EU-CIRCLE

A pan-European framework for strengthening Critical Infrastructure resilience to climate change

D4.5 CI RESILIENCE INDICATORS

Contractual Delivery Date: 05/2017	**Actual Delivery Date**: 08/2017
Type: Report	**Version**: v0.5

Dissemination Level : Public Deliverable

Statement

This report develops and explains a methodology to elaborate the overall resilience of network assets or network parts. The methodology proposed can also be used in order to elaborate the importance of different resilience capacities and for the evaluation of strategies to strengthen resilience.

EU-CIRCLE is a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653824. Please see http://www.EU-CIRCLE.eu/for more information

Preparation Slip			
	Name	Partner	Date
From	Nenad Petrovic	UVG	
Reviewer	Midori Million	Artelia	
Reviewer	Jean Lecroart	Artelia	
For delivery	Athanasius Sfetsos	NCSRD	

Document Log			
Issue	Date	Comment	Author / Organization
V0.0	12/04/2016 - 13/04/2016	Split	N.Petrovic/UVG V.Borscak/UVG A.Sfetsos/NCSRD
V0.0	18/05/2016	Milan	N.Petrovic/UVG A.Stranjik/UVG C.Pathirage/USAL A.Sfetsos/NCSRD
V0.0	30/10/2016	Initial TOC proposal	N.Petrovic/UVG
V0.0	05/12/2016 - 06/12/2016	Exeter	N.Petrovic/UVG A.Stranjik/UVG A.Sfetsos/NCSRD
		TOC and D4.1	N.Petrovic/UVG
V0.0	09/02/2017	Telco: discussion of involved partners about TOC and further work	N.Petrovic/UVG A.Stranjik/UVG M.Crnko/UVG M.Million/Artelia A.Sfetsos/NCSRD R.Hedel/FhG L.Vamvakeridou-Lyroudia/UNEXE A.Chen/UNEXE L.Shakou/EUC

			C.Pathirage/USAL T.Hisham/USAL M.Skitsas/ADITESS K.Kolowrocki/GMU
V0.1	10/02/2017	V0.1 of Resilience indicators	N.Petrovic/UVG
V0.1	17/02/2017	Comments to V0.1 of Resilience indicators	M.Million/Artelia
V0.1	17/02/2017	Comments to V0.1 of Resilience indicators	C.Strazza/DAPP
V0.1	17/02/2017	Comments to V0.1 of Resilience indicators	I.Koutiva/NCSRD
V0.1	17/02/2017	Comments to V0.1 of Resilience indicators	K.Kolowrocki/GMU
V0.1	17/02/2017	Safety indicators (GMU approach)	K.Kolowrocki/GMU
V0.1	20/02/2017	Comments to V0.1 of Resilience indicators	J.Lecroart/Artelia
V0.1	22/02/2017	Workshop in Zagreb (Croatia) – development of resilience category and possible input data/metadata	N.Petrovic/UVG A.Sfetsos/NCSRD A.Stranjik/UVG M.Crnko/UVG
V0.1	02/03/2017	Expansion of TOC document and Resilience indicators V0.2 (with category and subcategory)	N.Petrovic/UVG
V0.1	03/03/2017	Comments to V0.2 of Resilience indicators with category	C.Strazza/DAPP
V0.1	07/03/2017 - 08/03/2017	Workshop in Nicosia (Cyprus)	Stakeholders
V0.2	09/03/2017	Resilience indicators with metrics V1.0	N.Petrovic/UVG
V0.2	09/03/2017	Workshop in Nicosia (Cyprus): discussion of involved partners about proposed resilience metrics, aggregation methods and resilience indexes calculation	N.Petrovic/UVG A.Sfetsos/NCSRD A.Stranjik/UVG M.Million/Artelia L.Shakou/EUC C.Variannou /EUC T.Hisham/USAL L.Vamvakeridou-Lyroudia/UNEXE A.Chen/UNEXE D.Prior/XUV K.Kolowrocki/GMU A.Blokus-Roszkowska/GMU M.Skitsas/ADITESS
V0.2	08/05/2017 - 10/05/2017	Dubrovnik	N.Petrovic/UVG A.Stranjik/UVG M.Crnko/UVG D.Skanata/UVG A.Sfetsos/NCSRD

			M.Million/Artelia C.Strazza/DAPP L.Shakou/EUC T.Hisham/USAL C.Pathirage/USAL L.Vamvakeridou-Lyroudia/UNEXE A.Chen/UNEXE D.Prior/XUV K.Kolowrocki/GMU A.Blokus-Roszkowska/GMU M.Skitsas/ADITESS M.Matijas/NPRD P.Vitas/NPRD G.Eftychidis/KEMEA I.Gkotsis/KEMEA
V0.2	16/05/2017	Resilience indicators with metrics V2.0	N.Petrovic/UVG
V0.2	25/05/2017	Comments to V2.0 of Resilience indicators with metrics	C.Strazza/DAPP
V0.2	31/05/2017	Aggregation methods	R.Hedel/FhG
V0.2	31/05/2017	Absorption Indicators	K.Kolowrocki/GMU
V0.2	31/05/2017	Resilience Indicators - Reliability Approach (GMU approach)	K.Kolowrocki/GMU
V0.2	13/06/2017	Comments to V2.0 of Resilience indicators with metrics	L.Shakou/EUC
V0.2	14/06/2017	Comments to end user questionnaire	M.Matijas/NPRD
V0.2	15/06/2017	Comments to V2.0 of Resilience indicators with metrics	M.Million/Artelia
V0.3	19/06/2017	Answers to comments related to Resilience indicators V2.0 and new Resilience indicators with metrics V3.0	N.Petrovic/UVG
V0.3	19/06/2017	Resilience Assessment Tool V0.3 and short manual: How to use and full accessing Resilience assessment tool	N.Petrovic/UVG
V0.3	19/06/2017	Proposed changes of Resilience indicators from version V3.0 to V4.0	N.Petrovic/UVG
V0.3	19/06/2017	Telco: discussion of involved partners about Resilience Assessment Tool V0.3 - especially about end-user questionnaire, proposed changes of V0.3 Resilience indicators, inputs from other deliverables and how to use resilience indexes as input in another deliverables	N.Petrovic/UVG M.Million/Artelia J.Lecroart/Artelia L.Shakou/EUC T.Hisham/USAL C.Pathirage/USAL
V0.3	19/06/2017	Comments to V3.0 of Resilience indicators with metrics	L.Shakou/EUC

V0.3	19/06/2017	Comments to V3.0 of Resilience indicators with metrics	M.Million/Artelia
V0.3	19/06/2017	Comments to V3.0 of Resilience indicators with metrics	A.Sfetsos/NCSRD
V0.3	20/06/2017	Comments to proposed changes in Resilience indicators with metrics V0.3	A.Sfetsos/NCSRD
V0.3	20/06/2017	Answers to comments related to Resilience indicators V3.0	N.Petrovic/UVG
V0.3	20/06/2017	"Categories" 10, 3 or 5	A.Sfetsos/NCSRD
V0.4	21/06/2017	Resilience indicators with metrics V4.0	N.Petrovic/UVG
V0.4	22/06/2017	Comments to possible metric of indicator 1.1. Number of hazard and about possibility of two level resilience assessment and how to use resilience indexes in the D4.6 adaptation model	N.Petrovic/UVG M.Million/Artelia L.Shakou/EUC
V0.4	22/06/2017	CIRP integration of Resilience indicators – Resilience assessment tool/model	N.Petrovic/UVG
V0.4	22/06/2017	Implementation of RAT into CIRP	A.Kostaridis/Satways
V0.4	23/06/2017	Resilience index as input in D4.7	F.Anderssohn/MRK
V0.4	26/06/2017	Comments to V4.0 of Resilience indicators with metrics	J.Lecroart/Artelia
V0.4	27/06/2017	Answers on received comments to V4.0 of Resilience indicators with metrics	N.Petrovic/UVG
V0.4	30/06/2017	Comments to V4.0 of Resilience indicators with metrics with suggestion to further development	J.Lecroart/Artelia
V0.4	03/07/2017	Answers on received comments to V4.0 of Resilience indicators with metrics and discussion about network and network of network resilience assessment	N.Petrovic/UVG
V0.4	05/07/2017	Links between D4.3 and D4.5 and possibility for network and network of network level assessment	T.Hisham/USAL
V0.4	24/07/2015	Resilience Assessment model - figure	T.Hisham/USAL
V0.4	07/08/2017	Critical infrastructure & NoN	A.Sfetsos/NCSRD
V0.4	14/08/2017	Ecological impacts/costs	R.Hedel/FhG
V0.4	17/08/2017	List of CIRP Hazards	A.Sfetsos/NCSRD
V0.5	31/08/2017	Resilience indicators with metrics V5.0	N.Petrovic/UVG
V0.5	31/08/2017	Resilience assessment tool V0.5 - Asset	N.Petrovic/UVG

V0.5	31/08/2017	Resilience assessment tool V0.5 – Network and Network of network	N.Petrovic/UVG
V0.6		Final version for open review	N.Petrovic/UVG
V0.7		Final version for official review	N.Petrovic/UVG
V1.0		Final version for submission	N.Petrovic/UVG

Executive Summary

The main purposes of D4.5 is to define Resilience indicators, and the method of quantification of resilience capacities.

The indicators are based on the EU-CIRCLE methodology described in D1.5 and on the Resilience framework, initially described in D4.1 and more specifically described in D4.3. The calculation of the resilience index values is carried out using the methods described in D4.2.

Values of the resilience indexes of the 5 resilience capacities and value of the Overall resilience index will be used later in Cost-effectivenes analysis (D4.7), Business Continuity Model (D4.4) and Adapatation Model (D4.6).

Contents

1 Introduction

Within EU-CIRCLE, resilience indicators and metrics are elaborated on, that allow to (semi-) quantitively assess the resilience of:

- single network assets
- single networks
- networks of networks (NoN)

against climate or other threats.

The resilience measurement is organised on different hierarchy levels (Table 1): Highest level is the overall resilience index ORI as a composite or aggregate indicator depicting the level of achievement in the five aspects related to resilience capacities: anticipation, adaptation, restoration, coping and absorption. The level of achievement within each capacity index is measured with resilience indexes which are partly also calculated as aggregated indexes.

Table 1: Resilience indexes

Level	Description
1	Overall resilience index (ORI)
2	Capacity index (5):
	Anticipatory capacity resilience index (C-ant)
	Absorptive capacity resilience index (C-abs)
	Coping capacity resilience index (C-cop)
	Restorative capacity resilience index (C-rest)
	Adaptive capacity resilience index (C-adapt)
3	Resilience index (R)
4	Resilience subindex (I)

2 Resilience parameters

In order to put resilience into practice, we want to know what properties indicate resilience, how to measure or assess their resilience, and how to manage for resilience. There are several dimensions to resilience that need to be taken into consideration when trying to achieve a holistic approach for infrastructure resilience. One of the components of EU-CIRCLE resilience framework will be the resilience parameters that are related to critical infrastructures and their capacities.

The EU-CIRCLE resilience framework recognises five types of generic resilience parameters. These parameters correspond to the critical infrastructure capacities outlined in section *4.1.5. Capacities of Critical Infrastructure* in D4.1 and and are a way of quantifying these capacities. These parameters are as follows:

1. Anticipation,
2. Absorption,
3. Coping,
4. Restoration, and
5. Adaptation.

Generic indicators are shown in Table 2. These generic indicators are developed in a several levels.

The resilience indicators can be qualitative, quantitative or binary according to the type of data they utilize and may be absolute (e.g., speed of critical infrastructure failure) or relative (e.g., recovery/loss ratio) (Ellis, 2014; Prior, 2014).

Quantitative indicators (e.g. the average annual temperature, the number of projects developed in response to a policy, or the number of bridges constructed) are often preferred for monitoring and evaluation. Quantitative resilience indicators might be most appropriate for technical features of infrastructure. Where quantitative data is not available, and the issue is still considered important for monitoring purposes, qualitative or binary indicators may be utilized.

Qualitative indicators provide narrative or summary information regarding an item of concern. Qualitative indicators may be most appropriate when examining the quality of infrastructure organisation, operation, maintenance or management, or when assessing users interactions with infrastructure. Adaptation indicators, because they relate to processes, are more likely to be qualitative than climate change or climate impact indicators.

Binary indicators have a yes/no answer. Several indicators appropriate for climate adaptation could be binary, e.g. early warning systems in place (yes/no).

In principle, the strategy for measuring resilience is to quantify the difference between the ability of a critical infrastructure to provide services prior to the occurrence of an event and the expected ability of that infrastructure to perform after an event (Bruneau at al., 2003).

Good metrics are (Phillips and Tompkins, 2014):
- Comprehensive,
- Understandable,
- Practical,
- Non-redundant, and
- Minimal.

The above create defensible, transparent and repeatable metrics.

Table 2: Generic resilience indicators

Resilience parameters	Generic resilience indicators
Anticipation	1. Probability of failure 2. Quality of infrastructure 3. Pre-event functionality of the infrastructure 4. Quality/extent of mitigating features 5. Quality of disturbance planning/response 6. Quality of crisis communication/information sharing 7. Learnability
Absorption	1. Systems failure (Unavailability of assets) 2. Severity of failure 3. Just in time delivery - Reliability 4. Post-event functionality 5. Resistance 6. Robustness
Coping	1. Withstanding 2. Redundancy 3. Resourcefulness 4. Response 5. Economic sustainability 6. Interoperability
Restoration	1. Post-event damage assessment 2. Recovery time post-event 3. Recovery/loss ratio 4. Cost of reinstating functionality post-event
Adaptation	1. Substitutability (replacement of service) 2. Adaptability / flexibility 3. Impact reducing availability 4. Consequences reducing availability

A short description of generic resilience indicators is provided below.

Probability of failure: Probability of failure is an estimation of the expected impact and degradation of an infrastructure following a disturbance or shock (Prior, 2014). This probability will vary depending on the nature of the disturbance or shock, but also on the nature of the critical infrastructure itself.

Quality of infrastructure: Quality of infrastructure indicated of how well an infrastructure performs (Prior, 2014). Performance is influenced by design, materials, age, service life, and the quality of management and

maintenance. Infrastructures with lower quality are likely to be less operable after disturbance, and this indicator can be used to describe performance over time.

Pre-event functionality of the infrastructure: Assessing pre-event functionality is an important benchmarking exercise that can be used to inform on how rapidly critical infrastructure function returns after disturbance (Prior, 2014). Knowing the baseline level of functionality of a critical infrastructure is fundamental to assessing and quantifying functionality change both in normal operational circumstances, but especially after a disruption.

Quality/extent of mitigating features: Assessing the quality and extent of features associated with an infrastructure that can mitigate the consequences of disturbance or shock is an important a-priori resilience indicator (Prior, 2014). Mitigating features add to the robustness of the infrastructure, and an early assessment of their quality and extent can be useful in improving these features where the necessity exists. Mitigating features will be specific both to the type of infrastructure and the nature of disturbance the infrastructure is likely to be subject to.

Quality of disturbance planning/response: Technical assessments of infrastructure are perhaps the most obvious when considering resilience, yet considering organisational planning for preparedness and response are also important (Prior, 2014). Assessing the value of pre-determined policies that increase or maintain the quality and functionality of infrastructure can be a useful indicator of resilience. In addition, the nature and availability of repair facilities, resources or personnel can also increase the speed of recovery.

Quality of crisis communications/information sharing: The quality and nature of crisis communication structures, and organisational information sharing between managers of CI and government agencies can be a useful indicator of the CI resilience (Prior, 2014). Where crisis communication methodologies and technologies are of high functionality, their deployment at times of disturbance or shock may limit loss of functionality, and speed up the recovery of infrastructure function. Making either qualitative or quantitative assessments of information sharing processes and practices can be particularly good indicators of the strength of relationships of the managers of infrastructure systems that are characterised by significant interdependencies.

Learnability: Learnability is the ability of organisation to use the lessons of their own and others' experiences to better manage the prevailing circumstances, including using lessons in real time as they emerge (Gibson and Tarrant, 2010).

Systems failure (unavailability of assets): Observing an actual failure in an infrastructure can provide a clear indication of its resilience, and specifically what characteristic of the infrastructure, or its relationship to the disturbance, may have led to the failure (Prior, 2014). Many factors may influence the likelihood that a system fails completely, but also interdependencies, lack of security, poor management and disturbance planning, poor communications, etc. Systems failure can be measured in a binary fashion: fail, or not fail.

Severity of failure: For instance, old or poorly maintained infrastructures are likely to fail such that they lose functionality completely following disturbance, and consequently require a complete rebuild during recovery (Prior, 2014). By contrast, well-managed, newer infrastructure that is designed to cope with disturbance (the most likely to occur in any given location) is likely to suffer less as a result of disturbance, and some functionality may persist.

Just in time delivery – Reliability: Reliability is concerned with ensuring that the infrastructure components are inherently designed to operate under a range of conditions and hence mitigate damage or loss from an event (Cabinet Office, 2011; Watson at al., 2014; Fisher at al., 2010). The tendency of a reliability strategy is to focus only on the events within the specified range, and not events that exceed the range. Reliability cannot therefore be guaranteed, but deterioration can sometimes be managed at a tolerable level until full services can be restored after the event.

Post-event functionality: Measuring functionality of an infrastructure following a disturbance or shock, and comparing this level to the pre event assessment of functionality will provide an excellent indication of CI resilience (Prior, 2014). The closer the level of post-event functionality to the assessed pre-event functionality, the more likely the infrastructure is to be resilient (in relation to a consequential disturbance).

Resistance: The resistance is focused on providing protection (Cabinet Office, 2011; Fisher at al., 2010; Watson at al., 2014). The objective is to prevent damage or disruption by providing the strength or protection to resist the hazard or its primary impact. Resistance have significant weaknesses as protection is often developed against the kind of events that have been previously experienced, or those predicted to occur based on historic records.

Robustness: The robustness component of resilience is the ability to maintain critical operations and functions in the face of crisis (Bush at al., 2009; Fisher at al., 2010; Watson at al., 2014; IEA, 2015). It is directly related to the ability of the system to absorb the impacts of a hazard and to avoid or decrease the importance of the event that could be generated by this hazard. This can be reflected in physical building and infrastructure design (office buildings, power generation and distribution structures, bridges, dams, levees), or in system redundancy and substitution (transportation, power grid, communications networks).

Withstanding: Withstanding is ability to sustain the damage. This includes available dispatchable capacity, available demand response capacity, available link capacity, continuity of critical services, etc. (ARUP, 2014).

Redundancy: Redundancy is concerned with the design and capacity of the network or system (Cabinet Office, 2011; Watson at al., 2014; Fisher at al., 2010; IEA, 2015). The availability of backup installations or spare capacity will enable operations to be switched or diverted to alternative parts of the network in the event of disruptions to ensure continuity of services.

Resourcefulness: Resourcefulness is the ability to skillfully prepare for, respond to and manage a crisis or disruption as it unfolds (Bush at al., 2009; Fisher at al., 2010; Watson at al., 2014; IEA, 2015). Resourcefulness begins prior to an event and continues into the response phase. It comprises the steps taken prior to an event to prepare employees and management for possible threats and the application of the training and planning once an event occurs. This includes identifying courses of action, business continuity planning, training, supply chain management, prioritizing actions to control and mitigate damage, and effectively communicating decisions.

Response: Response have aims to enable a fast and effective response to disruptive events (Cabinet Office, 2011; Watson at al., 2014). The effectiveness of this element is determined by the thoroughness of efforts to plan, prepare and exercise in advance of events. Some owners of critical infrastructure understand the weaknesses in their networks and systems and have arrangements in place to respond quickly to restore services.

Post-event damage assessment: Geographic information systems (GIS) and remote sensing technologies can, and have been used in post disaster damage assessments (Prior, 2014). Such technologies can be used to yield quantitative measures of damage to many forms of infrastructure, and therefore give a direct idea of the robustness of infrastructure affected by the disturbance.

Interoperability: Interoperability is ability to cooperate at all levels with neighboring cities/states and other levels of government of critical systems and procedures. Interoperability needs to be assessed at multiple levels (UNISDR, 2014).

Recovery time post-event: Possibly the most well-known indicator of resilience in CI, the recovery time post-event is a measure of the amount of time it takes for an infrastructure to be brought back to its pre-event level of functionality (Prior, 2014).

Recovery/loss ratio: Closely related to 'recovery time post-event', the recovery/loss ratio is a calculation of speed of recovery based on the severity of loss (Prior, 2014). More severe loss, or decrease in functionality,

would generally be associated with a longer recovery time. However, for CI that is rated as having a high level of resilience, the speed at which recovery occurs may be higher than similar infrastructure with lower rated resilience.

Cost of reinstating functionality post-event: The cost of returning infrastructure to pre-event functionality can be used as an indirect measure of an infrastructure's resilience (Prior, 2014). This measure assumes that a greater expense (relative to the value of the infrastructure alone, not the value of the service the infrastructure provides to society) equates to more damage, and therefore lower resilience in the infrastructure.

Substitutability: Substitutability is an aspect of a CI system's redundancy, and a key characteristic associated with resilience in infrastructure (Prior, 2014). Substitutability reflects the possibility that the functional aspects of an infrastructure or infrastructure system can be replaced by back-up infrastructure or by other components in the system.

Adaptability and flexibility: Adaptability and flexibility are capacity or ability to change while maintaining or improving functionality, adopting alternative strategies quickly, responding to changing conditions in time, designing open and flexible structures (RAMSES, 2016).

Impact reducing availability: Impact reducing availability is availability of adaptive processes that reducing impact of climate changes, e.g. re-allocation of facilities, building new facilities in according to climate-ready standards, protection of existing critical infrastructures, etc (Barami, 2013).

Consequences reducing availability: Consequences reducing availability is availability of adaptive processes that reducing consequences of climate changes, e.g. re-routing transportation flows, developing flexibility of networks, etc (Barami, 2013).

Economic sustainability: Local communities are interested in ensuring they develop and maintain a vibrant and thriving economy, even amid hazard events (NIST, (2), 2015). Factors that might affect a community's economic sustainability after hazard events include the degree to which the local economy depends on a single industry.

3 Resilience indicators

EU-CIRCLE Resilience indicators with categories and subcategories are shown in Table 3.

Table 3: EU-CIRCLE Resilience indicators with categories and subcategories

Resilience Capacities	Resilience Indicators	Resilience Categories / Subcategories	Type of data		Input / Estimation		Related to		
			Number	Category	End-user	Model/CIRP	Asset	Network	Network of network
1. Anticipation	1.1. Number of hazards	1.1.1. Number of hazards related to asset or network (awareness)	x		x		x	x	x
	1.2. Quality / extent of mitigating features	1.2.1. Equipment and procedures for hazard mitigation exist		yes/no	x		x	x	x
		1.2.1.1. Procedures are documented		yes/no	x		x	x	x
		1.2.1.2. Procedures are regulary revised		yes/no	x		x	x	x
		1.2.1.3. How many hazards is cover	x		x		x	x	x
		1.2.1.4. How many assets is cover	x		x			x	x
		1.2.1.5. Network is cover		yes/no	x			x	x
		1.2.1.6. Hydro/meteo/climate changes are covered		yes/no	x		x	x	x
		1.2.1.7. Dependencies and interdependencies are covered		yes/no	x		x	x	x
		1.2.2. Early warning system exists		yes/no	x		x	x	x
		1.2.2.1. System is tested		yes/no	x		x	x	x
		1.2.2.2. System is up to date		yes/no	x		x	x	x
		1.2.2.3. How many hazards it cover	x		x		x	x	x
		1.2.2.4. How many assets it cover	x		x			x	x
		1.2.2.5. Network is cover		yes/no	x			x	x
		1.2.3. How many time installed capacity exceedes demand	x		x		x	x	x
	1.3. Quality of distrubance planing / response	1.3.1. Operational response plans exist		yes/no	x		x	x	x
		1.3.1.1. Plans are tested		yes/no	x		x	x	x
		1.3.1.2. Plans are trainied		yes/no	x		x	x	x
		1.3.1.3. Plans are up to date		yes/no	x		x	x	x
		1.3.1.4. How many hazards it cover	x		x		x	x	x
		1.3.1.5. How many assets it cover	x		x			x	x
		1.3.1.6. Network is cover		yes/no	x			x	x
		1.3.1.7. Hydro/meteo/climate changes are covered		yes/no	x		x	x	x
		1.3.1.8. Dependencies and interdependencies are covered		yes/no	x		x	x	x
	1.4. Communication Systems / Information sharing	1.4.1. Plans of communication and information sharing exist		yes/no	x		x	x	x
		1.4.1.1. Plans are tested		yes/no	x		x	x	x
		1.4.1.2. Plans are up to date		yes/no	x		x	x	x
		1.4.1.3. Network is cover		yes/no	x			x	x
		1.4.2. Communication system exist		yes/no	x		x	x	x

		1.4.2.1. System is tested		yes/no	x		x	x	x
		1.4.2.2. How many assets it cover	x		x			x	x
		1.4.2.3. Network is cover		yes/no	x			x	x
		1.4.3. Backup of communication system exist		yes/no	x		x	x	x
	1.5. Learnability / Training	1.5.1. Training system exist		yes/no	x		x	x	x
		1.5.1.1. How many hazards is covered by training	x		x		x	x	x
		1.5.1.2. Hours of training	x		x		x	x	x
		1.5.1.3. Training programm is tested		yes/no	x		x	x	x
		1.5.1.4. Training programm is up to date		yes/no	x		x	x	x
		1.5.1.5. Last training was within a year		yes/no	x		x	x	x
		1.5.2. Number of training people	x		x		x	x	x
		1.5.3. Trainig with other CI exist		yes/no	x		x	x	x
2. Absorption	2.1. System failure (integrtity of the CI affected)	2.1.1. Number of assets fully damaged (beyond reparability)	x			D3.4		x	x
		2.1.2. Number of assets partially damaged	x			D3.4		x	x
		2.1.3. Number of assets with a [over] certain percent (%) or range of damages	x			D3.4		x	x
		2.1.4. Time that CI is not able to serve its intended function	x			D3.4	x	x	x
		2.1.5. Costs of damaged assets	x			D3.4	x	x	x
	2.2. Severity of failure (services of the CI affected)	2.2.1. Loss for certain hazards level	x			Operational damage function	x	x	x
		2.2.2. Reduced network capacity	x			D3.4		x	x
		2.2.2.1. Connectivity Loss (CL)	x			D3.4		x	x
		2.2.2.2. Service Flow Reduction (SFR)	x			D3.4		x	x
		2.2.3. Number of assets fail	x		x			x	x
		2.2.4. Number of assets fully damaged (beyond reparability)	x			D3.4		x	x
		2.2.5. Number of assets partially damaged	x			D3.4		x	x
		2.2.6. Number of assets with a [over] certain percent (%) or range of damages	x			D3.4		x	x
		2.2.7. Loss of income as a result of not servicing demand	x		x		x	x	x
		2.2.8. Total time that person(s) is left without any CI services	x			D3.4	x	x	x
		2.2.9. Total time that person(s) is left without two or more CI services	x			D3.4	x	x	x
		2.2.10. How often in the future climate, CI thresholds will be exceeded	x			D2.3	x	x	x
	2.3. Vulnerability	2.3.1. Vulnerability assessment exist		yes/no	x		x	x	x
		2.3.1.1. How many hazards it covers	x		x		x	x	x
		2.3.1.2. How many assets it covers	x		x			x	x
		2.3.1.3. Network is cover		yes/no	x			x	x
		2.3.1.4. Hydro/meteo/climate changes are covered		yes/no	x		x	x	x
		2.3.1.5. Dependencies and interdependencies are covered		yes/no	x		x	x	x
	2.4. Resistance	2.4.1. Probability of failure	x			D3.4	x	x	x
		2.4.2. Failure > 50% for certain hazards level		yes/no		Operational damage function	x	x	x

		2.4.3. Aging of CI	x		x		x	x	x
		2.4.4. Safety design standards for respective hazards are applied		yes/no	x		x	x	x
		2.4.4.1. How many relevant standards is applied	x		x		x	x	x
		2.4.4.2. How many hazards is cover	x		x		x	x	x
		2.4.4.3. How many assets is cover	x		x			x	x
		2.4.4.4. Network is cover		yes/no	x			x	x
		2.4.5. Maintenance is regular		yes/no	x		x	x	x
		2.4.5.1. Maintenance plan exist		yes/no	x		x	x	x
		2.4.5.2. Maintenance plan is in line with the Construction project		yes/no	x		x	x	x
		2.4.5.3. Maintenance is performed according to the plan		yes/no	x		x	x	x
		2.4.5.4. Maintenance is documented		yes/no	x		x	x	x
		2.4.5.5. Critical infrastructure is fully operational according to specification		yes/no	x		x	x	x
	2.5. Robustnes	2.5.1. Asset backup exist		yes/no	x		x		
		2.5.2. Service replacement exist		yes/no	x		x	x	x
	3.1. Redundancy	3.1.1. How many assets have backup	x		x		x	x	x
		3.1.2. After how much time backup is available	x		x		x	x	x
		3.1.3. How long backup is available	x		x		x	x	x
	3.2. Resourcefulness	3.2.1. Availability of interconnected assets (provide reserve services, could be different CI)	x			D3.4	x	x	x
	3.3. Response	3.3.1. Special response plan exist		yes/no	x		x	x	x
		3.3.1.1. Plans are tested		yes/no	x		x	x	x
		3.3.1.2. Plans are trainied		yes/no	x		x	x	x
		3.3.1.3. Plans are up to date		yes/no	x		x	x	x
		3.3.1.4. How many hazard it covers	x		x		x	x	x
		3.3.1.5. How many assets it covers	x		x			x	x
		3.3.1.6. Network is cover		yes/no	x			x	x
		3.3.1.7. Hydro/meteo/climate changes are covered		yes/no	x		x	x	x
		3.3.1.8. Dependencies and interdependencies are covered		yes/no	x		x	x	x
3. Coping		3.3.2. Time needed to responese	x			D3.4	x	x	x
		3.3.3. Emergency plans under Climate Hazards (in the context of climate change) exists		yes/no	x		x	x	x
		3.3.3.1. Plans are tested		yes/no	x		x	x	x
		3.3.3.2. Plans are trainied		yes/no	x		x	x	x
		3.3.3.3. Plans are up to date		yes/no	x		x	x	x
		3.3.3.4. How many hazards it cover	x		x		x	x	x
		3.3.3.5. How many assets it cover	x		x			x	x
		3.3.3.6. Network is cover		yes/no	x			x	x
		3.3.3.7. Hydro/meteo/climate changes are covered		yes/no	x		x	x	x
		3.3.3.8. Dependencies and interdependencies are covered		yes/no	x		x	x	x
		3.3.4. Business continuity plans under Climate Hazards (in the context of climate change) exists		yes/no	x		x	x	x
		3.3.4.1. Plans are tested		yes/no	x		x	x	x
		3.3.4.2. Plans are trainied		yes/no	x		x	x	x

		3.3.4.3. Plans are up to date		yes/no	x		x	x	x
		3.3.4.4. How many hazards it cover	x		x		x	x	x
		3.3.4.5. How many assets it cover	x		x			x	x
		3.3.4.6. Network is cover		yes/no	x			x	x
		3.3.4.7. Hydro/meteo/climate changes are covered		yes/no	x		x	x	x
		3.3.4.8. Dependencies and interdependencies are covered		yes/no	x		x	x	x
	3.4. Economics of response	3.4.1. Cost of response (for CI only)	x		x		x	x	x
		3.4.2. Costs for replacements of services	x		x		x	x	x
		3.4.3. Backup cost	x		x		x	x	x
	3.5. Interoperability with public sector	3.5.1. Procedures exist		yes/no	x		x	x	x
		3.5.2. Communication system exist		yes/no	x		x	x	x
		3.5.3. Joint action plans exist		yes/no	x		x	x	x
		3.5.3.1. Plans are tested		yes/no	x		x	x	x
		3.5.3.2. Plans are trainied		yes/no	x		x	x	x
		3.5.3.3. Plans are up to date		yes/no	x		x	x	x
4. Restoration	4.1. Post-event damage assessment	4.1.1. Percentage change from base state	x			Structural damage function	x	x	x
	4.2. Recovery time	4.2.1. Special recovery plan exist		yes/no	x		x	x	x
		4.2.1.1. How many hazards it covers	x		x		x	x	x
		4.2.1.2. How many assets it covers	x		x			x	x
		4.2.1.3. Network is cover		yes/no	x			x	x
		4.2.1.4. Hydro/meteo/climate changes are covered		yes/no	x		x	x	x
		4.2.1.5. Dependencies and interdependencies are covered		yes/no	x		x	x	x
		4.2.2. Time needed to recovery	x		x		x	x	x
	4.3. Economics of restoration	4.3.1. Cost of restoration	x		x		x	x	x
		4.3.2. Loss of income during restoration	x		x		x	x	x
		4.3.3. Loss due to possible penalties from violating service level agreements with buyers	x		x		x	x	x
		4.3.4. Costs for replacements of services	x		x		x	x	x
		4.3.5. Maintenance costs after hazard	x		x		x	x	x
		4.3.6. Cost of reputation	x		x		x	x	x
		4.3.7. Insurance costs	x		x		x	x	x
5. Adaptation	5.1. Substitutability	5.1.1. Replacement of asset is possible		yes/no	x		x		
		5.1.1.1. Technical is possible		yes/no	x		x		
		5.1.1.2. Financial is possible		yes/no	x		x		
		5.1.2. Replacement of service is possible		yes/no	x		x	x	x
		5.1.2.1. Technical is possible		yes/no	x		x	x	x
		5.1.2.2. Financial is possible		yes/no	x		x	x	x
	5.2. Adaptability and flexibility	5.2.1. Adaptation to new climate conditions on time is possible	x		x		x	x	x
		5.2.2. Adaptation plan exist		yes/no	x		x	x	x
		5.2.2.1. How many hazards it covers	x		x		x	x	x
		5.2.2.2. How many assets it covers	x		x			x	x
		5.2.2.3. Network is cover		yes/no	x			x	x

		5.2.2.4. Hydro/meteo/climate changes are covered		yes/no	x		x	x	x
		5.2.2.5. Dependencies and interdependencies are covered		yes/no	x		x	x	x
	5.3. Impact / consequences reducing availability	5.3.1. Re-locate of facilities is possible		yes/no	x		x	x	x
		5.3.2. Building new facilities according to climate-ready standards		yes/no	x		x	x	x
	5.4. Economics of adaptation	5.4.1. New investments take consider a climate change		yes/no	x		x	x	x
		5.4.2. How many new clients can be reached by improving the service / climate adaptation polices	x		x		x	x	x
		5.4.3. Reputation is increased by implementing climate change adaptation options		yes/no	x		x	x	x
		5.4.4. Decisions on adaptation adopt due to market forces		yes/no	x		x	x	x

4 Metrics of Resilience indicators

EU-CIRCLE Resilience indicators metrics are shown in Table 4 to Table 8.

Table 4. Metrics of resilience indicators for anticipative capacities

Resilience Indicators	Resilience Categories / Subcategories	Metrics
1.1. Number of hazards	1.1.1. Number of hazards related to asset or network (awareness)	I = (number of identified hazards by end-user / number of total potential hazards impacting area of CI)*10
1.2. Quality / extent of mitigating features	1.2.1. Equipment and procedures for hazard mitigation exist	I = aggregated value (for No I = 0)
	1.2.1.1. Procedures are documented	i = 0 or 10
	1.2.1.2. Procedures are regulary revised	i = 0 or 10
	1.2.1.3. How many hazards is cover	i = (number of hazards that procedures covered / number of hazards impacting area of CI)*10
	1.2.1.4. How many assets is cover	i = (number of assets that procedures covered / total number of assets)*10
	1.2.1.5. Network is cover	i = 0 or 10
	1.2.1.6. Hydro/meteo/climate changes are covered	i = 0 or 10
	1.2.1.7. Dependencies and interdependencies are covered	i = 0 or 10
	1.2.2. Early warning system exists	I = aggregated value (for No I = 0)
	1.2.2.1. System is tested	i = 0 or 10
	1.2.2.2. System is up to date	i = 0 or 10
	1.2.2.3. How many hazards it cover	i = (number of hazards covered by system / number of hazards impacting area of CI)*10
	1.2.2.4. How many assets it cover	i = (number of assets covered by system / total number of assets)*10
	1.2.2.5. Network is cover	i = 0 or 10
	1.2.3. How many time installed capacity exceedes demand	I = (month per year that capacity exceedes demand / 12)*10
1.3. Quality of distrubance planing / response	1.3.1. Operational response plans exist	I = aggregated value (for No I = 0)
	1.3.1.1. Plans are tested	i = 0 or 10
	1.3.1.2. Plans are trainied	i = 0 or 10
	1.3.1.3. Plans are up to date	i = 0 or 10
	1.3.1.4. How many hazards it cover	i = (number of hazards covered by plans / number of hazards impacting area of CI)*10
	1.3.1.5. How many assets it cover	i = (number of assets covered by plans / total number of assets)*10
	1.3.1.6. Network is cover	i = 0 or 10
	1.3.1.7. Hydro/meteo/climate changes are covered	i = 0 or 10
	1.3.1.8. Dependencies and interdependencies are covered	i = 0 or 10
1.4. Communication Systems / Information sharing	1.4.1. Plans of communication and information sharing exist	I = aggregated value (for No I = 0)
	1.4.1.1. Plans are tested	i = 0 or 10
	1.4.1.2. Plans are up to date	i = 0 or 10
	1.4.1.3. Network is cover	i = 0 or 10
	1.4.2. Communication system exist	I = aggregated value (for No I = 0)
	1.4.2.1. System is tested	i = 0 or 10
	1.4.2.2. How many assets it cover	i = (number of assets covered by system / total number of assets)*10
	1.4.2.3. Network is cover	i = 0 or 10
	1.4.3. Backup of communication system exist	I = 0 or 10

1.5. Learnability / Training	1.5.1. Training system exist	I = aggregated value (for No I = 0)
	1.5.1.1. How many hazards is covered by training	i = (number of hazards covered by training / number of hazards impacting area of CI)*10
	1.5.1.2. Hours of training	i = (performed hours of training / necessary (planned) hours of training)*10
	1.5.1.3. Training programm is tested	i = 0 or 10
	1.5.1.4. Training programm is up to date	i = 0 or 10
	1.5.1.5. Last training was within a year	i = 0 or 10
	1.5.2. Number of trained people	I = (number of training people/number of related people)*10
	1.5.3. Trainig with other CI exist	I = 0 or 10

Table 5. Metrics of resilience indicators for absorptive capacities

Resilience Indicators	Resilience Categories / Subcategories	Metrics
2.1. System failure (integrtity of CI affected)	2.1.1. Number of assets fully damaged (beyond reparability)	I = (1 - (number of assets fully damaged / total number of assets))*10
	2.1.2. Number of assets partially damaged	I = (1 - (number of assets partially damaged / total number of assets))*10
	2.1.3. Number of assets with a [over] certain percent (%) or range of damages	I = (1 - (number of assets > certain %) / total number of assets))*10
	2.1.4. Time that CI is not able to serve its intended function	I = (acceptable time / total time out of function)*10 ; (Imax = 10)
	2.1.5. Costs of damaged assets	I = (acceptable cost / total cost)*10 ; (Imax = 10)
2.2. Severity of failure (services of the CI affected)	2.2.1. Loss for certain hazards level	I = (100 - p) / 10
	2.2.2. Reduced network capacity	I = aggregated value
	2.2.2.1. Connectivity Loss (CL)	i = (1 - CL) * 10
	2.2.2.2. Service Flow Reduction (SFR)	i = SFR * 10
	2.2.3. Number of assets fail	I = (1 - (number of assets / total number of assets))*10
	2.2.4. Number of assets fully damaged (beyond reparability)	I = (1 - (number of assets / total number of assets))*10
	2.2.5. Number of assets partially damaged	I = (1 - (number of assets / total number of assets))*10
	2.2.6. Number of assets with a [over] certain percent (%) or range of damages	I = (1 - (number of assets > certain %) / total number of assets))*10
	2.2.7. Loss of income as a result of not servicing demand	I = (1 - (total loss / acceptable loss))*10 ; (Imin = 0)
	2.2.8. Total time that person(s) is left without any CI services	I = (1 - (total time / acceptable time))*10 ; (Imin = 0)
	2.2.9. Total time that person(s) is left without two or more CI services	I = (1 - (total time / acceptable time))*10 ; (Imin = 0)
	2.2.10. How often in the future climate, CI thresholds will be exceeded	I = (1 - (expectable number per year / acceptable number per year))*10 ; (Imin = 0)
2.3. Vulnerability	2.3.1. Vulnerability assessment exist	I = aggregated value (for No I = 0)
	2.3.1.1. How many hazards it covers	i = (number of covered hazards / number of hazards impacting area of CI)*10
	2.3.1.2. How many assets it covers	i = (number of assets that assessment covered / total number of assets)*10
	2.3.1.3. Network is cover	i = 0 or 10
	2.3.1.4. Hydro/meteo/climate changes are covered	i = 0 or 10
	2.3.1.5. Dependencies and interdependencies are covered	i = 0 or 10
2.4. Resistance	2.4.1. Probability of failure	I = (100 - p) / 10
	2.4.2. Failure > 50% for certain hazards level	I = 0 or 10 (for p <= 50)
	2.4.3. Aging of CI	I = (1 - (age of critical infrastructure / infrastructure lifetime))*10 ; (Imin = 0)
	2.4.4. Safety design standards for respective hazards are applied	I = aggregated value (for No I = 0)
	2.4.4.1. How many relevant standards is applied	i = (number of applied standards / number of relevant standards)*10
	2.4.4.2. How many hazards is cover	i = (number of hazards that applied standards covered / number of hazards impacting area of CI)*10
	2.4.4.3. How many assets is cover	i = (number of assets that applied standards covered / total number of assets)*10
	2.4.4.4. Network is cover	i = 0 or 10
	2.4.5. Maintenance is regular	I = aggregated value (for No I = 0)
	2.4.5.1. Maintenance plan exist	i = 0 or 10
	2.4.5.2. Maintenance plan is in line with the Construction	i = 0 or 10

	project	
	2.4.5.3. Maintenance is performed according to the plan	i = 0 or 10
	2.4.5.4. Maintenance is documented	i = 0 or 10
	2.4.5.5. Critical infrastructure is fully operational according to specification	i = 0 or 10
2.5. Robustnes	2.5.1. Asset backup exist	I = 0 or 10
	2.5.2. Service replacement exist	I = 0 or 10

Table 6. Metrics of resilience indicators for coping capacities

Resilience Indicators	Resilience Categories / Subcategories	Metrics
3.1. Redundancy	3.1.1. How many assets have backup	I = (number of assets with backup / total number of assets)*10
	3.1.2. After how much time backup is available	I = (1 - (real time / acceptable time))*10 ; (Imin = 0)
	3.1.3. How long backup is available	I = (real time / acceptablel time)*10 ; (Imax = 10)
3.2. Resourcefulness	3.2.1. Availability of interconnected assets (provide reserve services, could be different CI)	I = (number of interconnected assets / total number of assets)*10
3.3. Response	3.3.1. Special response plan exist	I = aggregated value (for No I = 0)
	3.3.1.1. Plans are tested	i = 0 or 10
	3.3.1.2. Plans are trainied	i = 0 or 10
	3.3.1.3. Plans are up to date	i = 0 or 10
	3.3.1.4. How many hazards it covers	i = (number of hazards that plan covered / number of hazards impacting area of CI)*10
	3.3.1.5. How many assets it covers	i = (number of assets that plan covered / total number of assets)*10
	3.3.1.6. Network is cover	i = 0 or 10
	3.3.1.7. Hydro/meteo/climate changes are covered	i = 0 or 10
	3.3.1.8. Dependencies and interdependencies are covered	i = 0 or 10
	3.3.2. Time needed to response	I = (1 - (real time / acceptable time)*10 ; (Imin = 0)
	3.3.3. Emergency plans under Climate Hazards (in the context of climate change) exists	I = aggregated value (for No I = 0)
	3.3.3.1. Plans are tested	i = 0 or 10
	3.3.3.2. Plans are trainied	i = 0 or 10
	3.3.3.3. Plans are up to date	i = 0 or 10
	3.3.3.4. How many hazards it cover	i = (number of hazards that plan covered / number of hazards impacting area of CI)*10
	3.3.3.5. How many assets it cover	i = (number of assets that plan covered / total number of assets)*10
	3.3.3.6. Network is cover	i = 0 or 10
	3.3.3.7. Hydro/meteo/climate changes are covered	i = 0 or 10
	3.3.3.8. Dependencies and interdependencies are covered	i = 0 or 10
	3.3.4. Business continuity plans under Climate Hazards (in the context of climate change) exists	I = aggregated value (for No I = 0)
	3.3.4.1. Plans are tested	i = 0 or 10
	3.3.4.2. Plans are trainied	i = 0 or 10
	3.3.4.3. Plans are up to date	i = 0 or 10
	3.3.4.4. How many hazards it cover	i = (number of hazards that plan covered / number of hazards impacting area of CI)*10
	3.3.4.5. How many assets it cover	i = (number of assets that plan covered / total number of assets)*10
	3.3.4.6. Network is cover	i = 0 or 10
	3.3.4.7. Hydro/meteo/climate changes are covered	i = 0 or 10
	3.3.4.8. Dependencies and interdependencies are covered	i = 0 or 10
3.4. Economics of response	3.4.1. Cost of response (for CI only)	I = (1 - (total cost / acceptable cost)*10 ; (Imin = 0)
	3.4.2. Costs for replacements of services	I = (1 - (total cost / acceptable cost)*10 ; (Imin = 0)
	3.4.3. Backup cost	I = (1 - (total cost / acceptable cost)*10 ; (Imin = 0)
3.5. Interoperability with public sector	3.5.1. Procedures exist	I = 0 or 10

	3.5.2. Communication system exist	I = 0 or 10
	3.5.3. Joint action plans exist	I = aggregated value (for No I = 0)
	3.5.3.1. Plans are tested	i = 0 or 10
	3.5.3.2. Plans are trainied	i = 0 or 10
	3.5.3.3. Plans are up to date	i = 0 or 10

Table 7. Metrics of resilience indicators for restorative capacities

Resilience Indicators	Resilience Categories / Subcategories	Metrics
4.1. Post-event damage assessment	4.1.1. Percentage change from base state	I = (100 - Percentage) / 10
4.2. Recovery time	4.2.1. Special recovery plan exist	I = aggregated value (for No I = 0)
	4.2.1.1. How many hazards it covers	i = (number of hazards that plan covered / number of hazards impacting area of CI)*10
	4.2.1.2. How many assets it covers	i = (number of assets / total number of assets)*10
	4.2.1.3. Network is cover	i = 0 or 10
	4.2.1.4. Hydro/meteo/climate changes are covered	i = 0 or 10
	4.2.1.5. Dependencies and interdependencies are covered	i = 0 or 10
	4.2.2. Time needed to recovery	I = (1 - (real time / acceptable time)*10 ; (Imin = 0) Time unit is flexible and is determined by the end user - can be minute, hour or day
4.3. Economics of restoration	4.3.1. Cost of restoration	I = (1 - (real cost / acceptable cost)*10 ; (Imin = 0)
	4.3.2. Loss of income during restoration	I = (1 - (real cost / acceptable cost)*10 ; (Imin = 0)
	4.3.3. Loss due to possible penalties from violating service level agreements with buyers	I = (1 - (real cost / acceptable cost)*10 ; (Imin = 0)
	4.3.4. Costs for replacements of services	I = (1 - (real cost / acceptable cost)*10 ; (Imin = 0)
	4.3.5. Maintenance costs after hazard	I = (1 - (real cost / acceptable cost)*10 ; (Imin = 0)
	4.3.6. Cost of reputation	I = (1 - (real cost / acceptable cost)*10 ; (Imin = 0)
	4.3.7. Insurance costs	I = (1 - (real cost / acceptable cost)*10 ; (Imin = 0)

Table 8. Metrics of resilience indicators for adaptive capacities

Resilience Indicators	Resilience Categories / Subcategories	Metrics
5.1. Substitutability	5.1.1. Replacement of asset is possible	I = 0 or 10 (if both i = yes)
	5.1.1.1. Technical is possible	i = yes or no
	5.1.1.2. Financial is possible	i = yes or no
	5.1.2. Replacement of service is possible	I = 0 or 10 (if both i = yes)
	5.1.2.1. Technical is possible	i = yes or no
	5.1.2.2. Financial is possible	i = yes or no
5.2. Adaptability and flexibility	5.2.1. Adaptation to new climate conditions on time is possible	I = (1 - (real time needed for adaptation / acceptable time of adaptation)*10 ; (Imin = 0)
	5.2.2. Adaptation plan exist	I = aggregated value (for No I = 0)
	5.2.2.1. How many hazards it covers	i = (number of hazards that plan covered / number of hazards impacting area of CI)*10
	5.2.2.2. How many assets it covers	i = (number of assets / total number of assets)*10
	5.2.2.3. Network is cover	i = 0 or 10
	5.2.2.4. Hydro/meteo/climate changes are covered	i = 0 or 10
	5.2.2.5. Dependencies and interdependencies are covered	i = 0 or 10
5.3. Impact / consequences reducing availability	5.3.1. Re-locate of facilities is possible	I = 0 or 10
	5.3.2. Building new facilities according to climate-ready standards	I = 0 or 10
5.4. Economics of adaptation	5.4.1. New investments take consider a climate change	I = 0 or 10
	5.4.2. How many new clients can be reached by improving the service / climate adaptation polices	I = (p * 2) / 10 ; (Imax = 10)
	5.4.3. Reputation is increased by implementing climate change adaptation options	I = 0 or 10
	5.4.4. Decisions on adaptation adopt due to market forces	I = 0 or 10

5 Resilience assessment model

The shock or hazard impact of a disaster on overall CI service delivery shows considerable differences around time and space and are the result of the interaction between the various CI sectors as the various sectors have different capacities to absorb, recover and adapt to these diverse types of hazards. These different capacities can be defined by a range of different resilience indicators as indicated in D4.1 called the AARCA resilience capacities (absorptive, anticipatory, restorative, coping and adaptive capacities).

As mentioned previously CI asset networks are a combination of physical and social systems containing elements that can be both hard and soft systems. Any CI asset has a limited capacity to prevent, withstand and recover from a hazard event based on several factors such as the size of the hazard event, the vulnerability of the asset and resilience capacity of the asset. In the simulation framework these hazard events will be termed as shocks that have an impact on the functional or system performance of the asset (or asset network depending on the unit of analysis). The shock will impact the system performance of the CI asset in part due to the type of hazard/shock, the size and duration of exposure to that hazard/shock and will be represented in the framework as a loss to system performance.

The model will be able to evaluate both short-term shock events (in existing climatic conditions) and longer-term stress events (climate change related). The model will allow assessment at various scales: network of network, network or asset. The capacities measures in each case need to include additional indicators at each level.

The Resilience assessment model consists of a range of questions across the capacities shown in Figure 1 Once the relevant questions have been answered, weights can be applied at any of the category, capacity or measure level as determined by the model, data or expert opinion. These weighs should be a percentage value and must add to 100% across each set of indicators considered.

The weights will allow the user to place importance to one capacity over another. For example, one may determine that ‘anticipative capacity’ is more important than ‘adaptive’ and as such, the user should allocate a larger weight to that category to generate the correct score. It is important to note that the weights are subjective and will be based on user preference. In all instances, the individual scores for each question can be viewed and interrogated to determine reasons behind a specific principle or dimension score.

In summary, the approach to conducting a Resilience assessment model as follows:

1 - Determine the context of the assessment.
2 - Undertake the assessment using the questions relative to the context above and select scores for each.
3 - Apply weightings to the scores, as required.
4 - Generate resilience indexes for categories and capacities and an overall resilience index.
The process is described in diagram 4.1 which includes an initial determination of the context of resilience assessment model. This is then followed by the description of a Resilience indexes (*Table x.x*) developed in D4.5 which combine to form a resilience score from 10 (very high resilience) to 0 (very low resilience).

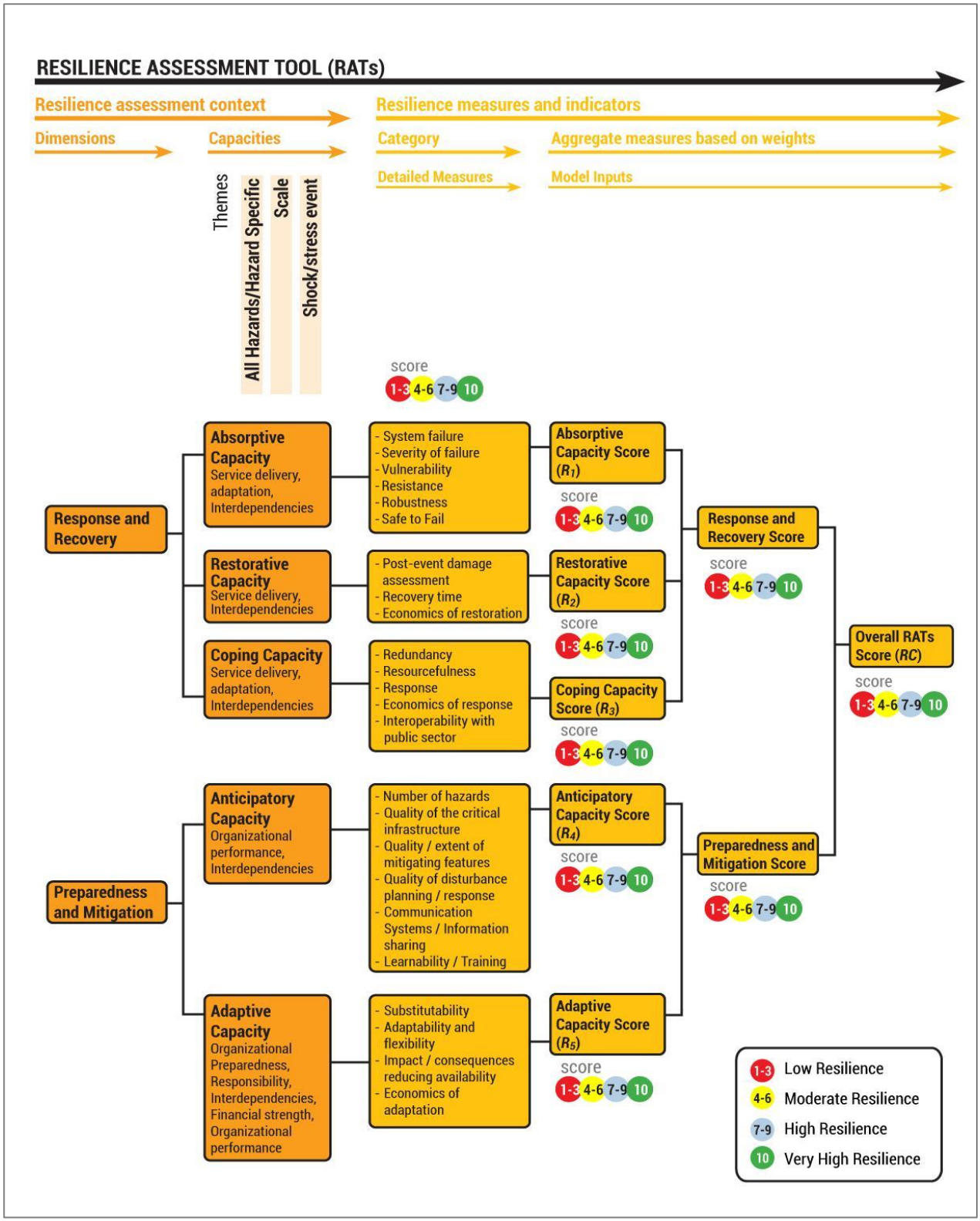


Figure 1: The Resilience Assessment Model and calculation of resilience capacities indexes

6 Meaning of indicator values

Meaning of indicator indexes values are shown in Table 9.

Table 9. Description of values of Resilience Indexes

Index value	Description
10	Very high resilience – meets all standards and requirements for continued service operation in the most difficult conditions
7-9	High resilience – acceptable performance in relation to capacities, some improvements can be made
4-6	Moderate resilience – less than desirable performance and specific improvements should be prioritised
1-3	Low resilience – poor performance and specific improvements across all capacities required urgently
0	Very low resilience – resilience practically not exist, improvements required urgently, without delay

The values of the Resilience Indexes represent variables based on which to evaluate the opportunities and make decisions on the necessary adaptations (D4.6 Adaptation model and D4.7 Cost-effectiveness model) and ensure business continuity (D4.4 Business continuity model).

7 Aggregation methods

Several methods for calculating weights and for aggregation have been introduced in the Deliverable D4.2 *Prioritisation module:*

- Rank order approaches,
- Direct quantitative valuation,
- Pairwise comparison,
- Multi-Attributive Utility Theory (MAUT),
- Analytical Hierarchy Process (AHP).

However, during the time of preparation of D4.2 only little information was available on the actual relevant resilience indicators and their positioning in the hierarchy. Therefore, D4.2 was a rather generic introduction. It is not the purpose of this working paper to reprint the methods described already in D4.2, therefore, this discussion will refer extensively to D4.2 and should be read in connection with this deliverable.

The following table (Table 10) gives an overview over the methods introduced in D4.2 together with some initial assessments on pro&contra. In this table, one additional method – compromise programming – has been introduced here, which has not been explained before in D4.2. This approach is explained further in this document.

Table 10: Overview over the aggregation methods

Purpose	Approach	Pro & contra
Aggregation	**Simple weighted sum**	+ simple, low requirements to stakeholders - no explicit consideration of compensation
	Compromise programming $(p > 1)$	+ technically simple to implement + explicit consideration of compensation - estimation of parameter p through expert required
	Analytical Hierarchy Process (AHP)	+ well established/validated procedure - very time-consuming process for stakeholders
Elicitation of indicator weights	**Calculation based on rank order taken from expert opinion**	+ least effort for decision maker + technically simple to implement - least scientifically validated
	Calculation from direct quantitative valuation based on expert opinion	+ little effort for decision maker - easy to implement
	Calculation from complete AHP or its core element pairwise comparison	+ best scientifically validated - most time-consuming

Compromise programming refers to an approach that allows to rank alternatives according to their „distance to an imaginary ideal point" that in reality is neither present nor achievable. The „distance" (L) of any alternative is calculated according to the next formula. In this formula, w represents the weight of an indicator, z^* the best attribute value („ideal") z_* the worst attribute value („anti-ideal"). The number of indicators is marked with n.

$$L_p = \left[\sum_{j=1}^{n} w_j^p \left| \frac{z_j^* - z_j}{z_j^* - z_{*j}} \right|^p \right]^{1/p} \rightarrow \min! \qquad \left(w_j > 0; \sum w_j = 1; p \geq 1; p \in \mathrm{N} \right)$$

An important element is the exponent p. With increasing p, the ranking result is more and more dominated by anti-ideal attribute values. With other words, this parameter determines the degree to which compensation between attribute values with other attributes values are possible. The selection of an adequate parameter is not trivial and requires expert knowledge. Usually, the calculation is done for three different values: p=1 (City block norm), p=2 (euclidic norm), p=10 (maximum norm).

The concept of compromise programming can also be adopted for aggregation of indicator values. However, the concept of normalisation of attribute values requires input values on sufficient high scale level, which is not always the case. For instance, if the input values are ranking orders, these ranking values must be transferred to a higher scale level [e.g. to interval [0..10]).

Since end-users will most often have no experience in applying decision-making methods, index aggregation in resilience indicators should be conducted using a simple and easy-to-understand method that does not require additional end-user training (Table 11).

Table 11: Resilience indicators aggregation methods

Aggregation level		Aggregation method	Elicitation of weights
IV	From i to I *Calculating Category index I*	Average value or Sum of all simple weighted sum	Without weights (for average) or alternatively Predefined weigt and priority (without end user input)
III	From I to R *Calculating Resilience index R*	Sum of all simple weighted sum	End user prioritisation input based on own expirience or simple pair comparision (see RAT). Weight based on rank order – rank sum $w_j = \frac{n - r_j + 1}{\sum_{k=1}^{n} (n - r_k + 1)}$
II	From R to C *Calculating Capacity index C*	Sum of all simple weighted sum	
I	From C to ORI *Calculating Overall resilience index ORI*	Sum of all simple weighted sum	

Weight coefficients are shown in Table 12.

Table 12. Weight table of Sum of all simple weighted sum aggregation method

Rank	Number of Items									
	1	2	3	4	5	6	7	8	9	10
1	1,00	0,67	0,50	0,40	0,33	0,29	0,25	0,22	0,20	0,18
2		0,33	0,33	0,30	0,27	0,24	0,21	0,19	0,18	0,16
3			0,17	0,20	0,20	0,19	0,18	0,17	0,16	0,15
4				0,10	0,13	0,14	0,14	0,14	0,13	0,13
5					0,07	0,10	0,11	0,11	0,11	0,11
6						0,05	0,07	0,08	0,09	0,09
7							0,04	0,06	0,07	0,07
8								0,03	0,04	0,05
9									0,02	0,04
10										0,02
SUM	1	1	1	1	1	1	1	1	1	1

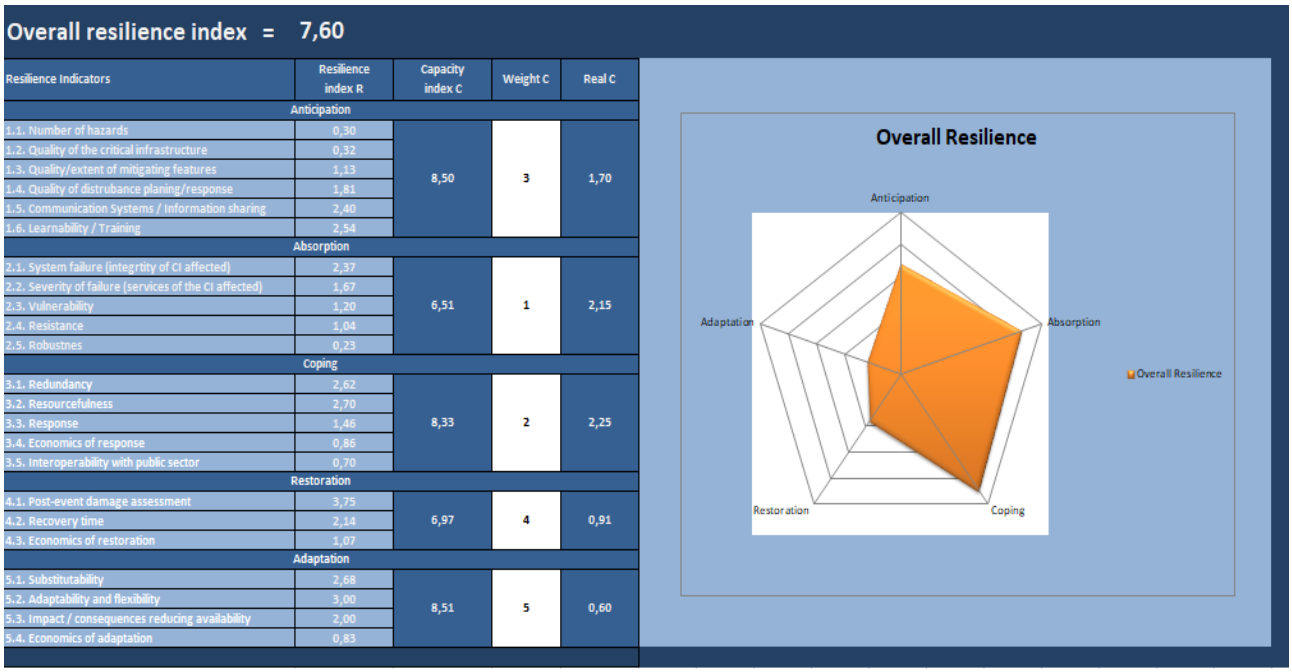
8 CIRP Implementation

Through the work on D4.5, the Resilience assessment tool (RAT) in Excel was developed (Figure 2). It is a functional prototype of the CIRP module, which will be implemented in the CIRP system.

For the resilience assessment, a large number of data should be provided - one part of this data (larger) will be given by end-users with the fill of end-user questionnaire (Table 13) and the other part of the data (smaller) will be draw down directly from CIRP (Table 14).

For the time being, 16 inputs are documented in D3.4 and 1 inputs is documented in D2.3. Two variables will read from operational damage functions and 1 variables from structural damage functions. All of these inputs are implemented in RAT in *Input from CIRP* worksheet (not repeated in *End-user questionnaire*).

For the moment there are a total of 139 questions for asset analysis, and 156 questions for network or network of network analysis. However, it is a kind of data that is not difficult to gather to end-users. 70-80% of the requested data are easily understood by operators / owners of critical infrastructures, so additional efforts should be made to collect those remaining 20-30%. The total number of end-user inputs will eventually be even lower because users will include some of this data in CIRP as part of the data set needed for risk analysis (such as number of hazards, number of assets, infrastructure aging, CI lifetime, etc.).



Overall resilience index = 7,60

Resilience Indicators	Resilience index R	Capacity index C	Weight C	Real C
Anticipation				
1.1. Number of hazards	0,30	8,50	3	1,70
1.2. Quality of the critical infrastructure	0,32			
1.3. Quality/extent of mitigating features	1,13			
1.4. Quality of distrubance planing/response	1,81			
1.5. Communication Systems / Information sharing	2,40			
1.6. Learnability / Training	2,54			
Absorption				
2.1. System failure (integrtity of CI affected)	2,37	6,51	1	2,15
2.2. Severity of failure (services of the CI affected)	1,67			
2.3. Vulnerability	1,20			
2.4. Resistance	1,04			
2.5. Robustnes	0,23			
Coping				
3.1. Redundancy	2,62	8,33	2	2,25
3.2. Resourcefulness	2,70			
3.3. Response	1,46			
3.4. Economics of response	0,86			
3.5. Interoperability with public sector	0,70			
Restoration				
4.1. Post-event damage assessment	3,75	6,97	4	0,91
4.2. Recovery time	2,14			
4.3. Economics of restoration	1,07			
Adaptation				
5.1. Substitutability	2,68	8,51	5	0,60
5.2. Adaptability and flexibility	3,00			
5.3. Impact / consequences reducing availability	2,00			
5.4. Economics of adaptation	0,83			

Figure 2: Resilience assessment tool

Table 13: End-user questionnaire

ITEM	RESILIENCE CATEGORIES / SUBCATEGORIES		VALUE	UNIT	NOTE
	GENERAL				
1.	Assesment is related to Asset - Network - Network of network		Asset		
2.	Select the hazards related to Critical infrastructure				
	Heat waves		yes		
	Cold snaps		no		
	Floods		no		
	Coastal floods		yes		
	Forest Fires		no		
	Droughts		no		
	Earth movement		no		
3.	Select the hazards related to area of Critical infratructure				
	Heat waves		yes		
	Cold snaps		yes		
	Floods		yes		
	Coastal floods		yes		
	Forest Fires		yes		
	Droughts		no		
	Earth movement		no		
4.	Construction year of Critical infrastructure		2010		
	Current year		2017		
5.	Lifetime of Critical infrastructure		100	Year	
6.	Number of Assets in Network		7		
	ANTICIPATION				

7.	Safety design standards (related to climate changes) is applied			yes		
	If yes:					
	How many relevant standards exist		4			
	How many relevant standards is applied		3			
	How many hazards applied standards covered		4			
	How many assets applied standards covered		4			n/a
	Network is cover by applied standards		yes			n/a
8.	Maintenance is regular			yes		
	If yes:					
	Maintenance plan exist		yes			
	Maintenance plan is in line with the Construction project		yes			
	Maintenance is performed according to the plan		yes			
	Maintenance is documented		yes			
	Critical infrastructure is fully operational according to specification		yes			
9.	Equipment and procedures for hazard mitigation exist			yes		
	If yes:					
	Procedures are documented		yes			
	Procedures are regulary revised		yes			
	How many hazards this procedures covered		4			
	How many assets this procedures covered		4			n/a
	Network is cover by procedures		yes			n/a
10.	How many hazards can be mitigated only by CI (level of self healing)			4		
11.	Early warning system exist			yes		
	If yes:					
	Early warning system is tested		yes			
	Early warning system is up to date		yes			
	How many hazards early warning system covered		4			
	How many assets early warning system covered		4			n/a

	Network is cover by early warning system	yes			n/a
12.	How many time installed capacity exceedes demand		1	Month per Year	
13.	Operational response plans exist		yes		
	If yes:				
	Operational response plans are tested	yes			
	Operational response plans are trainied	yes			
	Operational response plans are up to date	yes			
	How many hazards operational response plans covered	4			
	How many assets operational response plans covered	5			n/a
	Network is cover by operational response plans	yes			n/a
14.	Plans of communication and information sharing exist		yes		
15.	Communication system for communication and information sharing exist		yes		
16.	Backup of communication system exist		yes		
17.	Training system exist		yes		
	If yes:				
	How many hazards is covered by training system	4			
	Performed hours of training	80		Hour	
	Necessary (planned) hours of training	100		Hour	
	Training programm is tested	yes			
	Training programm is up to date	yes			
	Last training was within a year	yes			
18.	Number of trained people		30		
	Number of related people		40		
19.	Trainig with other CI exist		yes		
	ABSORPTION				
20.	Acceptable time that CI is not able to serve its intended function		24	Hour	
21.	Acceptable costs of damaged assets		1000000	EUR / National	

				valute	
22.	Number of assets fail		3		n/a
23.	Total loss of income as a result of not servicing demand		50000	EUR / National valute	
	Acceptable loss of income as a result of not servicing demand		1000000	EUR / National valute	
24.	Acceptable time that person is left without any CI services		6	Hour	
25.	Acceptable time that person is left without two or more CI services		12	Hour	
26.	Acceptable number of CI thresholds per year in the future climate		2	Event per Year	
27.	Vulnerability assessment exist		yes		
	If yes:				
	How many hazards it covers	3			
	How many assets it covers	3			n/a
	Network is cover	yes			n/a
28.	Protection measures & operational procedures exist		yes		
	If yes:				
	How many hazards it covers	4			
29.	Asset backup exist		yes		
30.	Service replacement exist		no		
	COPING				
31.	How many assets have backup		1		
32.	After how much time backup is available		2	Hour	
	Acceptable time for backup availability		4	Hour	
33.	How long backup is available		36	Hour	
	Acceptable time for backup availability		48	Hour	
34.	Special response plan exist		yes		
	If yes:				

		Plans are tested	yes			
		Plans are trainied	yes			
		Plans are up to date	yes			
		How many hazard it covers	3			
		How many assets it covers	5			n/a
		Network is cover	yes			n/a
35.	Acceptable time for response			6	Hour	
36.	Emergency plans under Climate Hazards (in the context of climate change) exist			yes		
		If yes:				
		Plans are tested	yes			
		Plans are trainied	yes			
		Plans are up to date	yes			
		How many hazards are covered by plans	3			
		How many assets are covered by plans	5			n/a
		Network is covered by plans	yes			n/a
37.	Business continuity plans under Climate Hazards (in the context of climate change) exist			yes		
		If yes:				
		Plans are tested	yes			
		Plans are trainied	yes			
		Plans are up to date	yes			
		How many hazards are covered by plans	3			
		How many assets are covered by plans	4			n/a
		Network is covered by plans	no			n/a
38.	Cost of response (for CI only)			100000	EUR / National valute	
		Acceptable cost of response		800000	EUR / National valute	
39.	Costs for replacements of services			2000000	EUR / National	

				valute	
	Acceptable cost of replacement		4000000	EUR / National valute	
40.	Backup cost		200000	EUR / National valute	
	Acceptable cost of backup		300000	EUR / National valute	
41.	Procedures for interoperability with public sector exist		yes		
42.	Communication system for interoperability with public sector exist		yes		
43.	Joint action plans with public sector exist		yes		
	If yes:				
	Plans are tested	yes			
	Plans are trainied	yes			
	Plans are up to date	yes			
	RESTORATION				
44.	Special recovery plan exist		yes		
	If yes:				
	How many hazard it covers	3			
	How many assets it covers	5			n/a
	Network is cover	yes			n/a
45.	Time needed to recovery		12	Month / Hour / Day	
	Acceptable time of recovery		48	Month / Hour / Day	
46.	Cost of restoration		200000	EUR / National valute	
	Acceptable cost of restoration		500000	EUR / National valute	
47.	Loss of income during restoration		50000	EUR / National valute	

	Acceptable loss of income		100000	EUR / National valute	
48.	Loss due to possible penalties from violating service level agreements with buyers		2000	EUR / National valute	
	Acceptable loss		50000	EUR / National valute	
49.	Costs for replacements of services		500000	EUR / National valute	
	Acceptable cost of replacement		2000000	EUR / National valute	
50.	Maintenance costs after hazard		25000	EUR / National valute	
	Acceptable cost of maintenance		40000	EUR / National valute	
51.	Indirect costs - socieconomic		15000	EUR / National valute	
	Acceptable indirect costs		25000	EUR / National valute	
52.	Cost of reputation		2000	EUR / National valute	
	Acceptable cost of reputation		10000	EUR / National valute	
53.	Insurance costs		25000	EUR / National valute	
	Acceptable insurance costs		50000	EUR / National valute	
ADAPTATION					
54.	Replacement of asset is technical possible		yes		
55.	Replacement of asset is financial possible		yes		
56.	Replacement of service is technical possible		yes		

57.	Replacement of service is financial possible		no		
58.	CI have ability to change while maintaining or improving functionality		yes		
59.	Quick adoption of alternative strategies is possible		yes		
60.	Responding to changing conditions in time is possible		yes		
61.	Re-locate of facilities is possible		yes		
62.	Building new facilities according to climate-ready standards		yes		
63.	Protection of existing critical infrastructure		yes		
64.	Development of flexibility of networks is possible		yes		n/a
65.	New investments take consider a climate change		yes		
66.	How many new clients can be reached by improving the service / climate adaptation polices		21	%	
67.	Reputation is increased by implementing climate change adaptation options		yes		
68.	Decisions on adaptation adopt due to market forces		yes		

Table 14: CIRP inputs

ITEM	RESILIENCE CATEGORIES / SUBCATEGORIES
1.	Probability of failure
2.	Failure for certain hazards level
	Certain hazards level (from 0 to 10):
	Heat waves
	Cold snaps
	Floods
	Coastal floods
	Forest Fires
	Droughts
	Earth movement
3.	Number of assets fully damaged (beyond reparability)
4.	Number of assets partially damaged
5.	Number of assets with a [over] certain percent (%) or range of damages
6.	Time that CI is not able to serve its intended function
7.	Costs of damaged assets
8.	Loss for certain hazards level
9.	Reduced network capacity
10.	Connectivity Loss (CL)
11.	Service Flow Reduction (SFR)
12.	Total time that person is left without any CI services
13.	Total time that person is left without two or more CI services
14.	How often in the future climate, CI thresholds will be exceeded
15.	Availability of interconnected assets (provide reserve services, could be different CI)
16.	Time to start response
17.	Percentage change from base state after event

9 Conclusion

The main purposes of D4.5 is to define Resilience indicators, and the method of quantification of resilience capacities.

The indicators are based on the EU-CIRCLE methodology described in D1.5 and on the Resilience framework, initially described in D4.1 and more specifically described in D4.3. The calculation of the resilience index values is carried out using the methods described in D4.2.

Values of the resilience indexes of the 5 resilience capacities and value of the Overall resilience index will be used later in Cost-effectivenes analysis (D4.7), Business Continuity Model (D4.4) and Adapatation Model (D4.6).

Through the work on D4.5, the Resilience assessment tool (RAT) in Excel was developed. It is a functional prototype of the CIRP module, which will be implemented in the CIRP system.

10 References

Bahadur, A., Peters, K., Wilkinson,E., Pichon,F., Gray, K and Tanner, T (2015). The 3As: Tracking Resilience Across Braced, Working paper, BRACED Knowledge Manager [Online] Available from: http://www.braced.org/ [Accessed April 2015]

Barami, B. (2013). Infrastructure Resiliency: A Risk-Based Framework. John A. Volpe National Transportation Systems Center, Cambridge, MA

Béné, C., Godfrey Wood, R., Newsham, A., Davies, M. (2012). Resilience: new utopia or new tyranny? Re ection about the potentials and limits of the concept of resilience in relation to vulnerability reduction programmes. Brighton: Institute of Development Studies.

Biringer, B., Vugrin, E. and Warren, D., (2013). Critical infrastructure system security and resiliency. CRC press.

Blaikie, P., Cannon, T., Davis, I., Wisner, B. (2003). At Risk: Natural Hazards, People's Vulnerability and Disasters. Abingdon: Routledge.

Bush, W., Grayson, M., Berkeley, A.R., Thompson, J. (ed.)(2009). Critical infrastructure resilience, Final report and recommendations. National infrastructure advisory council, USA

Cabinet Office (2011). Keeping the Country Running: Natural Hazards and Infrastructure. A Guide to improving the resilience of critical infrastructure and essential services. Whitehall, London

Dickson E., Baker J.L., Hoornweg D., Tiwari A. (2012).Urban Risk Assessments, Understanding Disaster and Climate Risk in Cities. International Bank for Reconstruction and Development/World Bank, Washington, DC

Fisher, R.E., Bassett, G.W., Buehring, W.A., Collins, M.J., Dickinson, D.C., Eaton, L.K., Haffenden, R.A., Hussar, N.E., Klett, M.S., Lawlor, M.A., Miller, D.J., Petit, F.D., Peyton, S.M., Wallace, K.E., Whitfield, R.G., Peerenboom, J.P. (2010). Constructing a resilience index for the enhanced critical infrastructure protection program

Folke, C., Carpenter, S.R., Walker, B., Scheffer, M., Chapin, T., Rockström, J. (2010). 'Resilience thinking: integrating resilience, adaptability and transformability'. Ecology and Society. 15(4). www.ecologyandsociety.org/vol15/iss4/art20/.

Gibson, C.A. & Tarrant, M. (2010). "A'conceptual models' approach to organisational resilience", Australian Journal of Emergency Management, The, vol. 25, no. 2, pp. 6.

IEA (2015). Making the energy sector more resilient to climate change. International Energy Agency, Paris

Kellett, & Peters. (2014). Dare to Prepare: Taking Risk Seriously. London: ODI

Klaver M.H.A., Luiijf H.A.M., Nieuwenhuijsen A.H. (2011). RECIPE project. Good practices manual for CIP policies. For policy makers in Europe

National Institute of Standards and Technology (2015). NIST Special Publication 1190: Community Resilience Planning Guide for Buildings and Infrastructure Systems Volume 2.

Prior, T. (2014). Measuring Critical Infrastructure Resilience: Possible Indicators, Risk and Resilience, Report 9. Center for Security Studies, ETH Zürich

RAMSES (2016). D2.1: Synthesis review on resilient architecture and infrastructure indicators. RAMSES Project (Grant Agreement n° 308497)

UN Office for Disaster Risk Reduction (2014). Disaster Resilience Scorecard for Cities Working Document Version 1.5, dated March 10th, 2014.

UNISDR (2009). Terminology [Online], http://www.unisdr.org/we/inform/terminology [accessed 8 November 2015]

Watson, J.P., Guttromson, R., Silva-Monroy, C., Jeffers, R., Jones, K., Ellison, J., Rath, C., Gearhart, J., Jones, D., Corbet, T. (2014). Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States. SAND2014-18019 Albuq. NM Sandia Natl. Lab.

Karni, E.; Werczberger (1995): The compromise criterion in MCDM: interpretationand sensitivity to the p parameter. Environment and planning B 22 (4), 407 – 418.

Tkach, J.-R.; Simonovic, S.-P. (1997): A New Approach to Multi-criteria Decision Makin in Water Resources. Journal of Geographic Information and Decision Analysis, vol. 1, no.1, S. 25 – 44

Zeleny, M. (1982): Multiple Criteria Decision Making. McGraw-Hill, New York.