identify new vulnerabilities	Addresses obvious vulnerabilities
Confidence			High	Moderate
Security			High	Effective
Continuity of Operations			Maximum	Able to operate effectively
Preparedness			Holistic strategy approach	Specific plans in place

BEST ←

TABLE 3. TABLE OF RESILIENCY TIERS, CONTINUED		
III	**II**	**I**
[Aware]	**[Confusion]**	**[Exposed]**
3	***4***	***5***
Minimum mission accomplished	Problems meeting any mission needs	Ineffective
Struggles to stay ahead of problems	Experiencing outages, delays, "blackouts," etc.—confused with anomalies	System failure, it crashes
Some protection available	"Band-aid" protection	No protection
Collaboration of effort to address issues	Attempting to resolve from within—disjointed actions	No clue what to do
Vulnerabilities exist	Few vulnerabilities known	Unaware of vulnerabilities
Realistic impact assessment	Minimal resiliency actions available	No resiliency designed in system
Some proactive measures in place	Reactive measures taken	No measures available
Aware of attacks	Can spell resiliency	Clueless
Medium	Low	Nonexistent
Appears to be adequate	Minimal with breaches	None
Barely meeting requirements	Failing	Complete breakdown
Minimal to acceptable	Insufficient	None

WORST

Qualitative and quantitative techniques assess and score the consequences. Wherever possible, consequences should use objective definitions across different criteria within each tier to ensure consistency in the process. Despite defining each condition as objectively as possible, scoring the consequences will inevitably involve a degree of subjectivity. Figure 2 contains the flow diagram for the Resiliency Tier assessment.

FIGURE 2. RESILIENCY TIER ASSESSMENT FLOW CHART

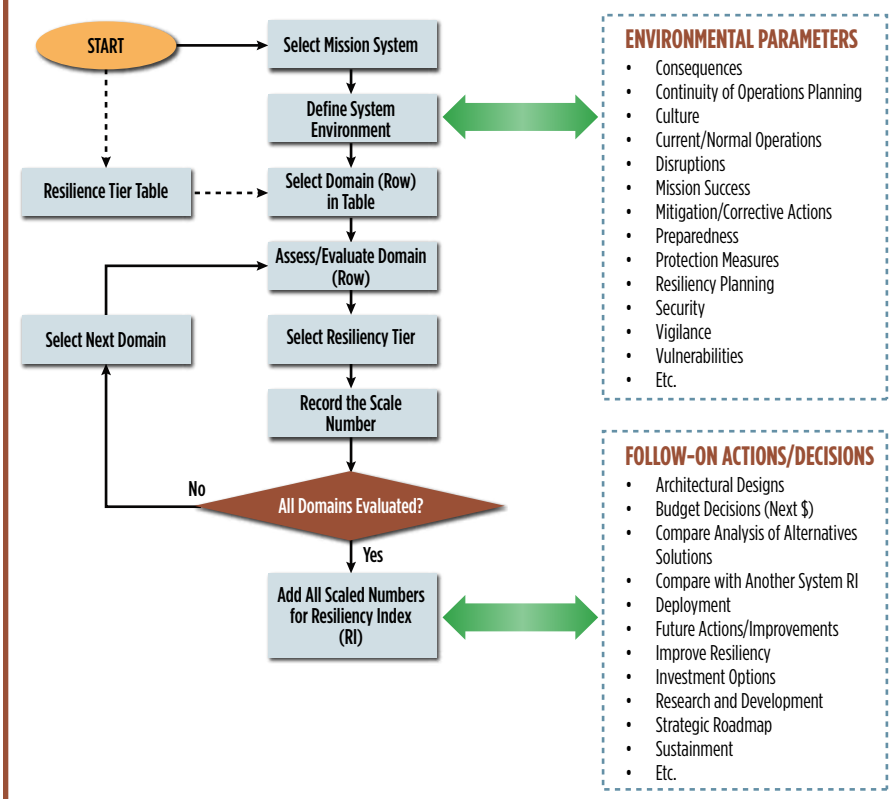


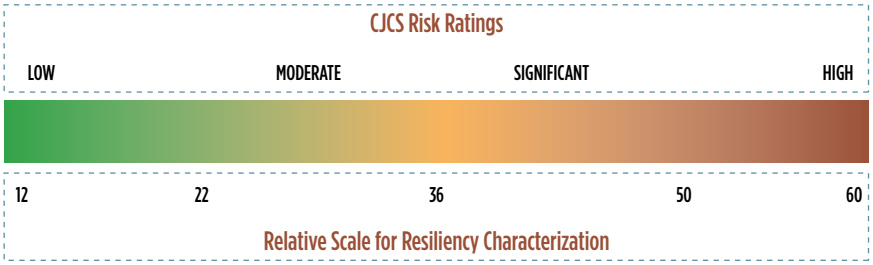
Table 3, Table of Resiliency Tiers, provides the framework to obtain an assessment of the State of Resiliency of a specific mission system. The process is:

- Select the mission system to review.
- Define explicitly the conditions (internally or externally) of the adverse consequences that are either encountered or might be encountered.

- Go to each row (criteria) in the table and identify the appropriate description, or tier, under the adverse condition. Appendix B contains further details for each term and description. Record the scale number at the top of each column. If a weighted value exists, multiply the scale number by the weighted value.
- Once all 12 rows are characterized, add all the scores based on the scale value (with or without weighted values) for each row. The total is the Resiliency Index.
- A variation to this table would be to change to another or different set of criteria or parameters. Add or delete a row. If one is added, establish the corresponding tier structure based on the new criteria. Keep modifications to a minimum. One of the benefits to having a set of criteria is the aspect of consistency in application.

This provides an overall resiliency assessment of the system: the greater the score, the lower the resiliency. The scores for this Resiliency Tier Framework (no weighting) would range from 12 (the best) to 60 (the worst). Putting these scores into perspective, compare them to the Chairman of the Joint Chiefs of Staff (CJCS) risk scale as part of the CJCS Resiliency Risk Spectrum (Figure 3).

FIGURE 3. RESILIENCY RISK SPECTRUM



The following is an example of how this Resiliency Tier Matrix is applied to a specific situation and system. Assume a large satellite terminal is located on foreign soil. The Status of Forces Agreement states physical protection is the responsibility of the host nation. Further, this terminal is vintage equipment nearing end of life. A local protest breaks out and the satellite signal is lost for the first time. After working with higher headquarters and taking approved mitigating actions, the maintenance crew restores the system to

Defense ARJ, July 2015, Vol. 22 No. 3 : 294–324

FIGURE 4. RESILIENCY ASSESSMENT EXAMPLE

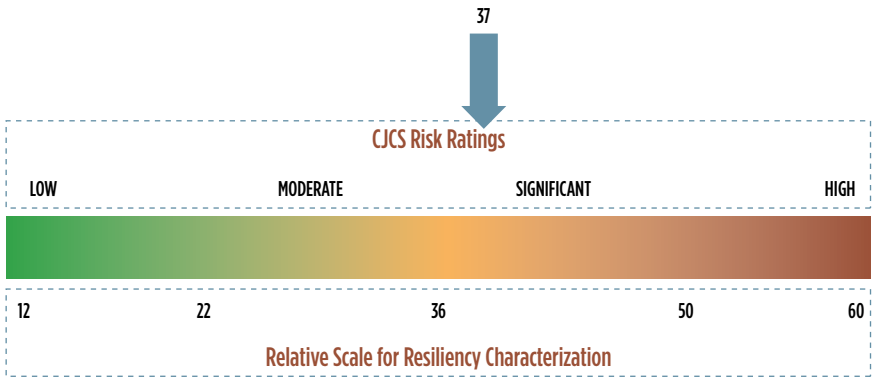
Domains \ Tiers		V [Capable]	IV [Operational]	III [Aware]	II [Confusion]	I [Exposed]
Scale		*1*	*2*	*3*	*4*	*5*
SYSTEM	Overview				■	
	Normal Operations			■		
	Protection				■	
	Corrective Actions		■			
	Vulnerabilities			■		
	Planning				■	
	Mitigations		■			
	Vigilance			■		
Confidence				■		
Security				■		
Continuity of Operations				■		
Preparedness				■		
Index = 37 →		**0**	**4**	**21**	**12**	**0**

full operational status within appropriate restoration time frames. Once all activities return to normal, the resiliency assessment (Figure 4) uses Table 3, highlighting the applicable tiers for each criteria within the Resiliency Tier Framework. Refer to Table 3 for the cell descriptions.

The sum of the respective scale numbers is 37. This number is displayed above the scale in Figure 5. An interpretation of this State of Resiliency would indicate:

- Increased system protection is imperative.
- Better planning for such events is necessary.
- Known vulnerabilities need more attention.
- The system is getting old.

FIGURE 5. RESILIENCY RISK SPECTRUM—STATE OF RESILIENCE



These four items would lead to a cost analysis of whether to upgrade or replace the system. They may also lead to a political discussion on the Status of Forces Agreement or whether or not the site should remain in its current location. Looking at a variation of the situation above where the terminal never goes down, discussions would be much different. Many of the cell evaluations in Figure 4 would move to the left.

This is a single application for illustration purposes; however, other options could be to maximize architectural designs, optimize investments, and differentiate resiliency between two systems supporting the same mission or among analysis of alternatives solutions. The analysis can be as rigorous as necessary with all details, a subset of details, or limited details depending on the purpose and desired outcome.

Summary

The tiered approach to resiliency can aid in planning for adverse or intrusive events proactively. This helps maximize return on investment from assets, technology, and people at the time when needed most. Using Resiliency Tiers to develop effective long-term strategies ensures that shorter term tactical actions are properly aligned and supports a military capability progress along the resiliency maturity continuum. Investing in resiliency measures at the program start will help make sure that long-term resiliency investments preserve value over time.

References

Black Box Model. (n.d.). *Investopedia* [Online investment dictionary]. Retrieved from http://www.investopedia.com/terms/b/blackbox.asp

Bodeau, D., Brtis, J., Graubart, R., & Salwen, J. (2013). *Resiliency techniques for systems-of-systems* (Report No. 13-3513). Bedford, MA: The MITRE Corporation.

Confidence, (n.d.). In *Oxford dictionaries* [Online dictionary].

Department of Defense. (2012). *Space policy* (DoDD 3100.10). Washington, DC: Office of the Secretary of Defense (Policy).

Department of Defense. (2013). *Task force report: Resilient military systems and the advanced cyber threat.* Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

Holistic Strategy Approach. (n.d.). In *BusinessDictionary.com* [Online business dictionary]. Retrieved from http://www.businessdictionary.com/definition/

IBM Business Continuity and Resiliency Services. (2009). *Business resilience: The best defense is a good offense: Develop a best practices strategy using a tiered approach.* Somers, NY: Author.

Joint Chiefs of Staff. (2010). *Department of Defense dictionary of military and associated terms* (Joint Publication 1-02). Washington, DC: Author.

Joint Chiefs of Staff. (2011). *Joint operations* (Joint Publication 3-0). Washington, DC: Author.

McLaren, S. (2009). *EPMO: A strategic enabler?* [Discussion paper]. St. Kilda, Victoria, Australia: Dignus Group.

National Patient Safety Agency. (2008). *A risk matrix for risk managers.* National Health Service. London, England: Author.

Peake, C., Underbrink, A., & Potter, A. (2012, September/October). Cyber mission resilience mission assurance in the cyber ecosystem. *CrossTalk, 25*(5), 29–34.

Preparedness. (n.d.) In *Oxford dictionaries* [Online dictionary].

The State of New York. (2013). *Community resilience techniques.* New York: My Rising Communities.

The White House, Office of the Press Secretary. (2007). *Directive on national continuity policy* (Reports No. NSPD-51 & HSPD-20). Retrieved from http://policy.defense.gov/portals/11/Documents/hdasa/references/HSPD-20.pdf

Wang, W. (2009). *A hierarchical analysis of terrestrial ecosystem model Biome-BGC: Equilibrium analysis and model calibration* (Manuscript draft). Elsevier Editorial System™ for Ecological Modeling. Retrieved from http://ecocast.arc.nasa.gov/pubs/pdfs/2009/ECOMOD-S-08-00413.fdf

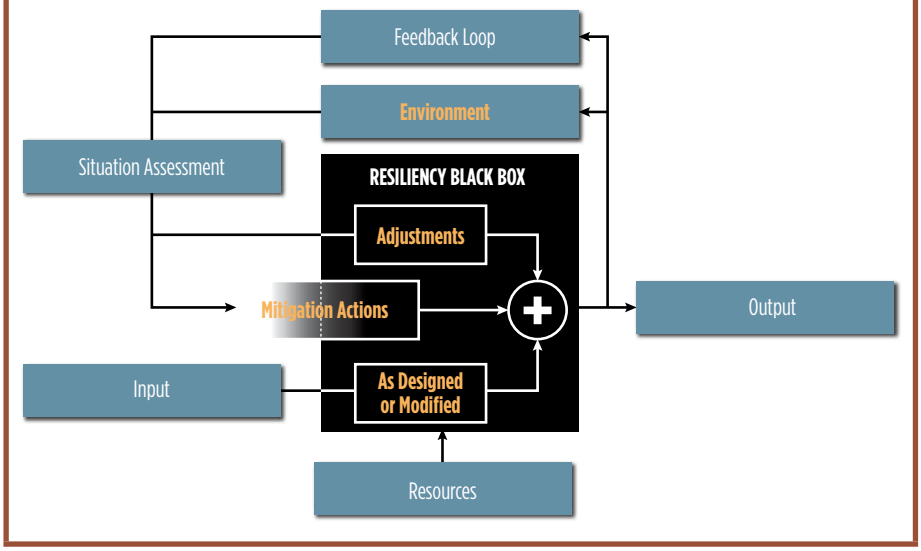
Zolli, A., & Healy, A. M. (2012). *Resilience: Why things bounce back.* New York, NY: Simon & Schuster.

Appendix A

Resiliency Black Box

In viewing the various parameters of Figure 1, Resiliency Umbrella, resiliency as a concept has many moving parts, elements, and metrics or components. At any one time, any of these can be a driving force for change. The result of that change could be a new equilibrium of interaction and collaboration. One way to visualize this interaction is to see resiliency as a black box. It has inputs (data, resources, and feedback) and has an output. In a more strict sense, a "black box" analysis "of [a] system contains formulas and calculations that the user does not see … to use the system. Black box systems are often used to determine optimal trading practices [in investments]" (Black Box Model, n.d.). In this case, the Resiliency Black Box Model depicted in Figure A-1 illustrates how the various inputs—Adjustments, Mitigation Actions, and As Designed or Modified (internally) and Environment (externally)—when altered, can reach a new system equilibrium or resiliency state. Putting it another way, equilibrium … refers to a steady status in which model state variables reach a dynamical balance (Wang, 2009, p. 9). This dynamic balance could result in a system achieving a reasonable, acceptable, or tolerable resiliency state. All the parameters contribute to the system equilibrium, whether new or a return to the previous state. The mission planner must assess the new resiliency state. If the resiliency state is unacceptable, a resiliency analysis needs to be accomplished to determine the best course of action that has a holistic effect on the system.

FIGURE A1. RESILIENCY "BLACK BOX" MODEL DIAGRAM



Generally, systems operate under two states: benign and hostile. The evaluation of these states occurs in the "Situation Assessment" block. Use the parameters, conditions, and/or metrics from Figure 1 to define and evaluate effectiveness. Pulling all of these together helps develop a Resiliency Index.

TABLE A2. DESCRIPTION OF THE DOMAINS

Criteria	Description
Scale	The measure of "how good" or "how bad" a system is relative to the Resiliency Tiers.
System	A functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements. (Joints Chiefs of Staff, 2011, p. GL-17)
Confidence	The feeling or belief that one can rely on someone or something; firm trust. (Oxford Dictionary, online reference)
Security	Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 1-02, page 226, 8 November 2010).
Continuity of Operations	The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. (Joint Chiefs of Staff, 2010, p. 54)
Preparedness	A state of readiness, especially for war. (Oxford Dictionary, online reference)

TABLE A3. DESCRIPTION OF TABLE ELEMENTS

Criteria		Tier	Tier Description	Tier Explanation
Scale			1-5	This is an attempt to quantify the current condition of a system or capability. The lower the score the more resilient a system or capability is.
SYSTEM	**Overview**	V	Highly capable	System is highly capable of completing the mission.
		IV	Effective	System experiences some minor problems but effectively accomplishes the mission.
		III	Minimum mission accomplished	System is struggling to meet mission minimum requirements.
		II	Problems meeting any mission needs	System can't meet most mission requirements, is distracted by problems, and cannot keep up with mitigating actions.
		I	Ineffective	System cannot meet mission requirements. Problems have the system on the verge of collapsing.
	Normal Operations	V	Full capabilities on-line	System is running all subsystems, processes and applications with no problems.
		IV	Maintains normal operations, reaches new equilibrium	System is running normal operations; however, it is continuously adjusting for disruptions. Each adjustment allows the system to reach a new equilibrium of operations.
		III	Struggles to stay ahead of problems	System cannot maintain mission accomplishment. It is struggling to stay ahead of the disruptions. Subsystems, processes, and applications are failing.
		II	Experiencing outages, delays, "blackouts," etc. —confused with anomalies	System is spending more time addressing disruptions than accomplishing the mission. The outages, delays, and disruptions are a distraction to the mission. Anomalies present no easy problems.
		I	System failure, it crashes	System crashes or is near to crashing under the weight of disruptions.

TABLE A3. DESCRIPTION OF TABLE ELEMENTS, CONTINUED

Criteria		Tier	Tier Description	Tier Explanation
SYSTEM	Protection	V	Protected	System-wide protection has proactive processes in identifying and mitigating disruptions. System is alert to new disruptions and puts corrective measures in place immediately.
		IV	Protection measures in place	System has many protective measures in place. It is not totally proactive in its corrective action. However, it is able to identify problems and react appropriately and swiftly.
		III	Some protection available	System has elementary protection measures. Primary mode of correction is reactionary to disruptions. Little time is available to be proactive.
		II	'Band-Aid' protection	No system-wide protection in place. Disruptions circumvent any protection measures attempted. Fixes turn out to be band-aids addressing symptoms and not causes.
		I	No protection	System has little or no protection at all.
	Corrective Actions	V	Cohesive actions among all players	When disruptions occur, there is a single focused team across the organization addressing any disruptions.
		IV	Synergy of actions among most actors	Pockets of excellence pop up throughout the organization to address any disruptions. There is a coordinated synergy among all actions taken. The effectiveness of these actions is greater than the sum of the individual actions.
		III	Collaboration of effort to address issues	There is a collaborative effort to address disruptions. This effort is initiated by the most affected subsystem or process or application. Coordination is not readily obtained. It takes time to address issues.
		II	Attempting to resolve from within—disjointed actions	Individual offices work independent of each other in attempting to solve any issues. In some cases it is counterproductive.
		I	No clue what to do	Little or no effort is put forward to address disruptions.

TABLE A3. DESCRIPTION OF TABLE ELEMENTS, CONTINUED

Criteria		Tier	Tier Description	Tier Explanation
SYSTEM	Vulnerabilities	V	Potential vulnerabilities identified	System is aware of all vulnerabilities, has a means of identifying new vulnerabilities, and is able to project vulnerabilities that result from new technology development.
		IV	Know of most vulnerabilities	System knows of its primary vulnerabilities and can sense new vulnerabilities as they manifest themselves. System has an excellent means of assessing new technologies for possible impacts.
		III	Vulnerabilities exist	System knows vulnerabilities exist; however, it is not aware of most of them. It reacts to disruptions. Has no ability to project vulnerabilities from new technology.
		II	Few vulnerabilities known	System has the basic understanding of vulnerabilities and is aware of most. Has no effort in place to address new vulnerabilities ahead of disruptions.
		I	Unaware of vulnerabilities	System's awareness of vulnerabilities is no more than elementary and probably much less.
	Planning	V	Holistic resilience strategy	System has a resilience strategy or Plan in place that is supported by the entire organization. It is ingrained in the architecture of the system and culture of the organization. It covers current conditions and future projected environments. It has provisions for training and education.
		IV	Resiliency measures	System has a coherent set of resiliency measures that apply to any and every subsystem, capability or process. The concept is accepted organization wide; however, emphasis is different in different work centers or offices.
		III	Realistic impact assessment	Realistic risk and operational assessments provide focused courses of action and necessary organizational involvement for current conditions. No long-term plan.

TABLE A3. DESCRIPTION OF TABLE ELEMENTS, CONTINUED

Criteria		Tier	Tier Description	Tier Explanation
SYSTEM	Planning, continued	II	Minimal resiliency actions available	Any resiliency actions available are reactive and localized to specific subsystems, capabilities or processes. There is no effort to address issues at a system level.
		I	No resiliency designed in system	Resiliency is taken for granted. There is no underlying theme or approach to Resiliency.
	Mitigation	V	Attacks have little or no effect on operations	Attacks are generally insignificant. System is able to tolerate and mitigate them and continue operations as normal.
		IV	Successful in mitigating or avoiding most attacks	Attacks are annoying. Specific actions need to be taken; however, they are successful in mitigating any effects.
		III	Some proactive measures in place	Attacks are serious and cannot be ignored. More reactive than proactive measures are necessary. Many consequences of attacks are unexpected.
		II	Reactive measures taken	Attacks are critical to the system operation and mission accomplishment. The reactive measures do not handle all of the attacks.
		I	No measures available	Attacks are catastrophic and result in system shutdown.
	Vigilance	V	Method to identify new vulnerabilities	System has means to research and assess new sources of disruptions and the vulnerabilities. It is generally expected that the system is prepared for new technology attacks.
		IV	Addresses obvious vulnerabilities	System is in place to address all known vulnerabilities. The ability to address the surfacing of new vulnerabilities is a reactive, but effective, process.
		III	Aware of attacks	System is aware of new vulnerabilities as they are attacked. It has no means of identifying the new vulnerabilities prior to an attack.

TABLE A3. DESCRIPTION OF TABLE ELEMENTS, CONTINUED

Criteria		Tier	Tier Description	Tier Explanation
SYSTEM	Vigilance, Continued	II	Can spell resiliency [surprised by attacks]	System needs to take time to study an attack and the symptoms before it can generate the awareness of a new vulnerability. It may not be able to correct or mitigate the new vulnerability.
		I	Clueless [does not know what to do]	System seeks outside help because it does not understand the new vulnerability or the extent it affects the mission.
Confidence		V	High	System confidence is high, fully confident that the system or capability will perform the mission with little or no disruptions affecting operations.
		IV	Moderate	System has moderate confidence that it will accomplish the mission in spite of potential disruptions.
		III	Medium	Medium confidence illustrates concern over mission accomplishment and integrity of the system.
		II	Low	Low confidence lacks any belief that the system can be counted on to do the mission.
		I	Nonexistent	No confidence means that the system is not acceptable.
Security		V	High	There are no acts that can bypass or contravene security policies, practices, or procedures.
		IV	Effective	In an environment of minor security breaches, security policies, practices, or procedures are able to protect the system effectively for mission accomplishment.
		III	Appears to be adequate	On the surface, security policies, practices, or procedures appear to be effective; however, security problems exist and often prevail.
		II	Minimal with breaches	Security breaches dominate the system and create an environment of mistrust. This leads to minimal to no mission accomplishment
		I	None	There are no security policies, practices, or procedures in place to prevent breaches.

Appendix B

Resiliency Tier Descriptions

TABLE B1. DESCRIPTION OF THE FIVE TIERS

Tier		Description
V	**Fully Capable**	May result in a slight perturbation in operations; however, the system/capability continues operating with nothing more than a "hiccup." Any disruption is an exceptional circumstance. (Insignificant disruptions)
VI	**Operational**	May experience a disruption resulting in possible resets or reboots; however, mission is accomplished and the disruptions are immediately isolated and mitigated. Disruptions can occur at any time; however, they are not showstoppers. (Negligible disruptions)
III	**Aware**	Is cognizant of operating environment, hazards therein, and vulnerabilities. Disruptions have a reasonable likelihood of occurring at any time. Mitigating actions are not always effective. Capability tolerates disruptions, but also does not handle the consequences well. (Moderate disruptions)
II	**Confusion**	Disruptions result in permanent partial disability or operational incapacity. Likelihood of disruptions happening is high. There is no requisite understanding of the problems. (Extensive disruptions)
I	**Exposed**	Disruptions are inevitable and greatly impact the system/capability. The capability is unprotected, totally exposed to hazardous environment. Damage may be irreversible. (Catastrophic disruptions)

Author Biography

Col Dennis J. Rensel, USAF (Ret.), is currently a senior space analyst with Booz Allen Hamilton, Inc., supporting the Office of the Secretary of Defense Cost Analysis Performance Evaluation (CAPE) Simulation Analysis Center (SAC). Prior to joining Booz Allen 12 years ago, he retired from the U.S. Air Force as a colonel following 25 years of military service. Col Rensel holds a JD from The Catholic University of America's Columbus School of Law; an MS in Electrical Engineering with a concentration in Electrical Engineering and Digital Systems from the Air Force Institute of Technology; and a BS in Electrical Engineering with a minor in Computer Science from the United States Air Force Academy.

(E-mail address: dennis.j.rensel.ctr@mail.mil)