Vaasan yliopisto
UNIVERSITY OF VAASA

Technical Report TR 4.1

Critical Infrastructure Resilience Evaluation Guidelines

Mike Mekkanen

1st June 2022

Vaasa 2022

Programme for Sustainable Growth and Jobs

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

Contents

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

Abbreviations

CI	Critical Infrastructure
ENISA	European Union Agency for Cybersecurity
lEC	International Electrotechnical Commission
NIST	National Institute of Standards and Technology

Leverage from
the EU
2014–2020

European Union
European Regional
Development Fund
European Social Fund

Executive Summary

Any security techniques that are in operation, sooner or later, may disrupt/fail for any reason, according to experience/records. As a result, and bearing in mind that CI security investments/efforts can be easily exploited. In addition the fact that today's our society, lives are integrally tied with key sectors that provide critical services in which that recognized so crucial to our well-being that their incapacity or destruction would have a significant impacts on the global economy, national security, and public health and safety. Therefore, CIs resilience had/have been gained more interest and the resilience approach is going far more than ecology and resources managements to include fields market development, transportation, health, food security, society planning and disaster management.

Furthermore, the manner that current CIs are connected to one another and to the Internet, as well as being publicly accessible for remote access, has produced new threats, such as data, CI assets, and activity, which are increasingly being targeted by hackers in order to obtain some benefits. As a result, critical infrastructure threats have increased considerably in recent years. These cyberattacks have progressed to the point where they may have had far-reaching and unexpected societal consequences. As a result, cyberattacks on vital infrastructure have been named one of the top five worldwide dangers by the World Economic Forum.

As a result, stakeholders involved in the safeguarding of such sensitive and crucial have reached a level of awareness that strongly suggests CIs resiliency should be more emphasis. As well as CIs operators are increasingly looking into ways to improve the resiliency of their systems, industrial controls, and business continuity.

However, these CIs resiliency measurements/enhancements are facing some challenges in order to assess their feasibility/suitability for each different CIs systems and complexity to measure. As a result, CIs operators/businesses must have in-depth knowledge of their CI systems and their dynamic capacities-capabilities. This CIs deep knowledge need to be evaluated incessantly along with the CI different dimensions perspectives to draw lessons on extract an essence into useful entities for resiliency evaluation metrics. Where, each entities that contributes to Resilience index metrics is given a relative weight. On the other hand evaluating a limited selection of outcomes or limiting resilience evaluation to a single dimension of measurement may obstruct the deeper understanding of CI system dynamics required to apply resilience thinking and advise management decision makers. Thus, in order to evaluate CI resiliency and produce consistent CI resiliency measurements, four resiliency CI dimensions (resiliency evaluation model) would be included within the continuous evolution process, and several outcome indicators must be tracked.

Leverage from
the EU
2014–2020

European Union
European Regional
Development Fund
European Social Fund

Scope

This work is aiming for providing a recommendation and practical hints on how to evaluate the concept of Resilience in the domain of Critical Infrastructures (CI). The document is not an engineering manual nor a research agenda. The work intend to be a reference document general enough to be applied to all different CI sectors, as well as to be used and customized to draft sector specific similar documents.

The work progresses from the notion of resilience, beginning with today's Best Practices, to a resilience state, attempting to highlight system resilience evaluation holistic approach at the border of the single CI's assets or the CI's full perimeter. This will necessitate a dynamic and continuously adapted system resilience various dimensions, capacities, capabilities, and outcome indicators ready to begin with system study state operating and progress through disaster recovery and business continuity processes in case of failure or cyber-attack.

The job was completed by take in due considerations the results of several previous activates and approaches as proposed and described in official reports authority organization standards such as ENISA, NIST, IEC etc.

Objective

The goal of this work is to highlight the Resilience concept for critical infrastructures CIs. The work is intended to address several basic questions (Resilience: of what, from what, to whom) and supporting the operators/owners of CI already in operation (resilience evaluation) holistic approach. How to foster resilience in an under-design project (resilience engineering). In addition, providing a recommendation and practical hints on how to evaluate the concept of Resilience in the domain of CIs, and why does the infrastructure system have a certain degree of resilience? As well as can be applied and customized to any type of infrastructure systems?

Audience

The report focuses on those who work/interest from both industry and academia in the design and development of CIs operation control associated information exchange-data and communications security (system resilience). As well as personnel who are being targeted include:

- CIs integrator, developers, configurators, researchers and who assess energy system communication.
- Policy makers, administrators, project designers, and network analysts
- OT/IT network security personnel
- Expert insights on securing and monitoring power systems

Document Structure

The resilience historically root term is identified at the beginning of this work, followed by the generic definition of resilience reflecting different dimensions/disciplines point view (technologies, people, processes and organizations) in which may overlapped with thoughts such as robustness, fault-tolerance, adaptability, survivability, and agility, among others is presented. Then the resilience evaluate model is analyzed along with its initiated different dimensions and entities. The overall resilience evaluating recommendations and mechanisms that able to adapt the CIs to address threat landscape, reduce the reaction time and increase the reconfiguration capabilities to reduce the impact on our society is defined.

Finally, examples of resilience outcomes cards driven approach support different resilience evaluation dimensions. As well as resilience evaluation example using metrics defining inputs given the energy resilience metrics for electrical system at the system level is presented in Annex A.

1 Introduction

From experience point view that any security approaches which are in activity, sooner or afterward, may disrupt/fail to any causes. For this reason, and being mindful of the truth that the investments/efforts put in for security of CIs can be effortlessly bypassed. At this point, stakeholders involved in the safeguarding of such sensitive and crucial have reached a level of awareness that strongly suggests CIs resiliency should be more emphasis. Let's begin with what the resilience phrases represent to better comprehend the CI's resilience strategy. The Latin word "resilience" is where the contemporary resilience terms come from, and it means "bounce back"[1] in which that directly refers to an entity's or system's capacity to return to its normal condition following the occurrence of an event that disrupts its equilibrium. Such a broad term encompasses subjects as diverse as ecology, materials science, psychology, economics, and engineering.

There have been several attempts to define resilience. Many are comparable, while many overlap with other ideas like as robustness, fault-tolerance, adaptability, survivability, and agility, among others. There have been several generic definitions of resilience suggested that include a wide range of disciplines. For instance in [2] they define the resilience as the “capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.” Resilience definition might also approach from a variety viewpoint and across application domains, since CIs is made up of people, processes, and organizations, not just technologies. In order to be full and successful, every resilience assessments should take into account all of these entities.

1.1 Resilience deferent dimensions view point

In this part, the definition of resilience, along with the holistic CI system view point that includes all system entities such as people, processes, and organizations, not simply technology, as any CI system is comprised of, is provided as follows:,

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

1.1.1 Social resilience

Social resilience where Individual, groups, and community capacities in interaction with the environment are studied, for instance in [3] authors defined social resilience as “ability of groups or communities to cope with external stresses and disturbances as a result of social, political, and environmental change.” In [4] authors define resilience within the social domain as “the ability of community members to take meaningful, deliberate, collective action to remedy the effect of a problem, including the ability to interpret the environment, intervene, and move on”, within the “problem” word authors include both the internal and external faults, shortages, changes etc. that the community members need to take action and cope whit this “problem” and back to normal stage. In addition the social domain resilience could be also classified in several subdomain such as ecology, psychology and sociology where they have extensively researched in[5], [6], [7] respectively.

1.1.2 Economic resilience

Economic resilience, economic success is becoming increasingly visible as a function of an area's capability to prevent, tolerate, and rapidly recover from major disruptions (i.e.,'shocks') to its objective basis. Several definitions of economic resilience place a heavy emphasis on the ability to rapidly recover from an incident. In the context of economic growth, however, economic resilience encompasses three major characteristics: the capability to rapidly recover from a shock, the ability to tolerate a shock (accept some level of shock), and the ability to learn from the past events, and prepare to avoid such events entirely in future. For instance in [8] defines the economic resilience as “the capacity to reconfigure, that is adapt, its structure (firms, industries, technologies, institutions) so as to maintain an acceptable growth path in output, employment and wealth over time.” Thus, in order to establish economic resilience in a local or regional economy, it is necessary to be able to identify risk vectors, assess the critical economic assets that risk vectors might affect, or have a highly likelihood to occur. Then allocate resources (system capacities), develop/evaluate the system response capability (system dynamic capability) for each individual risk vector in a dynamic manner (continuous process) [9].

1.1.3 Organizational resilience

Organizational resilience refers to the organization availability to sense their environment and gather the data, analyze and extract useful information. This useful information is used for planning to, respond to, and adapt to rapidly changing according to the developed resiliency "protection" strategy against unexpected disturbances. This dynamically continuous process will enhance the organizational resiliency, help the organization to survive from unexpected disturbances and grow based on improving/increasing the organizational capacities leading to dynamic capabilities [10]. Several definition for organizational resilience in literature for instance in [11] authors defined it as "the ability of an organization to absorb strain and improve functioning despite the presence of adversity." In [12] author defines resilience for company as "the company's ability to, and speed at which they can, return to their normal performance level (e.g., inventory, capacity, service rate) following by disruptive event." Cross-checking is a recurrent theme in the preceding definitions; erroneous acts can be detected fast enough to limit negative consequences and return to the normal performance level or even enhance it by learning from the past event and might use/targeting new features that improve the organizational performance .

1.1.4 Engineering resilience:

Engineering resilience is a term that has been widely used for a long time for several domains, however for engineering resilience is relatively new. Engineering domain consist from technical systems designed by engineers and usually they are multidisciplinary complex system of systems. The focus of resilience engineering is thus resilient systems performance rather than assets. In first early engineering resilience definition was given in [13]," The essence of resilience is therefore the intrinsic ability of an organization (system) to maintain or regain a dynamically stable state, which allows it to continue operations after a major mishap and/or in the presence of a continuous stress". Other definition in [14] as "the intrinsic ability of a system to adjust its functionality in the presence of a disturbance and unpredicted changes”. Understanding the regular system functionality and the system technology behind, as well as the expected failures, is curtail for resilience engineering designing and evaluation. In [15] authors define the engineering resilience as “the ability of a system to sustain external and internal disruptions without discontinuity of performing the system's function or, if the function is disconnected, to fully recover the function rapidly”. Whereas, in [16] authors highlight six factors that might enhanced engineering resiliency in which they are begin with minimization of failure, limiting of impacts, administrative controls/procedures, flexibility, controllability, and end with the early detection.

Engineering resiliency encompasses all aspects of CI design, building, operation, and maintenance with the goal of ensuring the capability to prevent, absorb, adapt, recoup from a troublesome event, whether natural or malicious cyber activates. Where, resiliency stress the importance of a whole rethinking around the concept of CIs protection. CIs protection relates to the capacity to protect or mitigate the consequences of an emergencies. Whereas CIs resiliency refer to the capability to cope with adverse occurrences in a way that prevent, absorb, adapt or might accept some ratio of disruptive events while reducing the magnitude, effect, length of a disruption and return back to normal operation as far as possible. Where as in some cases might accessed the previous equilibrant point and achieve new record as mentioned above. Thus today’s CIs must deal with an ever-changing threat and vulnerability landscape. That’s where resilience emerges from and becomes an important part of the playing field. A resilient approach is a holistic set of a dynamic continuous procedures and measures that encompasses the entire structure of an organization and include whole different resilience dominations. Starting from the physical part (Engineering resilience), to ensure the ability to prevent, absorb, adapt, and recover to an attack, either physical or cyber. Then the management part (Social resilience), putting organization personnel on a cooperative level and ongoing training to upgrade, update and achieve best practices (aimed at reduce personal mistakes, environmental inertia and social engineering issues). Thus in order to limit the resiliency concept confusing the transdisciplinary links is depicted in Figure 1, where holistic resilience approach need to be addressed to have a reliable system resilience measures.

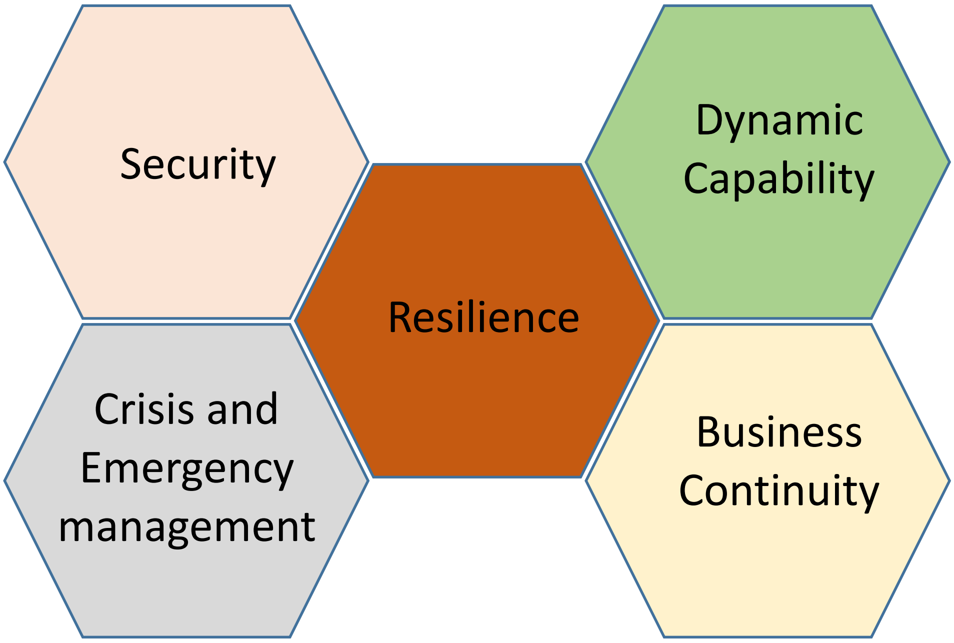


Figure 1. Resilience transdisciplinary

At this point, resilience that is a step ahead to business continuity. System Resiliency provide a full picture of a system in which that it mix among system availability, continuity, security, recovery, knowledgeability and scalability focusing first on how to unlock the power of purpose and value as depicted in Figure 2.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

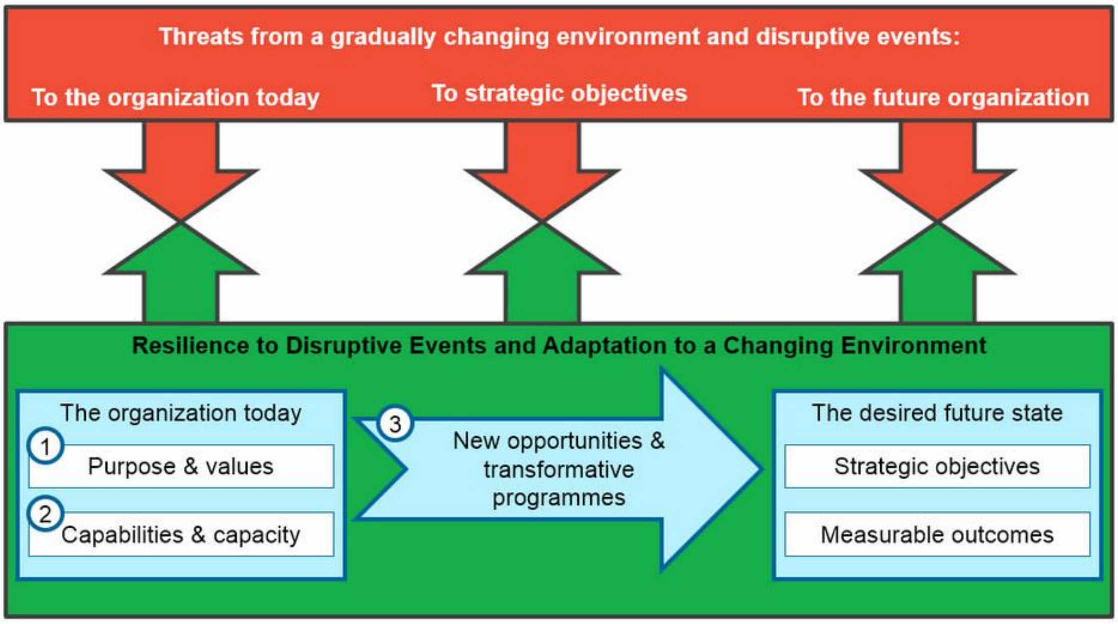

Threats from a gradually changing environment and disruptive events:
To the organization today
To strategic objectives
To the future organization
Resilience to Disruptive Events and Adaptation to a Changing Environment
The organization today
1
Purpose & values
2
Capabilities & capacity
3
New opportunities & transformative programmes
The desired future state
Strategic objectives
Measurable outcomes

Figure 2. Business resilience process [17]

Organizations with high preparation resilience can quickly "self" adjust to internal and external disruptive events such as failure or crisis, guaranteeing a continuous service. With the explicit goal of providing an initial policy for building a resilience strategy for CI Resilience Evaluation, it can be said that such policy should be based on a generic resilience model that the concept will be valid for different CI systems. As well as this resilience model need to be simple to apply and whose effectivity is simple to measure which is the objective current work.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

2 Resilience evaluation

A number of definition had already been presented in Part 1., in this report author will be in line with the definition stated in [18]” Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event”. It is clear that the CI may face different level of disruptive events occurrences. In reality, various disruptive events can influence a system in different ways, necessitating distinct recovery strategies, in order to achieve various level of resiliency. Thus in order to evaluate CI resiliency, critical question/factors need to answer and explore include for instance,

- Is the service has been degraded?
- How much of the service has been degraded?
- How soon the service has been recovered?
- How thoroughly the service has been restored?
- How comprehensively the services has been enhanced? in case of developing system capacities-capabilities after destructive events been wiped

As a result, five question/factors must be revealed in order to evaluate CI resilience reliably.

To begin with is the condition of service supplied by a CI in reaction to a disturbance, this situation is illustrated in Figure 3. Where it shows the CI system under disruptive event and the processing that the CI under hardening attempts to response, absorb, adapt and rapidly recover to return back to normal operation (equilibrium state), which is the CI operational steady state point in the sense of no disruptive events have/had occurred yet.

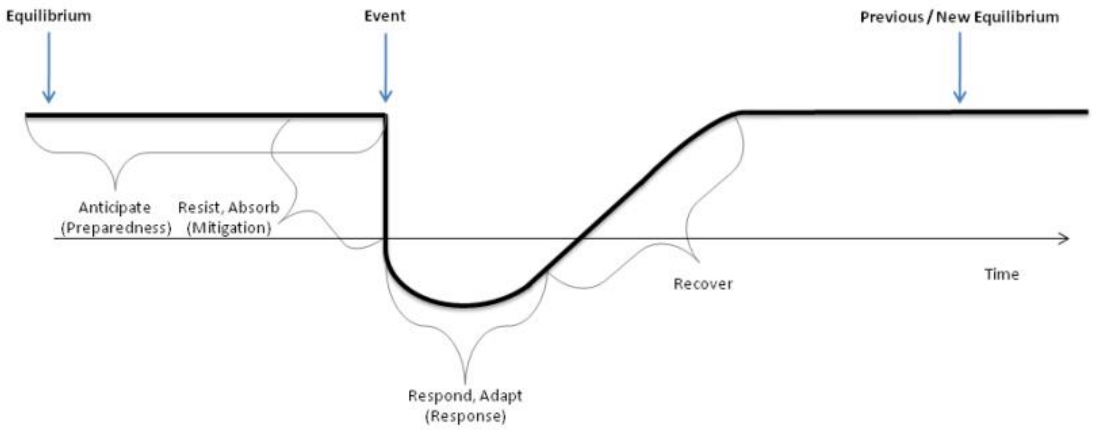

Equilibrium
Event
Previous / New Equilibrium
Anticipate (Preparedness)
Resist, Absorb (Mitigation)
Time
Recover
Respond, Adapt (Response)

Figure 3. CI Resilience according to disruptive event different time steps occurrence and recover [18].

A natural calamity, an industrial accident, failure, cyber-attack or a terrorist assault are different kinds of disruption events that might all cause a disruption to the CIs. The duration of the disruption and the pace of service reduction would be determined by the nature of the incident, the CI architecture, and the mode in which the CI is run. The duration of the interruption (measured in time and represented along the x-axis), as well as the rate and extent of recovery, would be determined by the same factors. Recovery may not be complete, however as shown in Figure 3 the CI system presented is return back to the equilibrium state as before the disruptive event has been occurs and 100% service delivery is achieved.

The second factor that need to consider to address the CI resiliency is the CI state where it determined by the CI development methodology and its operation conditions. For example, CI constructed with the broad redundancy idea, which quickly isolates the affected entities/subsystems and reconnects the healthy one, may have a less severe and shorter disruption. As a result, if a disruptive event occurs, the CI is more robust than a system with less redundancy, fewer backups, and is more difficult to reconstruct as illustrated in Figure 4.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

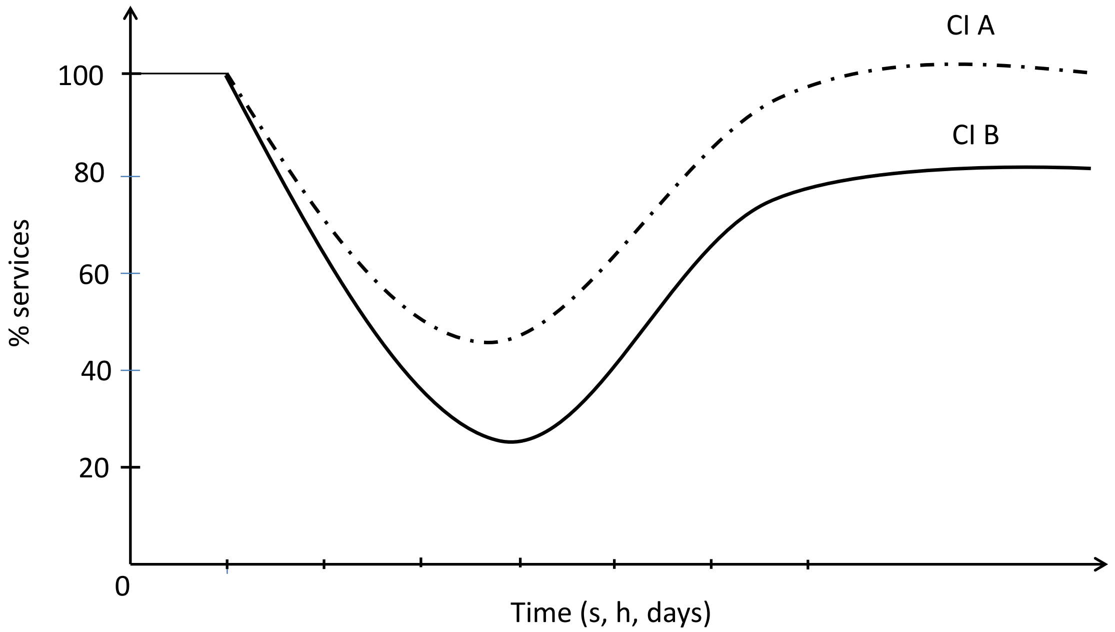


Figure 4. CIs A and B have different recovery time/level and resilience to the same disruption events

The third factor to consider when addressing CI resiliency is how different CIs respond to distortion events and the time required to completely recover. Thus the timescale dependency for CI resiliency/operation regardless of the occurrence of any destructive events is crucial. For example the CI resiliency service supplied may improve if the CI is constantly maintained, upgraded and updated, although at a cost. Whereas if the CI maintenance and improvements are not scheduled, performed, CI operations may be less expensive, but service may degraded in the future as illustrated in Figure 5. Whereas CI A with degraded operation functionality has less resilient awareness as well as less CI management capacities-capabilities, resulting in this degraded provision of services following occurrences.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

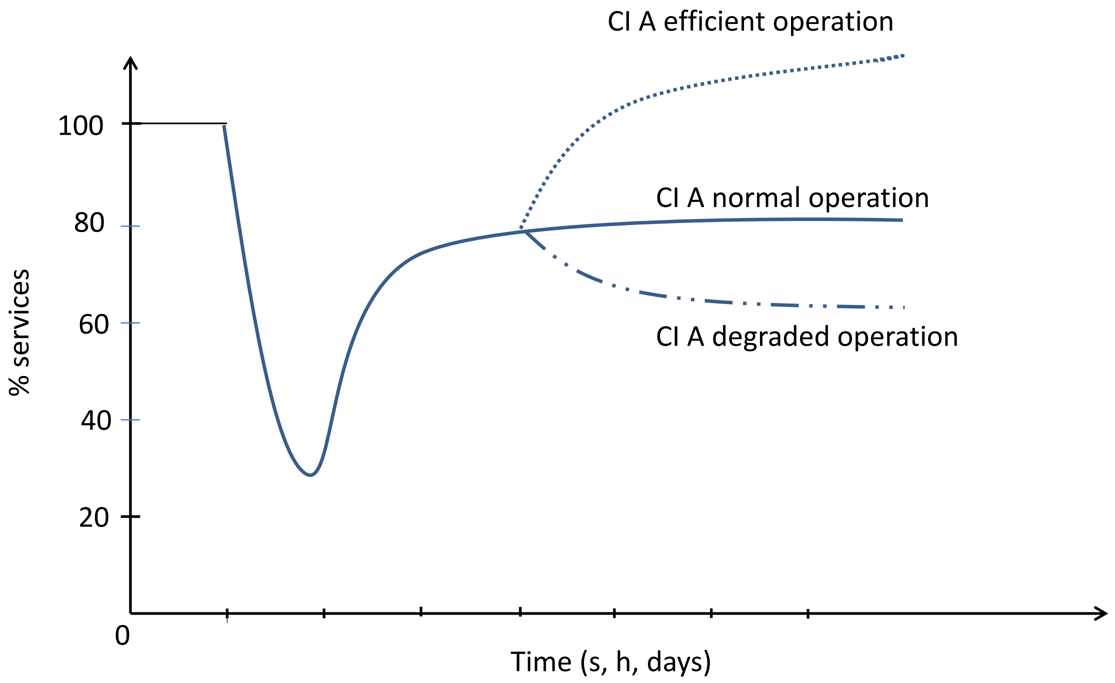


Figure 5. CI A upon different operation and response methods over timescale

Whereas the last two factors that need to consider in which that they play a significant role at the resiliency evaluation task that depending on the CI design and which kind of operation for instance CI detection-responding techniques/process, CI capacities and dynamic capabilities for allocating resources, lead to different resilience than other CIs but at a different costs. As CI is given greater resources, it may be able to reconstruct, activate new features, learn from the wiped past events (after a disaster) with more-efficient technologies. In this circumstance, and as a result of the fact that the CI has been rebuilt with more functionality/feathers, the quality of service provided after recovery may surpass the initial level of the specified services as illustrated in Figure 6. Where CI C has a higher resiliency and quality of services supplied after recovery. Whereas CI A and B upon additional resource has been allocated to rebuild the CI capacities-capabilities after the disruption events has been eliminated.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

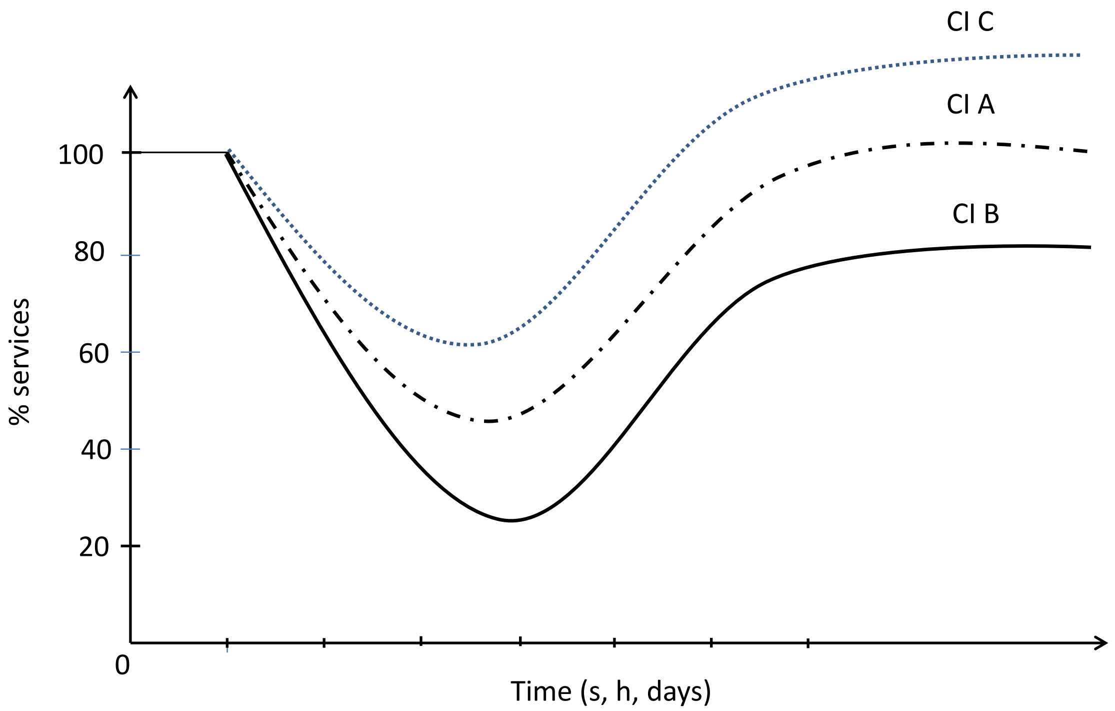


Figure 6. CIs Different resilience upon different responses based on different costs

At this stage, while creating the resilience evaluation model metrics for CIs, it is more important to capture the essential elements mentioned above that are directly related to CI design, operations, disruptions, and service delivery in relation to their time-scale [19].

2.1 Resilience evaluation model

The resilience characteristics are predicated on the notion that a CI is comprised of people, organizations, and technology (i.e.). These entities are reliant on other CI resilience dimensions. These dimensions may be layered in an abstraction degree order beginning with the greatest abstraction level of complexity, Technical Dimension. Then Community/Personal Dimension, Organizational Dimension and ending with the lowest abstraction degree level Cooperative Dimension. All of these resilience dimensions must be included in any Resilience Evaluation (or even Engineering) effort. As a result, Figure 7 depicts the resilience assessment hierarchy model, which incorporates all of the several dimensions of resilience evaluation entities that may be encountered in any CI system.

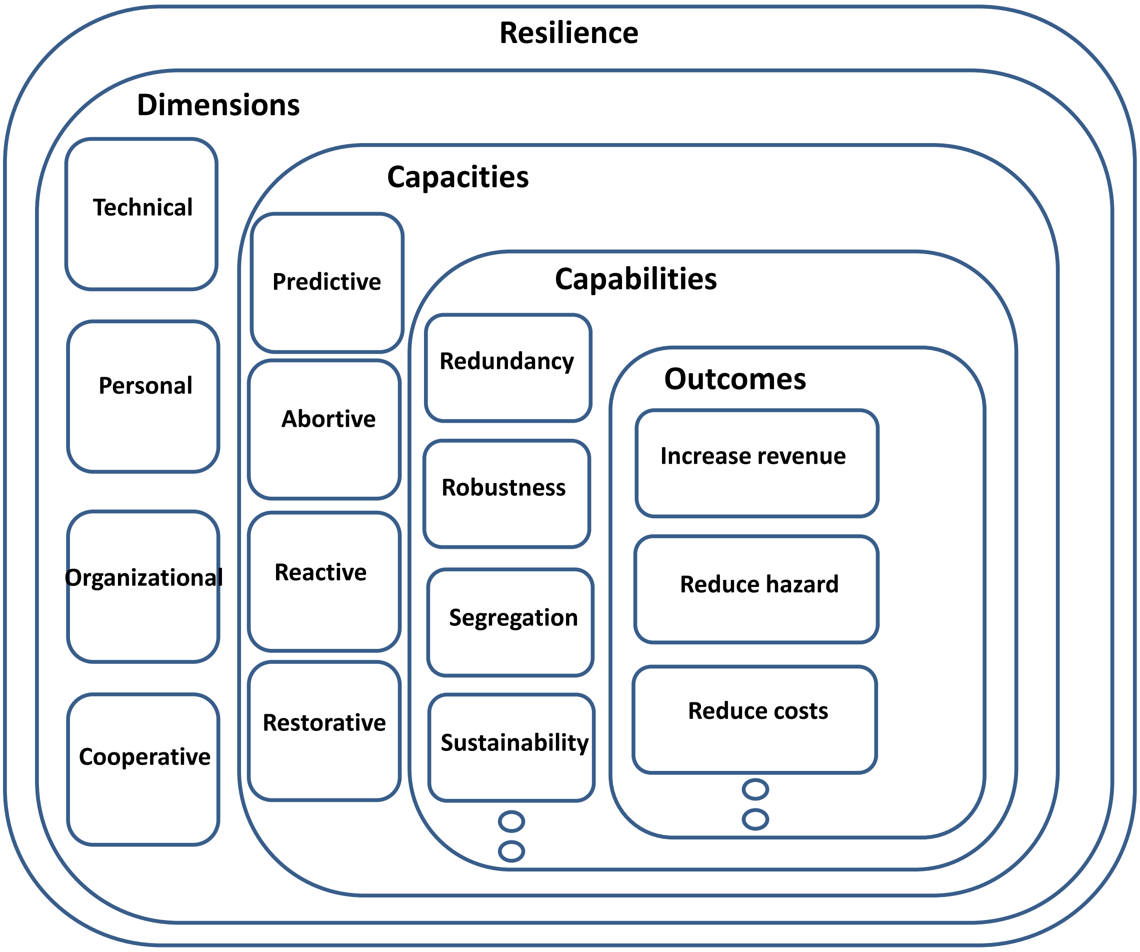


Figure 7. Resilience evaluation model

At this point resilience evaluation model for any CI system align with resilience holistic approach need to consider all different dimensions in order to have a reliable CI resilience measurements. Where each resilience dimension shown in Figure 7 is associated with four resilience capacities. These CI capacities may be linked to one or more of the system capabilities, where capabilities represent the existing infrastructure design implementations of the system. Furthermore resilience evaluation model has indicators for all CI dimensions which is the outcomes block. The resilience evaluation model outcomes is quantifiable features (indicators) of all the resilience dimensions. At this point, the CIs subject to assessment are defined by their capacities and capabilities.

2.1.1 CI resilience evaluation model capacities

CI resilience capacity is refers to the inherent features of the system infrastructure (inputs) that are applied into each of the resilience dimensions to make the system resilient.

According to the predefined resilience evaluation model four capacities had been identified (predictive/preventive, absorptive, adaptive and restorative).

2.1.1.1 Predictive/preventive

Predictive/preventive CI capacity is the ability of the system to foresee (detect) and prevent disruptive occurrences is referred to as predictive/preventive CI capacity.

2.1.1.2 Absorptive capacity

Absorptive capacity: refer to system's ability to automatically absorb the effect of system disruptions and minimize their consequences.

2.1.1.3 Adaptive capacity

Adaptive capacity: refer to the level where the system may self-organize and rebuild in order to restore system performance levels.

2.1.1.4 Restorative capacity

Restorative capacity reflect the system ability to be repaired, recovered fast and simply.

In the event of a disruptive situation, the four capacities will be activated as a deliberate process, beginning with predictive/preventive and progressing to restorative, based on the actual need.

The predefined CI capacities can be linked to one or more of system capabilities,

2.1.2 CI resilience evaluation model capabilities

CI Resilience capabilities which represent actual infrastructure engineering functional solutions that might be used to enhance CI resilience. The capabilities may encompass, but are not limited to, all tasks that may be performed (e.g., Robustness, Redundancy, Segregation, Diversity, Training, Governance, Automatic reaction, Rerouting, Human Resources Substitution etc.). Despite the fact that these capabilities contribute to CI resilience, they must be included in the development and evaluation of CI resilience.

2.1.3 CI resilience evaluation model outcomes

CI resilience outcomes which is the last entity within the resilience model. CI resilience outcomes is that quantitative qualities of the dimensions, capacities and capabilities that characterize the CI subject to resilience evaluation.

Thus assessing resilience outcome includes determining the level of acceptability of resilience adopting solutions at the most fundamental level of implementation to support system capacities. Resilience evaluation model outcomes are the fundamental tools and indicators for the CI resilience evaluation process. Figure 8 present the resilience tree and components that contribute to the CI resilience indicted by specific resilience outcomes.

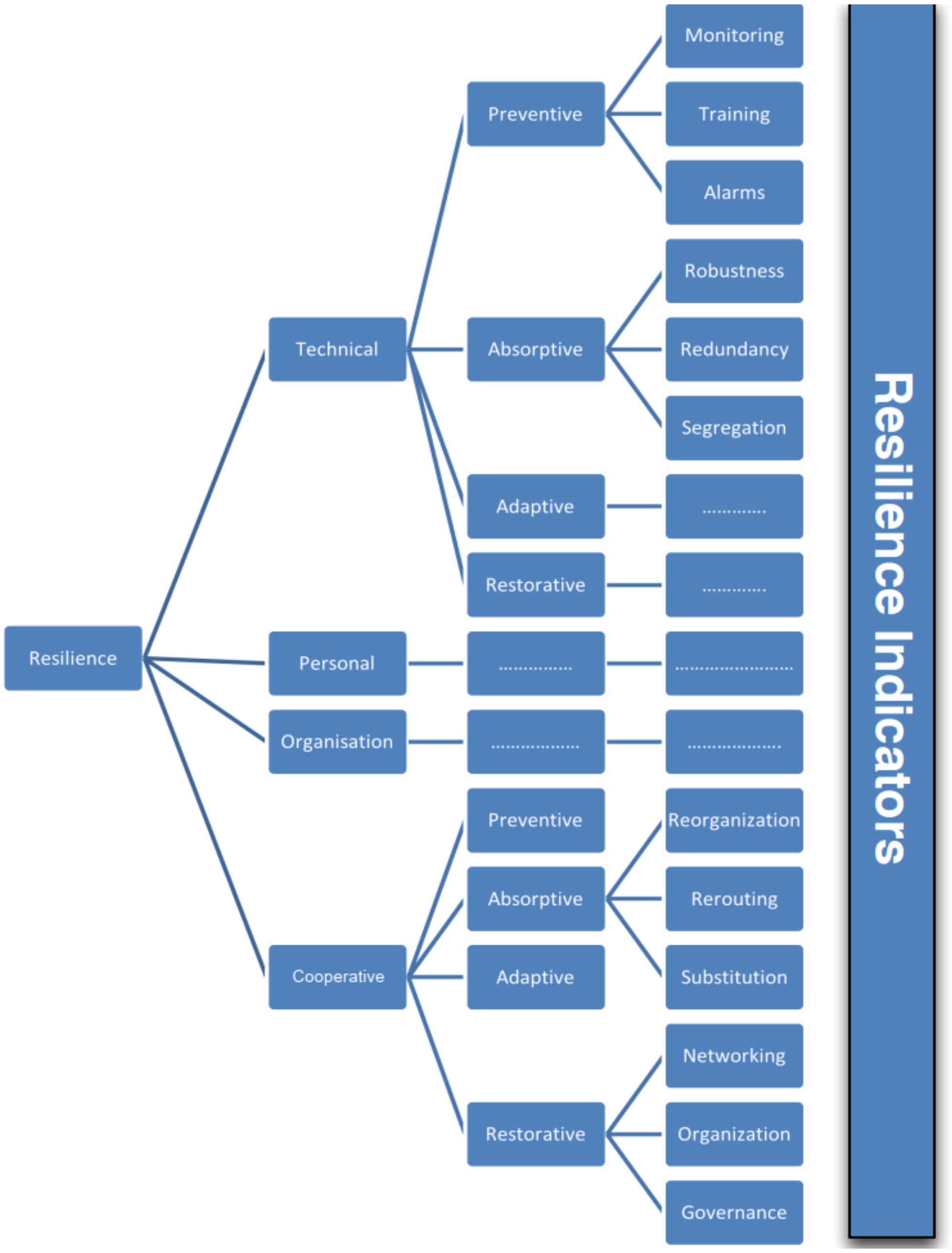


Figure 8. Resilience entities that system resilience depends on organized in tree hierarchy [18]

Consequently, the System resilience evaluation challenges may be separated into two concerns that must be addressed:

- What is being evaluated?
- What is the evaluation mechanism?

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

From the first challenge there is a set of questions expressing the resilience evaluation process. These questions must be addressed in order to fulfill the first challenge criteria, Table 1, shows a set of raising questions.

Table 1. Set of resilience evaluation raising questions

No.	Questions resilience evaluation: what is being evaluated?
1	How many dimension does the evaluation include?
2	How many capacities does the evaluation include?
3	What is the smallest unit of analysis?
4	Resilience outcomes characterizing the unit under analysis?
5	Is the evaluation inductive or deductive?
6	is the evaluation standardized or tailored to the context

Whereas according to the second challenge, the resilience evaluation model presupposes the use of the resilience outcomes in order to determine the extent to which each outcome proposal is implemented within the system under evaluation. Such a problem can be approached in a variety of ways (qualitative, quantitative, semi-quantitative, etc.) and with varying degrees of complexity. Furthermore, the issue of linkage among multiple outcomes occurs. These outcomes are highly interdependent since any CI system is consists from a number of subsystems where each subsystem provides services that linked to final outcomes. Thus quantifying CI resilience necessitates an indexed computation based on the weighted value of each outcome. Though that "*data emanating from the four dimensions have to be correlated and a composed value of resilience for the overall CI inferred using tailored composing algorithm account for the dependency level between the resilience of the different dimensions and layers*"[18] as shows below;

$$R_{System} = f(R_{tech}, R_{pers}, R_{Org}, R_{part}) \tag{1}$$

Function f in equation (1) must be specified at each levels of specificity (single asset, critical infrastructure, system-of-systems). At various levels of abstraction, each entities that contributes to Resilience index metrics is given a relative weight. In [18] several resilience outcomes cards has been identified in order to be selected and customized for specific CI system/application resilience evaluation, whereas in [19] other approach for CI system resilience evaluation is presented using metrics defining inputs given the energy resilience metrics for electrical system at the system level as an example of both approaches are shown at Annex A.

References

[1] C. Bowers, C. Kreutzer, J. Cannon-Bowers, and J. Lamb, “Team resilience as a second-order emergent state: A theoretical model and research directions,” *Front. Psychol.*, vol. 8, no. AUG, pp. 1–14, 2017, doi: 10.3389/fpsyg.2017.01360.

[2] B. Allenby and J. Fink, “Toward inherently secure and resilient societies,” *Science (80-.).*, vol. 309, no. 5737, pp. 1034–1036, 2005, doi: 10.1126/science.1111534.

[3] W. N. Adger, “Social and ecological resilience: Are they related?,” *Prog. Hum. Geogr.*, vol. 24, no. 3, pp. 347–364, 2000, doi: 10.1191/030913200701540465.

[4] B. J. Pfefferbaum, D. B. Reissman, R. L. Pfefferbaum, R. W. Klomp, and R. H. Gurwitch, “Building Resilience to Mass Trauma Events,” *Handb. Inj. Violence Prev.*, no. August 2020, pp. 347–358, 2007, doi: 10.1007/978-0-387-29457-5_19.

[5] S. Carpenter, B. Walker, J. M. Anderies, and N. Abel, “From Metaphor to Measurement: Resilience of What to What?,” *Ecosystems*, vol. 4, no. 8, pp. 765–781, 2001, doi: 10.1007/s10021-001-0045-9.

[6] S. S. Luthar, D. Cicchetti, and B. Becker, “The construct of resilience: A critical evaluation and guidelines for future work,” *Child Dev.*, vol. 71, no. 3, pp. 543–562, 2000, doi: 10.1111/1467-8624.00164.

[7] Y. Yu *et al.*, “Resilience and social support promote posttraumatic growth of women with infertility: The mediating role of positive coping,” *Psychiatry Res.*, vol. 215, no. 2, pp. 401–405, 2014, doi: 10.1016/j.psychres.2013.10.032.

[8] R. Martin, “Regional economic resilience, hysteresis and recessionary shocks,” *J. Econ. Geogr.*, vol. 12, no. 1, pp. 1–32, 2012, doi: 10.1093/jeg/lbr019.

[9] U.S. Economic Development Administration, “Comprehensive Economic Development Strategy (CEDS) Content Guidelines,” pp. 1–26, 2016, [Online]. Available: https://www.eda.gov/ceds/content/economic-resilience.htm

[10] J. Fiksel, “Organizational Resilience,” *Resilient by Des.*, pp. 129–147, 2015, doi: 10.5822/978-1-61091-588-5_8.

[11] T. J. Vogus and K. M. Sutcliffe, “Organizational resilience: Towards a theory and research agenda,” *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, no. May, pp. 3418–3422, 2007, doi: 10.1109/ICSMC.2007.4414160.

[12] Y. Sheffi and J. B. Rice, “A supply chain view of the resilient enterprise,” *MIT Sloan Manag. Rev.*, vol. 47, no. 1, 2005.

[13] D. D. Woods, E. Hollnagel, E. Hollnagel, and D. D. Woods, “Resilience Engineering : Concepts and Precepts PROLOGUE : RESILIENCE ENGINEERING CONCEPTS PART I : EMERGENCE UNSTABLE,” no. August, 2016.

[14] Erik Hollnagel, “Resilieance engineering”, [Online]. Available: https://erikhollnagel.com/ideas/resilience-engineering.html

[15] B. Cai *et al.*, “Resilience evaluation methodology of engineering systems with dynamic-Bayesian-network-based degradation and maintenance,” *Reliab. Eng. Syst. Saf.*, vol. 209, no. January 2020, p. 107464, 2021, doi: 10.1016/j.ress.2021.107464.

[16] L. T. T. Dinh, H. Pasman, X. Gao, and M. S. Mannan, “Resilience engineering of industrial processes: Principles and contributing factors,” *J. Loss Prev. Process Ind.*, vol. 25, no. 2, pp. 233–241, 2012, doi: 10.1016/j.jlp.2011.09.003.

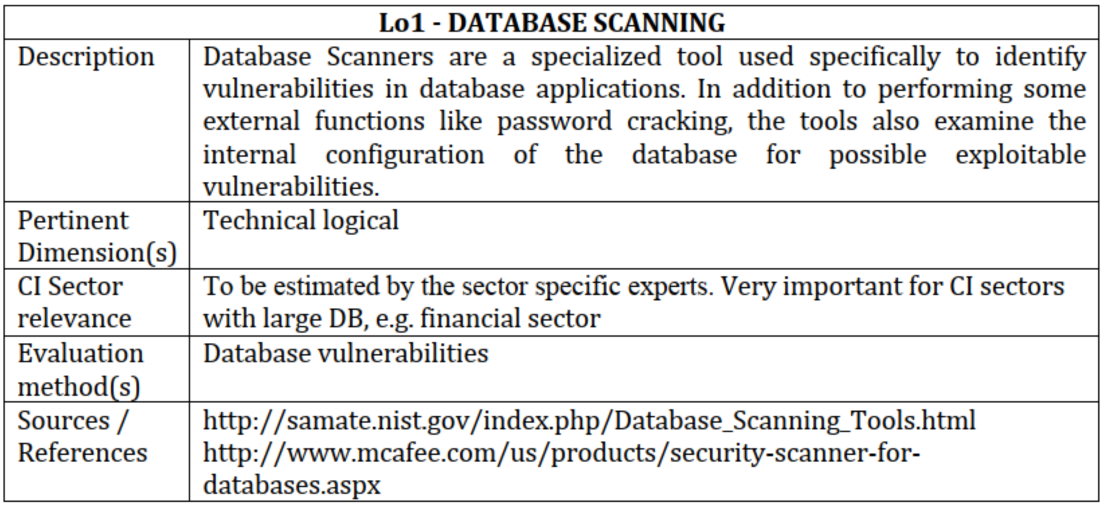
[17] Robin Gaddum, “People: the untouched lever of business resilience,” *Bus. Contin.*, 2015, [Online]. Available: https://www.continuitycentral.com/index.php/news/resilience-news/723-people-the-untouched-lever-of-business-resilience

[18] G. Bertocchi *et al.*, “Guidelines for Critical Infrastructures Resilience Evaluation,” no. February, pp. 1–101, 2016, doi: 10.13140/RG.2.1.4814.6167.

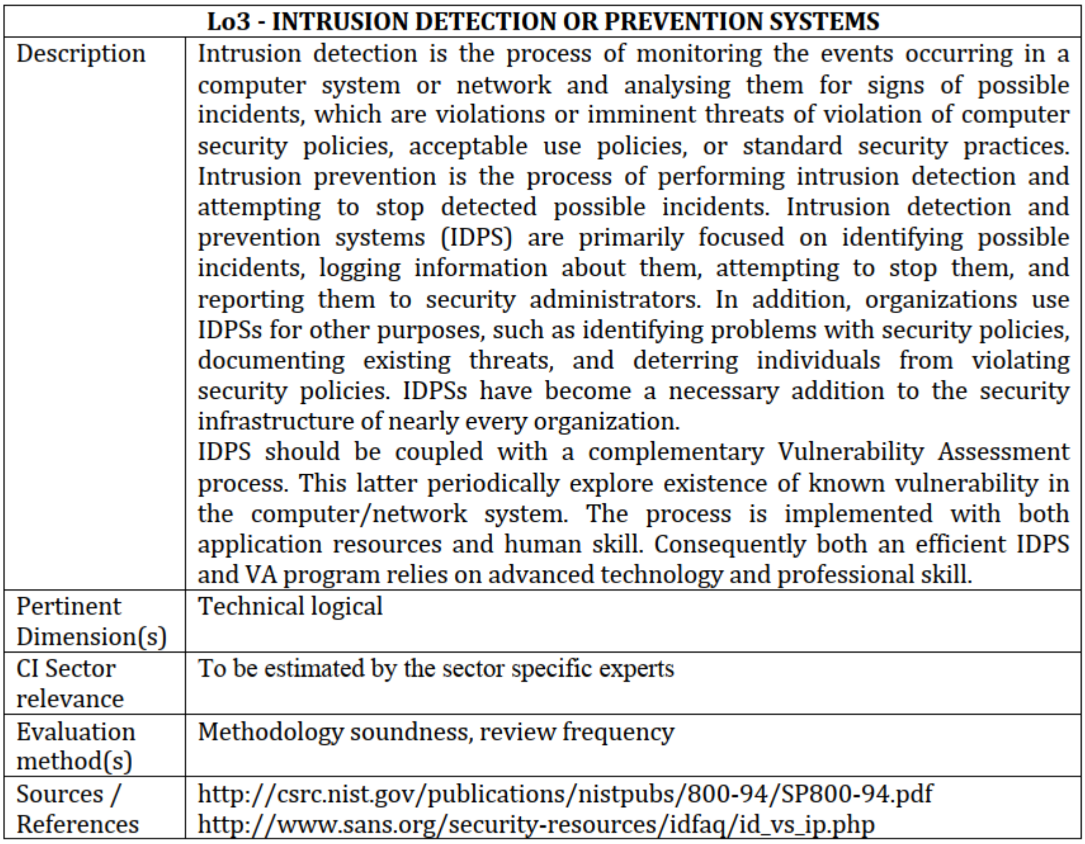
[19] H. H. Willis and K. Loa, “Measuring the Resilience of Energy Distribution Systems, RAND Corporation: May 2015,” *RAND Corp.*, 2020, [Online]. Available: https://www.rand.org/pubs/research_reports/RR883.html

3 Annex A

At the beginning examples of resilience outcomes cards driven approach support different resilience evaluation dimensions is presented as follows;



Lo1 - DATABASE SCANNING	
Description	Database Scanners are a specialized tool used specifically to identify vulnerabilities in database applications. In addition to performing some external functions like password cracking, the tools also examine the internal configuration of the database for possible exploitable vulnerabilities.
Pertinent Dimension(s)	Technical logical
CI Sector relevance	To be estimated by the sector specific experts. Very important for CI sectors with large DB, e.g. financial sector
Evaluation method(s)	Database vulnerabilities
Sources / References	http://samate.nist.gov/index.php/Database_Scanning_Tools.html http://www.mcafee.com/us/products/security-scanner-for-databases.aspx



Lo3 - INTRUSION DETECTION OR PREVENTION SYSTEMS	
Description	Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization. IDPS should be coupled with a complementary Vulnerability Assessment process. This latter periodically explore existence of known vulnerability in the computer/network system. The process is implemented with both application resources and human skill. Consequently both an efficient IDPS and VA program relies on advanced technology and professional skill.
Pertinent Dimension(s)	Technical logical
CI Sector relevance	To be estimated by the sector specific experts
Evaluation method(s)	Methodology soundness, review frequency
Sources / References	http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf http://www.sans.org/security-resources/idfaq/id_vs_ip.php

Lo4 – PERIPHERAL PROTECTION: FIREWALLS, TUNNELLING & VPN	
Description	Since a couple of decades, firewalls are and stay as the main resources for an efficient perimeter protection. They span from the simplest "packet filtering" still widely in use kind to more complex architectures like the "screened host" one. A firewall system efficiency relies basically on two pillars: a sound and needs tailored rules set and a regular logs analysis. This latter task should be obviously carried on by skilled people, even if with the support of specialized software able to reduce the bulky volume of information supplied by logs. Tunnelling is the process to design and implement a Virtual Private Network using TCP/IP family protocols, often packed in "bundles" (as IPSec) able to assure all necessary services: cryptography, keys negotiation, session negotiation etc. Even if ready to use commercial application are widely available on the market, internal skills able to evaluate such application and accomplish an independent choice are recommended.
Pertinent Dimension(s)	Technical logical
CI Sector relevance	To be estimated by the sector specific experts
Evaluation method(s)	Presence, percentage of applications/processes involved.
Sources / References	http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

Lo5 -MALWARE: PREVENT OR QUICKLY DETECT APTs	
Description	A protection policy able to protect data against malware is a basic issue now-a-day for both public and private entities. Malware is today a multifaceted evil with different functionalities and different levels of potential danger. In all cases it should be detected as early as possible and eradicated. Is recommended that malware, in all its various manifestations, is faced with an actual specific policy which covers all the aspects of the process: functions definition, roles and responsibilities assignment, products selection and usage criteria etc. Advanced persistent threats (APTs)—sophisticated, covert attacks bent on surreptitiously stealing valuable data from targeted and unsuspecting companies—can inflict serious harm to your business. Their relentless, persistent intrusions typically target key users within organizations to gain access to trade secrets, intellectual property, state and military secrets, computer source code, and any other valuable information available. And no one—from government agencies to start-ups—is immune today. You can, however, take proactive and rigorous steps to detect APTs in their early stages and implement asset-protecting remediation. Because APTs operate covertly and are difficult to detect, months can pass with no visible compromises to the organization quietly under attack. Moreover, single instances may be detected while multiple others inside the same organization go unnoticed. Comparable to combating a life-threatening disease, early detection is vital.
Pertinent Dimension (s)	Technical logical
CI Sector relevance	To be estimated by the sector specific experts
Evaluation method(s)	Anti-malware software presence; effective APT activity.
Sources / References	https://www.paloaltonetworks.com/products/features/apt-prevention.html http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf

Pe1 – EMPLOYEES ARE TRAINED AND MADE AWARE OF RESILIENCE REQUIREMENTS	
Description	Employees receive standard training and, further to that, are introduced to the basic concepts of resilience.
Pertinent Dimension(s)	Personal and organizational
CI Sector Relevance	To be estimated by the sector specific experts. HR should have a significant role in this evaluation
Evaluation methods	Presence/absence
Sources / References	M. Mullen "*On Total Force Fitness in War and Peace*" – MILITARY MEDECINE, 175, 8:1, 2010 Carlin Leslie, Air Force Public Affairs Agency OL-P "*Comprehensive Airman Fitness: A Lifestyle and Culture*", August 19, 2014.

Pe2 – SPECIFIC RESILIENCE CAPACITIES AND FEATURES CONCEPTS DURING SAFETY AND HEALTH TRAINING THAT WILL INVOLVE ALL THE CI PERSONNEL	
Description	Safety and health training occasions are used to deliver also resilience-oriented training. Where applicable, this training involves all the resources, even those not specifically devoted to crisis and emergency management.
Pertinent Dimension(s)	Personal and organizational
CI Sector Relevance	To be estimated by the sector specific experts. HR should have a significant role in this evaluation
Evaluation method(s)	Number of hours of specific resilience training
Sources / References	Regina A. Shih, Sarah O. Meadows, Margret T. Martin "*Medical Fitness and Resilience*" RAND Project AIR FORCE Series on Resilience,2013 Sean Robson "*Psychological Fitness and Resilience*" RAND Project AIR FORCE Series on Resilience,2014. Sean Robson, Nicholas Salcedo "*Behavioural Fitness and Resilience*" RAND Project AIR FORCE Series on Resilience,2014. Sean Robson "*Physical Fitness and Resilience*" RAND Project AIR FORCE Series on Resilience,2014.

Or2 - Organization's resilience Management System	
Description	A resilience management system in Critical Infrastructures, enables an organization, to establish the context, define, plan, implement, operate, check, review, and improve its resilience. It helps an organization to design a balanced system to reduce the likelihood and minimize the consequences of disruptive events. It provides a framework for businesses to assess the risks of disruptive events, develop a proactive strategy for prevention, response and recovery, establish performance criteria, and evaluate opportunities for improvement. It empowers the organization to implement an organizational resilience management system appropriate to its needs and those of its stakeholders. It supports any organization wishing to enhance its resilience and preparedness.
Pertinent Dimension(s)	Organizational
CI Sector Relevance	To be estimated by the sector specific experts
Evaluation method(s)	Presence & Maturity level of Adoption by the Organization
Sources / References	https://www.asisonline.org/News/Press-Room/Press-Releases/2010/Pages/OrganizationalResilienceANSIStandard.aspx http://catalogo.uni.com/pdr/pub/uni_pdr_6_2014.pdf

Or3 – Governance Framework – Stakeholders Analysis	
Description	Stakeholder analysis is a process of systematically gathering and analysing qualitative information to determine the interests that should be taken into account when developing and/or implementing a policy or program. It involves the gathering of Stakeholders' needs in order to contribute to identify the overall resilience objectives. This is a relevant step to determine the resilience program of critical infrastructures also beyond business interest objectives; for example, when involving essential services to citizens and other national level interests (i.e. political and economic stability, etc.). Stakeholders' needs support also the definition of the organization intent and objectives, thus contributing to identify also the resiliency posture.
Pertinent Dimension(s)	Organizational
CI Sector Relevance	To be estimated by the sector specific experts
Evaluation method(s)	Presence & maturity level of adoption by the Organization
Sources / References	http://transformed.businesscatalyst.com/media/articles/stakeholder_analysis.html http://www.eestum.eu/voorbeelden/Stakeholders_analysis_guidelines.pdf

Or7 – Governance Framework - Resource allocation for Resilience	
Description	Resilience is not a zero-cost process: a specific allocation of investment is needed. The effectiveness of such investment should be suitably evaluated through a Return on Resiliency Investment index. The investments are to be intended for any tangible (human resources, technical infrastructure and equipment) and intangible (culture, knowledge) asset deemed necessary. The Chief Financial Officer of the organization should be involved in the decision regarding the implementation of the Resilience program and his evolutions.
Pertinent Dimension(s)	Organizational
CI Sector Relevance	To be estimated by the sector specific experts
Evaluation method(s)	Presence & Maturity level of Adoption by the Organization
Sources / References	https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment http://www.isaca.org/Journal/Blog/Lists/Posts/Post.aspx?ID=263

Co1 –RELATIONSHIP WITH EXTERNAL BUSINESS PARTNERS	
Description	A partnership is an agreement between two or more entities that need to work together to accomplish a goal in a trusted environment providing them mutually beneficial relationship. This means a partnership is on voluntarily basis, built on trust, and based on mutual benefits. Relationships with external actors impact every aspect of business operations. Cooperation may occur as individual one-to-one partnerships or it may involve multiple parties such as in external alliances, suppliers' customers' relationships. A potential CI operator/manager must therefore take a structured approach to set reliable partnership able to complement and enhance existing business activities.
Pertinent Dimension(s)	Cooperative
CI Sector Relevance	To be estimated by the sector-specific experts
Evaluation method(s)	Existence of formal cooperation protocols
Sources / References	http://www.bsigroup.com/LocalFiles/en-GB/bs-11000/resources/BSI-BS-11000-implementation-guide-UK-EN.pdf

Co2 – NEED TO GUARANTEE QUILITY IN PROVIDED SERVICES	
Description	Dependency from external actors for the productions of goods or provision of services may strongly affect resilience performance of a potential CI operator/manager. Service Level Agreements (SLAs) are formalized way to guarantee the reliability of the input to the productive process. They imply an indirect commitment of the external actors to improve their resilience in order to not have cascading effects on their clients. The punishment of not respecting the SLA is an additional cost in terms of reimbursement to clients affected by the loss of service under the agreed threshold.
Pertinent Dimension(s)	Cooperative
CI Sector Relevance	To be estimated by the sector specific experts
Evaluation method(s)	Existence of SLAs
Sources / References	https://www.cpni.gov.uk/documents/publications/undated_pubs/1001002-guide_to_telecomms_resilience_v4.pdf http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5339893&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5339893

Then example for CI system resilience evaluation is presented using metrics defining inputs given the energy resilience metrics for electrical system at the system level is presented in [19] as follows;

Inputs	Capacities	Capabilities	Performance	Outcomes
Energy feedstock (H) (McCarthy, Ogden, and Sperling, 2007) **Energy not supplied** (L) (Brancucci Martínez-Anido et al., 2012) **Energy storage** (L) (Bhatnagar et al., 2013) **Generators available (#)** (H) (Roe and Schulman, 2012) **Hydrophobic coating on equipment** (L) (Keogh and Cody, 2013) **Key replacement equipment stockpile** (L) (Keogh and Cody, 2013) **Redundant power lines** (L) (Keogh and Cody, 2013) **Reinforced concrete versus wooden distribution poles** (L) (Keogh and Cody, 2013) **Siting infrastructure** (L) (Keogh and Cody, 2013) **Underground, overhead, undersea distribution/ cable lines** (M) (Doukas et al., 2011; Rouse and Kelly, 2011) **Unique encrypted passwords for utility "smart" distribution** (L) (Keogh and Cody, 2013) **Workers employed (#)** (H) (McCarthy, Ogden, and Sperling, 2007; Keogh and Cody, 2013)	**Communication/control systems/ control centers** (L) (Ward, 2013) **Electrical protection and metering** (L) (Ward, 2013) **Equipment positioning** (L) (Keogh and Cody, 2013) **Flow paths, line flow limits** (L) (Bompard, Napoli, and Xue, 2010) **Gen/load bus distribution** (L) (Bompard, Napoli, and Xue, 2010) **Reserve/spare capacity** (M) (Willis and Garrod, 1997; Molyneaux et al., 2012) **Substations (switchyards)—overhead lines** and **underground cables** are interconnected (L) (Ward, 2013)	**Ancillary service** (L) (Bhatnagar et al., 2013) **Hazard rate relating function**—altered hazard rate of component after a certain maintenance (M) (Wang and Guo, 2013) **Line mitigation**—reroute electrical flows due to line overloading or "congestion" (L) (Roe and Schulman, 2012) **Load biasing**—major adjustments in automated dispatching software (L) (Roe and Schulman, 2012) **Net-ability**—measures the aptitude of the grid in transmitting power from generation to load buses efficiently (L) (Bompard, Napoli, and Xue, 2010) **Path redundancy**—assesses the available redundancy in terms of paths in transmitting power from a generation to a load bus based on entropy (L) (Bompard, Napoli, and Xue, 2010) **Protective and switching devices**—mean time to repair (M) (Yeddanapudi, 2012) **Protective and switching devices**—switching reliability (M) (Yeddanapudi, 2012) **Protective and switching devices**—mean time to switch (M) (Yeddanapudi, 2012) **Viability of investments** (L) (McCarthy, Ogden, and Sperling, 2007)	**Coefficient of variation of the frequency index of sags** (M) (Shun et al., 2012) **Control Performance Standard 2 violations**—one of the California Independent System Operator CIISO principal reliability standards (H) (Roe and Schulman, 2012) **Bulk electric system reliability performance indices** (M) (Billinton and Wangdee, 2006) **Derated power**—rated power multiple with the reliability of the plant (M) (Voorspools and D'Haeseleer, 2004) **Dropped/lost phase**—power quality metric (M) (Rouse and Kelly, 2011) **Edge resilience trajectory**—relationship between reliability and resilience tracking a moving range of R^2 for the Control Performance Standard 2 (H) (Roe and Schulman, 2012) **Energy efficiency/intensity** (H) (Gnansounou, 2008; Molyneaux et al., 2012; Wang et al., 2012) **Failure rate** (M) (Wang and Guo, 2013) **Flicker**—power quality metric (M) (Rouse and Kelly, 2011) **Harmonic distortions**—power quality metric (M) (Rouse and Kelly, 2011) **Overhead and underground line segments**—mean time to repair (L) (Yeddanapudi, 2012) **Overhead and underground line segments**—permanent failure rate (L) (Yeddanapudi, 2012)	**Load loss damage index**—damage caused by fire to the electrical system (M) (Lucia, 2012; Bagchi, Sprintson, and Singh, 2013)

Inputs	Capacities	Capabilities	Performance	Outcomes
Transmission lines available (#) (M) (Roe and Schulman, 2012)	**Functional zones**—generation, transmission, and distribution (H) (McCarthy, Ogden, and Sperling, 2007) **Hierarchical levels (HLI, HLII, HLIII)**—HLI considers only generating facilities, HLII adds transmission facilities, and HLIII includes all three functional zones (H) (McCarthy, Ogden, and Sperling, 2007) **Operator training** (L) (Keogh and Cody, 2013) **Mutual assistant agreements** (L) (Keogh and Cody, 2013) **Transformers**—connecting parts of the network operating at different voltages (L) (Ward, 2013) **Tree trimming metrics** (L) (Keogh and Cody, 2013)	**Adequacy**—the ability of the system to supply customer requirements under normal operating conditions (H) (McCarthy, Ogden, and Sperling, 2007) **Congestion control** (L) (Carvalho et al., 2014)	**Average Service Availability Index (ANSI)** (H) (Layton, 2004) **Average Service Interruption Duration Index** (H) (Yeddanapudi, 2012) **Customer Average Interruption Duration Index**—sustained outage metric; measures average duration of sustained outage per customer (H) (Layton, 2004; Eto and LaCommare, 2008; Rouse and Kelly, 2011) **Customer Total Average Interruption Duration Index** (H) (Yeddanapudi, 2012) **Customer Average Interruption Frequency Index**—measures customer average interruption frequency (H) (Layton, 2004; Rouse and Kelly, 2011) **Customers experiencing longest interruption durations (CELID-X; CELID-8)**—sustained outage metric; measures the percentage of customers experiencing extended outages lasting more than X hours (H) (Rouse and Kelly, 2011) **Customers experiencing multiple interruptions (CEMI-X)**—sustained outage metric; measures the percentage of customers with multiple outages. This metric helps to measure reliability at a customer level and can identify problems not made apparent by systemwide averages (H) (Rouse and Kelly, 2011) **Customers experiencing multiple momentary interruptions (CEMMI-X; CEMMI-4)**—measures the percentage of customers who experienced X momentary interruptions (H) (Rouse and Kelly, 2011) **Customers interrupted per interruption index** (H) (Layton, 2004)	**Annual price cap** (H) (Billinton and Wangdee, 2006) **Annual allowed revenue** (H) (Billinton and Wangdee, 2006) **Cost of interruption**—social, commercial, industrial, etc. (L) (Doukas et al., 2011) **Impact factor on the population**—share of the population affected by the power loss (M) (Poljansek, Bono, and Gutierrez, 2012) **Long-distance transmission costs** (M) (Doukas et al., 2011) **Noise** (L) (Doukas et al., 2011) **Performance-based regulation reward/penalty structure** (L) (Billinton and Wangdee, 2006) **Price of electricity** (M) (Doukas et al., 2011) **Value of lost load**—value of unserved energy; customers' value of the opportunity cost of outages or benefits forgone through interruptions in electricity supply (L) (Willis and Garrod, 1997; Lucia, 2012)

Inputs	Capacities	Capabilities	Performance	Outcomes
Storm reserve funds (L) (Keogh and Cody, 2013)	**Concentration of market suppliers** (M) (Blyth and Lefevre, 2004) **Herfindahl-Herschmann index**—used to measure market concentration risk; square of each participant's market share added together across all participants with the largest shares (M) (Blyth and Lefevre, 2004; Reymond, 2007) **Geopolitical market concentration risk** (M) (Blyth and Lefevre, 2004)			**CO_2 emissions** (M) (Doukas et al., 2011) **Deregulated electricity markets**—allocation of losses (L) (Doukas et al., 2011) **Public deaths/injuries** (due to power interruptions) (M) (Australian Electrical Regulatory Authorities Council, 2005–2006; Rouse and Kelly, 2011) **Public deaths/injuries** (due to interactions with the distribution system) (M) (Australian Electrical Regulatory Authorities Council, 2005–2006; Rouse and Kelly, 2011)

Inputs	Capacities	Capabilities	Performance	Outcomes
Hubs—nodes with the most links are the most interconnected and serve as *hubs* (H) (Nadeau, 2007) **Links**—flow between nodes takes place on *links* (roads, electric power transmission lines, water mains, etc.) (H) (Nadeau, 2007; Vugrin and Turnquist, 2012; Ellison, Corbet, and Brooks, 2013) **Nodes**—element of the network that can receive gas from storage facilities, pipeline interconnections, or production areas (H) (Anderson 2001; Nadeau, 2007; Ellison, Corbet, and Brooks, 2013) **Primary energy supply**—includes the systems and processes used to supply a primary energy resource to its point of conversion into the final energy product of interest (H) (McCarthy, Ogden, and Sperling, 2007) **Storage facilities/nodes, intermediate storage (#)** (H) (Vugrin and Turnquist, 2012; Ellison, Corbet, and Brooks, 2013)		**Emergency procedures/ emergency shutdown system** (M) (Hsu, Shu, and Tsao, 2010) **Maximum/minimum flow** (H) (Ellison, Corbet, and Brooks, 2013)	**Cost per unit of flow** (H) (Ellison, Corbet, and Brooks, 2013) **Efficiency of flow**—one minus the fraction of gas burned as compressor fuel (H) (Nadeau, 2007; Ellison, Corbet, and Brooks, 2013) **Response to equipment outages—**degree to which the system is able to continue to reliably operate in the event of equipment downtime (L) (McCarthy, Ogden, and Sperling, 2007)	

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund