



# **Resilience Capacities Assessment for Critical Infrastructures Disruption**

## **D 2.1 READ Preparedness Tool Material and User Guide**



The READ Project (GA- HOME/2013 CIPS/AG/4000005064) is co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union.



Programme	CIPS – Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks
Type of Action	CIPS Action Grant 2013
Project Title	Resilience Capacities Assessment for Critical Infrastructures Disruption
Acronym	READ
Project n.	GA -HOME/2013/CIPS/AG/4000005064

Work Package	WP2
Lead Partner	Fondazione Politecnico di Milano
Contributing Partner(s)	All
Security Classification	CO (Confidential)
Date	07/03/2017
Version	3.0



## Document history

Version	Date	Comments	Authors
1.0	2017/02/10	Initial draft to partners	Boris Petrenj, Paolo Trucco
2.0	2017/02/22	Partner comments integrated	All
3.0	2017/03/07	Final version	Boris Petrenj, Paolo Trucco

## Statements of originality and responsibility :

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

**The project leading to these has been funded with support from the European Commission. This document reflects the views of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.**





## Table of Contents

<b>1.</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>4</b>
<b>2.</b>	<b>INTRODUCTION .....</b>	<b>5</b>
<b>3.</b>	<b>READ TOOL LOGIC .....</b>	<b>6</b>
<b>4.</b>	<b>READ TOOL IMPLEMENTATION .....</b>	<b>8</b>
<b>5.</b>	<b>TOOL DESCRIPTION AND USER GUIDELINES .....</b>	<b>9</b>
5.1.	System description (Edit the System) .....	9
5.2.	Characterisation: .....	15
5.3.	Resilience assessment and analysis .....	17
<b>6.</b>	<b>OUTPUTS .....</b>	<b>20</b>
	<b>ANNEX: LIST OF PREDEFINED CAPABILITIES AVAILABLE INSIDE THE TOOL .....</b>	<b>25</b>



## Table of Figures

Figure 1: Overall logic and procedure .....	7
Figure 2: Capability improvement cycle.....	7
Figure 3: READ tool relationship diagram .....	8
Figure 4: The Dashboard (main menu) .....	9
Figure 5: Specification of system elements - menu.....	10
Figure 6: Editing organisations .....	10
Figure 7: Resilience capabilities specification and classification.....	11
Figure 8: Editable three-level taxonomy of Hazards & Threats.....	12
Figure 9: Infrastructure system definition (three-level) .....	15
Figure 10: Accident specification .....	16
Figure 11: Vulnerability assessment (asset vs. accident) .....	17
Figure 12: Resilience Assessment menu .....	18
Figure 13: Description and Assessment of individual resilience capabilities .....	19
Figure 14: Proposed assessment scale .....	19
Figure 15: Gap Analysis .....	20
Figure 16: Detailed overview .....	21
Figure 17: Colour coded Gap Analysis (example).....	21
Figure 18: Gap share by EM Cycle (left) and Resilience Capacities (right) .....	22
Figure 19: Colour coded Gap Analysis (example).....	23
Figure 20: An example of a more detailed gap analysis (Absorptive-Recovery) .....	23
Figure 21: Capability improvement cycle, READ tool coverage.....	24

## Table of Tables

Table 1: Hazard & Threat taxonomy.....	13
--	----



## 1. Executive Summary

---

READ is a research project, funded under the Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks Programme (CIPS) Action Programme (European Commission – Directorate-General Home Affairs). The project aims at improving resilience capacities required to manage Critical Infrastructure (CI) disruptions and enhancing current emergency management practices to better address the challenges raised by cross border CI disruptions.

Project partners are:

- Fondazione Politecnico di Milano (Coordinator, IT)
- Risk Governance Solutions S.r.l. (IT)
- Technical University of Denmark (DK)
- Tecnalìa (SP)
- Regione Lombardia (IT)

We would also like to acknowledge the contribution to the project by:

- Danish Emergency Management Agency (DEMA)
- Capital Region Pre-Hospital Services (Pre-Hosp)
- Oresundsbron (Oresund)

The overall objective of READ is to support the improvement of European emergency management practices by integrating issues related to trans-boundary critical infrastructures disruptions and related cascading effects into the current emergency management set-up. This objective will be achieved by providing adequate knowledge, tools and related strategies to prepare for, cope with and recover from cross-border crisis situations resulting from the interruption of essential services supply.

A key part of the READ project is development of a conceptual and methodological framework to maintain resilience capabilities for coping with trans-boundary CI disruptions. The approach to be developed should integrate the resilience capabilities of CIs into the Emergency Management (EM) cycle, which would allow emergency services to explicitly address resilience improvement measures while planning to cope with CI disruptions. The framework shall have a sound theoretical foundation as well as practical relevance for, in particular, developing assessment and training tools for CI stakeholders. Following this limited scope of the project, the framework is by choice focused primarily on the response and early recovery phases of CI interruptions and to a lesser extent on the wider tasks of preparation (including contingency plans) and long-term recovery and possible adaptation to novel and possibly very different circumstances of service.

In this deliverable, we present the key features and the functionalities of the READ tool that translates the READ framework (Deliverable 1.1) for the integration of CI resilience capabilities in the emergency management set-up.



## 2. Introduction

---

READ aims at increasing the resilience capacities required to manage CI disruptions and enhancing current emergency management practices to better address the challenges raised by cross border CI disruption.

The specific objectives of READ are:

- To develop a comprehensive framework to identify, build and assess specific resilience capacities required to prepare, cope and recover from cross-border CI disruptions;
- To develop a tool (the READ Tool) aiming at supporting the stakeholders involved in emergency management activities, including the CI operators, to assess their own resilience capacities with respect to cross border CI disruptions and thus identify the main areas where progress is needed;
- To test the READ Tool during the preparation activities in the context of public-private-partnerships for Critical Infrastructure protection and Resilience;
- To test the READ Tool during a table-top exercise involving selected stakeholders (emergency managers, civil protection authorities, first responders and CI operators);
- To build on the READ project activities to raise awareness of EU stakeholders involved in emergency management activities on the need to assess their resilience capacities to the view to integrate and improve their current emergency management practices to address cross-border CI disruptions.

The target groups and beneficiaries of READ activities and results are the emergency management & civil protection authorities, first responders, CI operators and the main public authorities in charge of critical infrastructure protection and/or resilience programmes.

Given the focus and objectives of READ project, the partnership building strategy focused on assuring both practical relevance, international and cross-border dimension of the issues addressed and the ability of developing innovative emergency management solutions. As for the first strategic priority, technical partners were selected according to their recognised excellence in the emergency management domain, with a strong research tradition on Safety and Risk Management, Emergency Management and Critical Infrastructure Protection related subjects, as well as a long record of joint research activities in the same subject areas.

Expected results of READ range from a better understanding and an increased knowledge of target groups on what are the resilience capacities related to the emergency management cycle to address cross-border CI disruptions, up to a specific toolkit to support stakeholders involved in emergency management activities to assess their current practices against resilient capacities.



### 3. READ Tool Logic

---

There are three main phases in the use of the tool (Figure 1):

- system description (set-up);
- characterization;
- resilience assessment.

1) **System and environment specification** is the initial phase, where the characteristics of the system under analysis, the organisational and environmental contexts must be specified, independently from each other. In this part, the users should go through a few setup steps, namely: Those include:

- a. **Infrastructures** and their parts (i.e. assets)
- b. **Organisations** involved (both public and private)
- c. **Hazards and Threats (H&T)** – the tool contains a predefined taxonomy of Hazards & Threats
- d. **Resilience capabilities** – the tool contains a preliminary list of capabilities

2) **System characterization** involves three main steps:

- a. **Accident specification** – where different possible future events can be described and documented as the scenario of reference for the assessment and planning phases (e.g. electrical blackout event, heavy snowfall, flooding, etc.). User defines an accident by selecting a combination of (or at least one of) Hazards & Threats and their magnitude.
- b. **Asset vulnerability** – user defines vulnerability of each asset when facing accidents of interest (defined in the previous step)

3) **Resilience assessments** includes:

- a. **Capability assessment** – organisations describe their individual capabilities and perform a capability assessment (current and target level) considering each specific accident
- b. **Outputs** – includes various analyses, main being *Capability overview* and *Gap analysis* which can have more steps and provide deeper insights.

Each of the steps is described in more detail in the following sections.



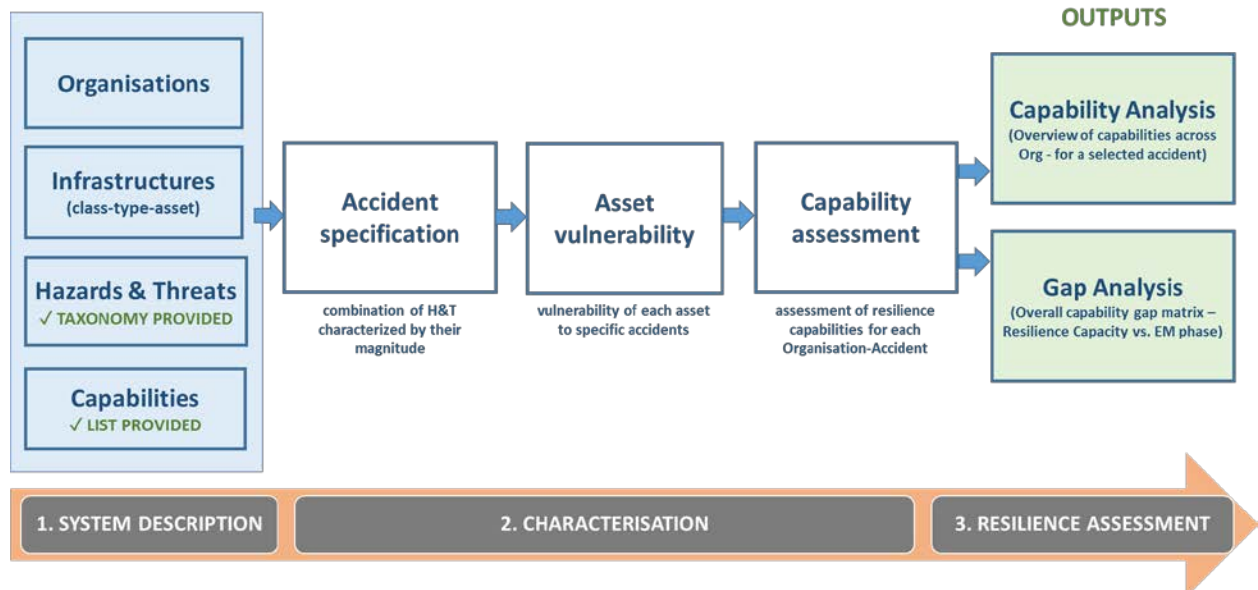


Figure 1: Overall logic and procedure

The **Capability Building Cycle** presents an operational approach for continuous process of programme design and implementation, through which the system resilience is enhanced. It consists of four steps (Figure 4):

- 1) In the first step the current state of the resilience capabilities is assessed;
- 2) In the second step a Gap Analysis is performed where the gaps in the capabilities are identified considering the accidents and related system vulnerabilities. Based on the analysis, a target value for each capability is deliberated. Target values aim to cover all the gaps and make the system completely fitting with its exposure to the context;
- 3) In the third step, the objectives are set, and the implementation plan is decided upon. Objective values identify the expected improvements to be achieved during the next planning cycle, hence they could be lower than the target values.
- 4) The fourth step (which is also the first step of the next planning cycle) is where the resilience capabilities are reassessed and reviewed after a single improvement cycle.

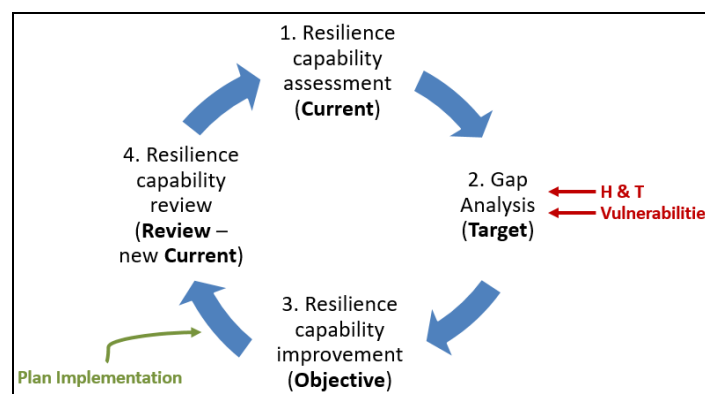


Figure 2: Capability improvement cycle

#### 4. READ Tool Implementation

The READ tool prototype was implemented in Microsoft Access™. MS Access is used by small businesses, within departments of large corporations, and hobby programmers to create ad hoc customized desktop systems for handling the creation and manipulation of data. Access can also be used as the database for basic web based applications hosted on Microsoft's Internet Information Services and utilizing Microsoft Active Server Pages ASP. One of the benefits of Access from a programmer's perspective is its compatibility with SQL—queries may be viewed and edited as SQL statements, and SQL statements can be used directly in Macros and VBA Modules to manipulate Access tables. Users may mix and use both VBA and Macros for programming forms and logic and offers object-oriented possibilities.

For query development, Access utilizes the Query Design Grid, a graphical user interface that allows users to create queries without knowledge of the SQL programming language. Microsoft Access can be applied to small projects but it doesn't scale up well to larger projects involving multiple concurrent users. That's because it is a desktop application, not a true client-server database. MS Access is chosen for development environment mainly because of availability and user-friendly issues of the program. The aim of developing this program had not been delivering a fully functioning system but to illustrate a real-life example on a relatively small scale of information.

The relationship graph between the tool tables is given in Figure 3.

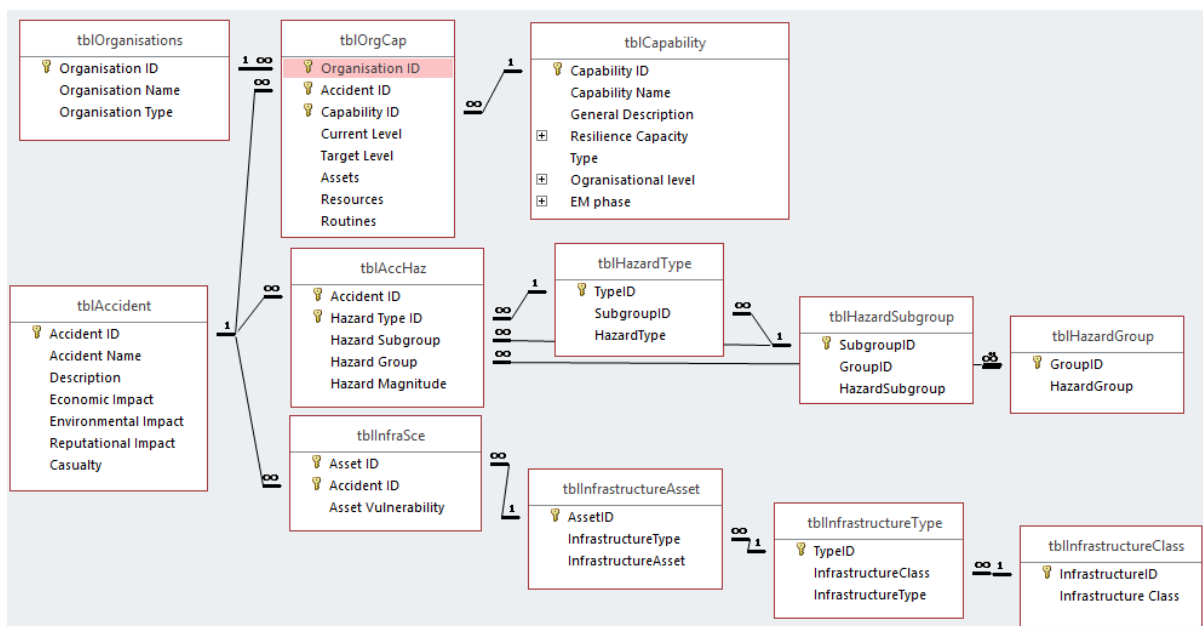


Figure 3: READ tool relationship diagram



## 5. Tool description and User guidelines

This section aims to guide the proposed end-users () on how to use, understand and benefit from the tool. As common in software applications, the end-user interaction with the program is limited with the user interface.

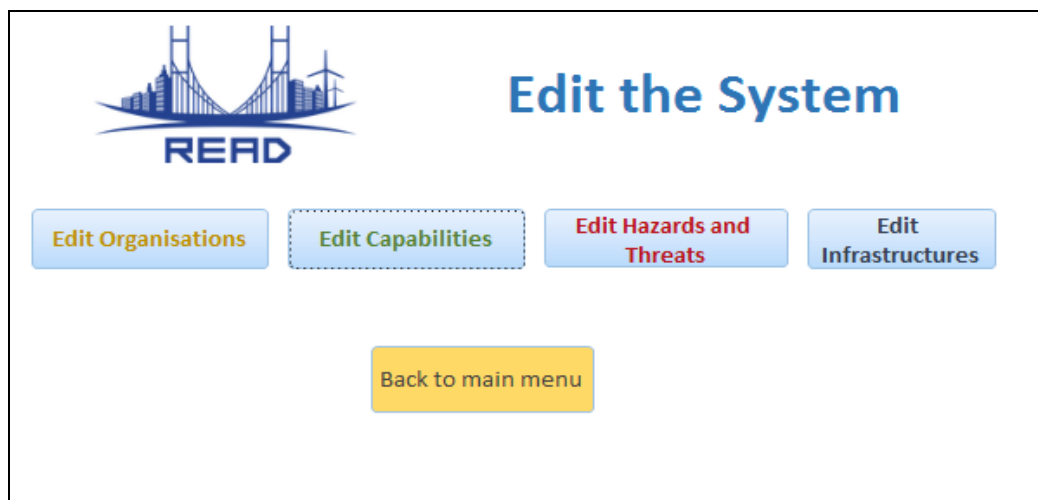
Upon running the tool, READ Dashboard shows up as the main screen (Figure 4). It consists of four click bars: **Edit the System** (belonging to the *System description* part), **Edit Accidents** & **Edit Asset Vulnerability** (belonging to the *System Characterization*) and finally **Resilience Assessment** in which user can carry out Resilience analysis and Gap analysis.



Figure 4: The Dashboard (main menu)

### 5.1. System description (Edit the System)

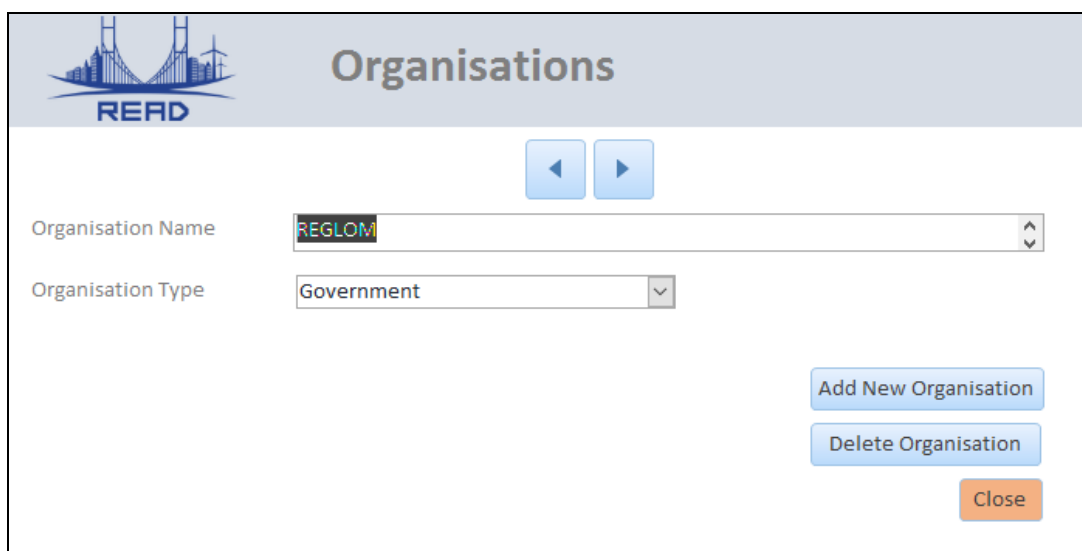
Inside this section of the tool we describe infrastructure system and its environment. There are four aspects, namely: Organizations, Capabilities, Hazards & Threats, and Infrastructures (Figure 5).



**Figure 5: Specification of system elements - menu**

“Back to main menu” button takes user back to the READ tool Dashboard. Other options are explained below.

- a) “**Edit organizations**” option is used to create a list of organizations involved in the study (Figure 6). Each organization is described by its name and type (Operator, Government, Responder...). Buttons to add and delete organizations are available. ‘Close’ option takes user to the previous menu - “Edit the system”.



**Figure 6: Editing organisations**

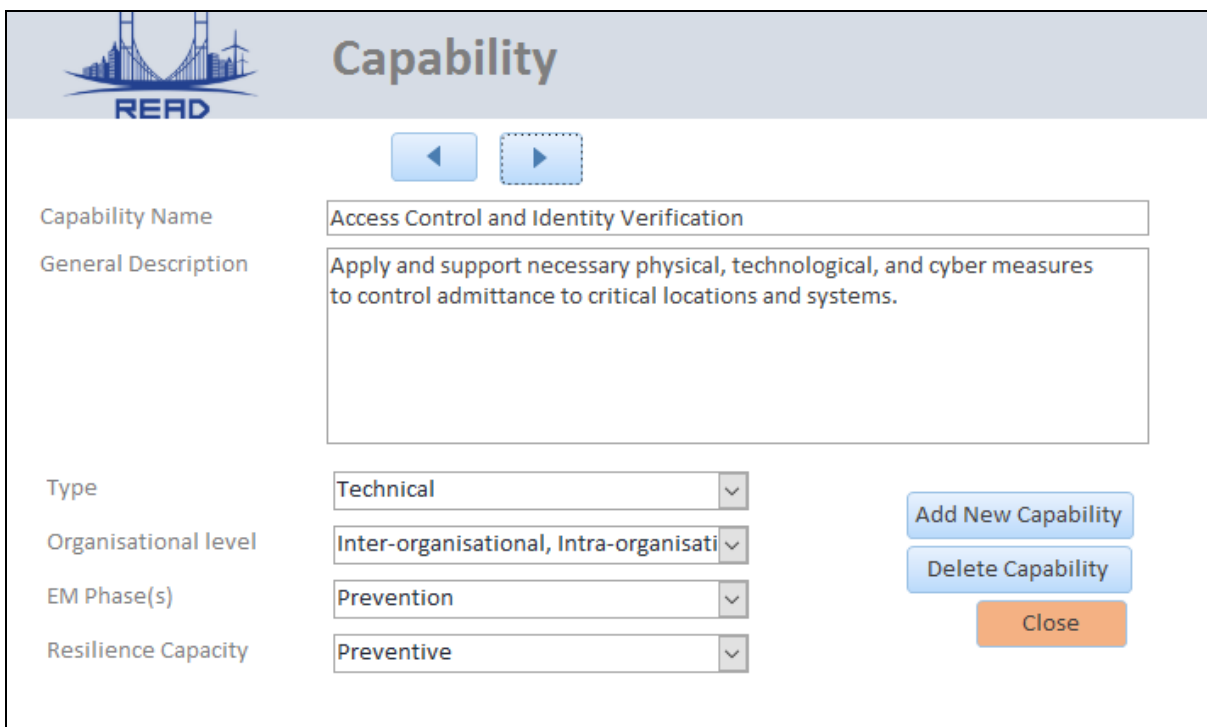
- b) “**Edit Capabilities**” option enables user to manage the list of capabilities. The tool offers a predefined list of 24 resilience capabilities (including their general description), which is of course editable. As a starting point for the definition of the complete list of READ resilience capabilities, reference was made to the 32 core

capabilities identified by FEMA in the National Preparedness Goal (NPG; <https://www.fema.gov/core-capabilities>). The final list of the READ capabilities is reported in the Annex. Each capability is classified according to (Figure 7):

- **Type** (Technical, Organisational);
- **Organisational level** (Intra-Organisational and/or Inter-Organisational);
- **Emergency Management** phases in which is used (Preparedness, Protection, Prevention, Response, Recovery);
- **Resilience goals/capacities** to which it contributes (Prevent, Absorb, Adapt, Restore).

The capability classification helps the analysis (after the capability assessment is performed) of the gap from different perspectives.

‘Delete Capability’ and ‘Add Capability’ options are available. ‘Close’ button takes user back to previous menu - “Edit the system”.



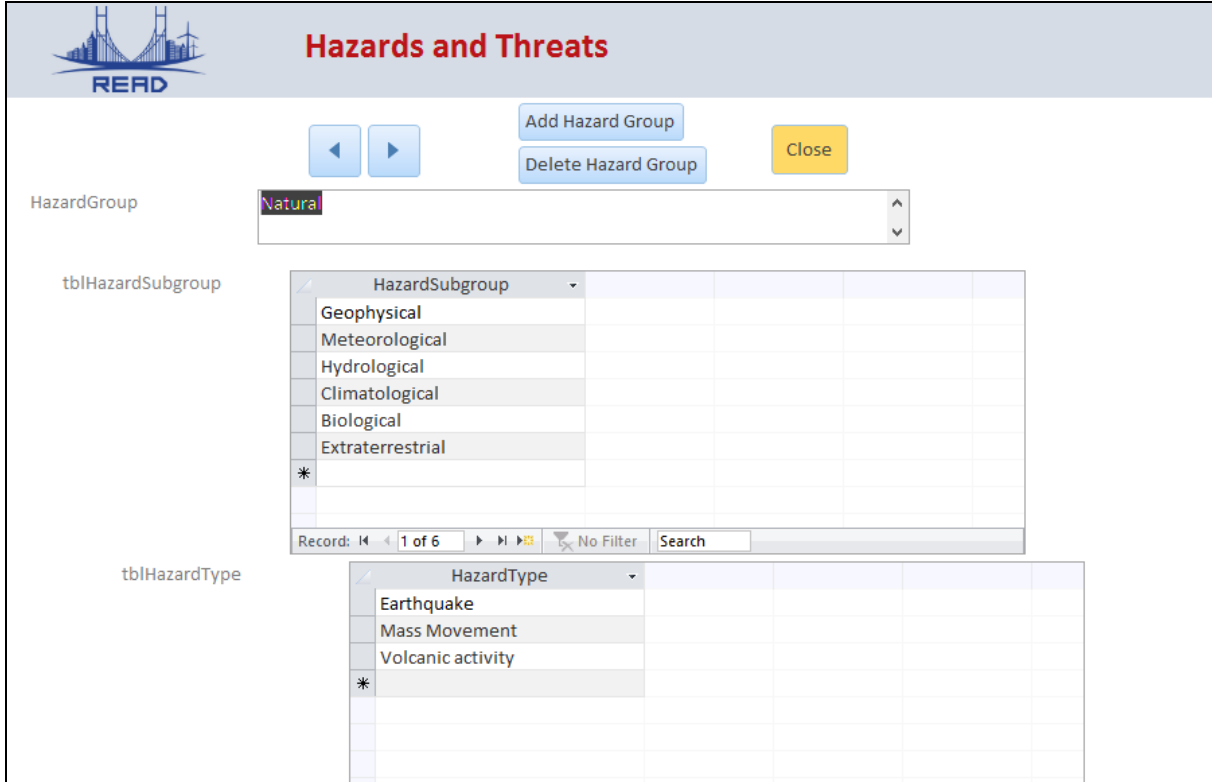
The screenshot shows the 'Capability' configuration screen in the READ tool. At the top left is the READ logo. The title 'Capability' is centered at the top. Below the title are two navigation arrows: a solid blue left arrow and a dashed blue right arrow. The main form contains the following fields:

- Capability Name:** Access Control and Identity Verification
- General Description:** Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.
- Type:** Technical (dropdown menu)
- Organisational level:** Inter-organisational, Intra-organisati (dropdown menu)
- EM Phase(s):** Prevention (dropdown menu)
- Resilience Capacity:** Preventive (dropdown menu)

On the right side of the form, there are three buttons: 'Add New Capability' (blue), 'Delete Capability' (blue), and 'Close' (orange).

**Figure 7: Resilience capabilities specification and classification**

- c) “**Edit hazards and threats**” section shows the predefined Hazard & Threat taxonomy (Figure 8). It is organized in three levels: Group – Subgroup – Type. The taxonomy is comprehensive but fully editable. ‘Close’ button takes user back to previous menu - “Edit the system”.



**Hazards and Threats**

HazardGroup:

tblHazardSubgroup:

HazardSubgroup	
Geophysical	
Meteorological	
Hydrological	
Climatological	
Biological	
Extraterrestrial	
*	

Record: 1 of 6 | No Filter | Search

tblHazardType:

HazardType	
Earthquake	
Mass Movement	
Volcanic activity	
*	

**Figure 8: Editable three-level taxonomy of Hazards & Threats**

The available classification of Hazards & Threats is shown in Table 1.

**Table 1: Hazard & Threat taxonomy**

Group	Subgroup	Main Type
Natural	Geophysical	Earthquake
		Mass Movement
		Volcanic activity
	Meteorological	Extreme Temperature
		Fog
		Storm
	Hydrological	Flood
		Landslide
		Wave action
	Climatological	Drought
		Glacial Lake Outburst
		Wildfire
	Biological	Epidemic
		Insect infestation
		Animal Accident
	Extraterrestrial	Impact
		Space weather
Technological	Industrial accident	Chemical spill
		Collapse
		Explosion
		Fire
		Gas leak
		Poisoning
		Radiation
		Other
	Transport accident	Air
		Road
		Rail
		Water
	Miscellaneous accident	Collapse
		Explosion
		Fire
		Human/Organisational error
		Other

Intentional Threats	Terrorism	Cyberterrorism
		Narcoterrorism
		Stampedes
		Crime
		Chemical Agents
		Biological agents
		Nuclear and radiological weapons
		Conventional explosives
	Mass Shootings	School shootings
		Workplace violence
		Hate crimes
	Civil Disobedience	Labour riots
		Race riots
		Political riots

d) “**Edit Infrastructures**” allows description of the considered infrastructure system (Figure 9). It is described in three levels:

- Infrastructure class (e.g. Transportation, Energy)
- Infrastructure type (e.g. Road, Rail, Water in *Transportation*; Electricity, Gas in *Energy*, etc.)
- Infrastructure asset include concrete assets used for the vulnerability assessment. For example, we can have infrastructure class “transportation” in which we have types of transport infrastructure i.e. rail, road and airports. Inside infrastructure assets we can have names of the train stations, if we choose type of infrastructure “rail”.

‘Close’ button takes user back to previous menu - “Edit the system”.



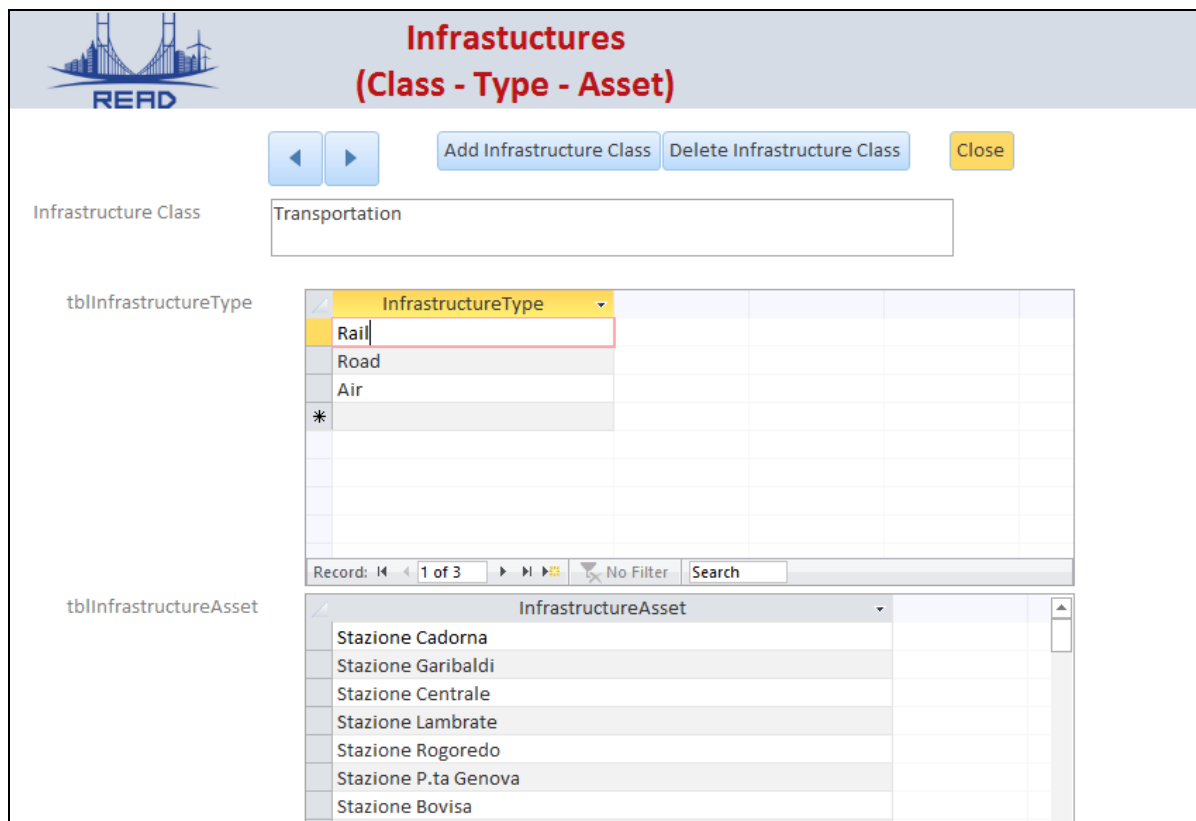



Figure 9: Infrastructure system definition (three-level)

## 5.2. Characterisation:

System Characterisation includes accident and assets' vulnerability (to those accidents) specification - '*Edit Accidents*' and '*Edit Asset Vulnerability*' buttons in the main menu, respectively (Figure 4)

a) "***Edit accident***" button opens the Accident Specification window (Figure 10). An Accident is described as a combination of active Hazards & Threats, each characterized with its magnitude (five level scale). User can add/remove accidents as well Hazards and Threats inside each of the accidents. Accident description box allows a free description of the accident, to avoid a misunderstanding between the organisations.

In this section, user can also define different potential impacts of the scenario (economic, environmental, reputational and causality), if relevant for the analysis. "Done" button will take user to the main menu, where he can make the next step.



## Accident Specification

◀ ▶

Add New Accident  
Delete Current Accident  
Edit Capabilities

Accident Name

Description 

The simulated blackout scenario involves the failure of the HHT/HT transformation station on the northern part of Milan. The event took place at 7:00 A.M and lasted until 11:00 A.M approximately.

frmAccHaz

	Hazard Group	Hazard Subgroup	Hazard Type	Hazard Magnitude
	Natural	Meteorological	Storm	Medium
	Technological	Miscellaneous accide	Collapse	Very High
	Technological	Miscellaneous accide	Explosion	High
	Technological	Miscellaneous accide	Fire	Medium
*				

Record: 1 of 4 No Filter Search

Economic Impact

Environmental Impact

Reputational Impact

Casualty

Done

**Figure 10: Accident specification**

b) **“Edit Asset Vulnerability”** (Figure 11) invites user to assess the vulnerability of the assets in respect to defined accidents (five level scale). User should move asset by asset (record by record) and set its vulnerability for previously defined scenarios.

Asset vulnerability is considered in the next step, while assessing resilience capabilities. “Done” button will take user to the main menu. After this point user is ready to move to Resilience Assessment.

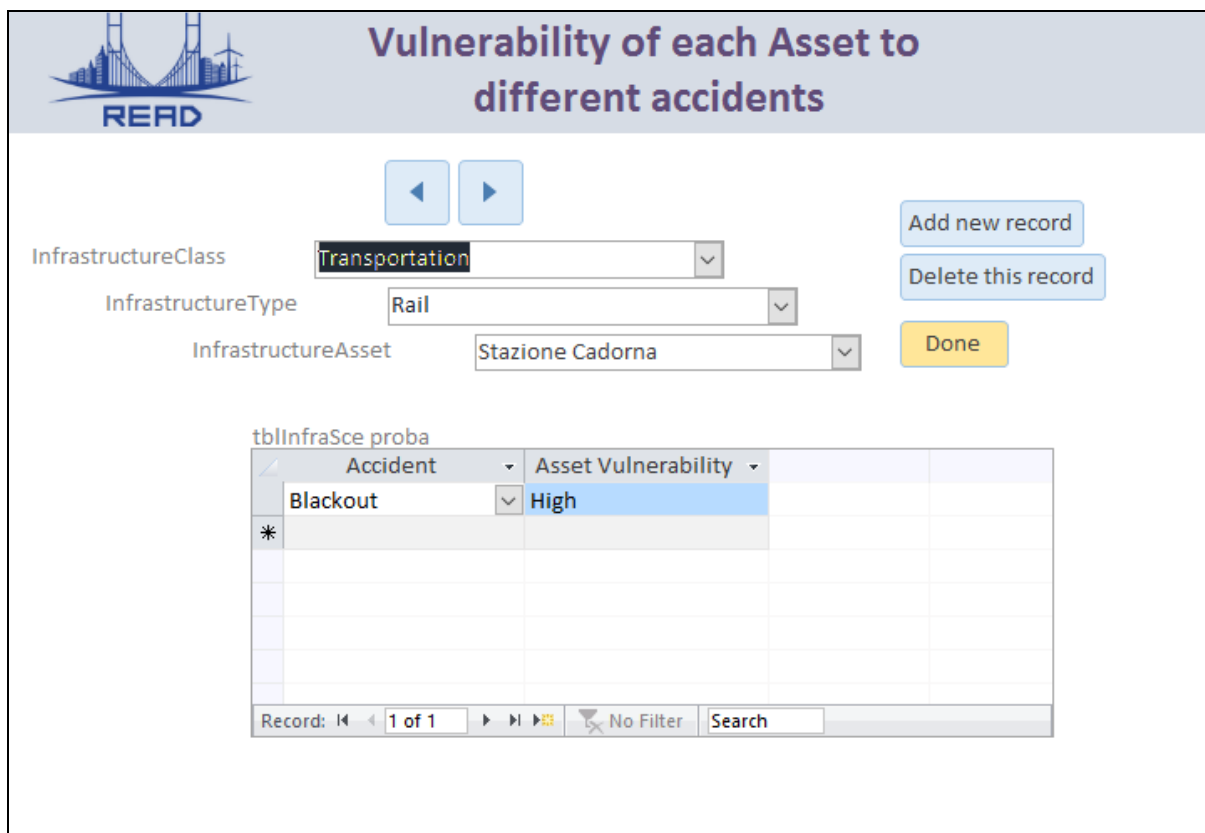


Figure 11: Vulnerability assessment (asset vs. accident)

### 5.3. Resilience assessment and analysis

After the system specification, the user moves into the 'Resilience Assessment' module of the tool. Resilience Assessment (Figure 12) is accessible through the Main Menu (Figure 4) It consists of Capability Assessment performed by user, which then enables generation of the output, with the Gap analysis as its main part.



**Resilience Assessment**

**Assessment of Capabilities**

Please choose Accident for which you want to run the capability analysis

Show Capability Analysis

Gap Analysis is not related to a specific accident but to the overall EM and Resilience state, based on available Capabilities. Includes all organisations

Show Gap Analysis

Back to main menu

**Figure 12: Resilience Assessment menu**

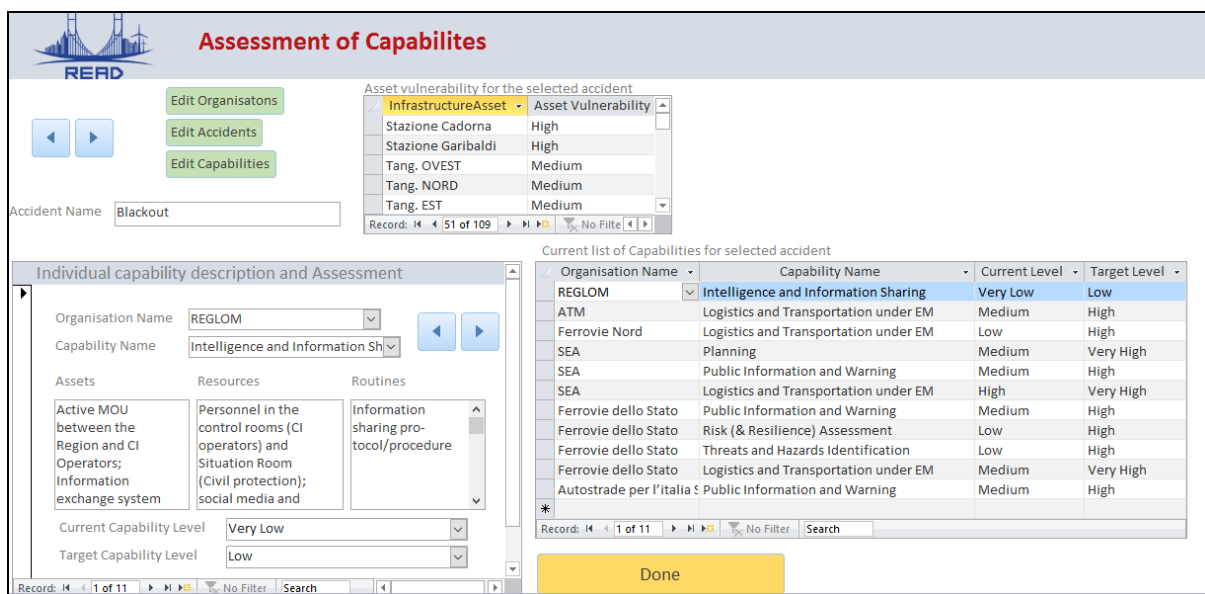
“**Assessment of capabilities**” section is where the main assessment happens (Figure 13). The first thing to pay attention to is the Accident Name. Assessment is done referring to a specific accident event at a time (if there is more than one). User can navigate through Accidents using the arrows.

There are two tables that assist user to perform the assessment. ‘**Asset vulnerability for the selected accident**’ window (at the top) shows the list of defined Infrastructure Assets side-by-side with their vulnerability for the selected Accident, to be considered while doing assessment.

Capabilities are managed inside ‘**Individual Capability description and assessment**’ window. The first step is to select a pair, Organisation Name and Capability Name, both from the dropdown menus. User then describes in which way the capability is specifically implemented in the organization, by means of *Assets*, *Resources* and *Processes*, typing in the text boxes right underneath. The last step consists of assessing the *Current Capability Level* (as it is at the moment) and the *Target Capability Level* (i.e. desired level), as planned by the corresponding organization. ‘**Current list of Capabilities for selected accident**’ window gives a list of the list of existing Organisation-Capability pairs (including their assessments) for an easier navigation and a better overview.

To sum up, the Gap Analysis is performed to identify the weaknesses (gaps) in the capabilities, considering the accidents and related system vulnerabilities. Target value for each capability should be deliberated with the aim to cover all the gaps and make the system completely fitting with its exposure to the considered accident.

“Done” button will take user back to the Resilience Assessment window where he can now do the analysis.



**Figure 13: Description and Assessment of individual resilience capabilities**

The capability assessment scale we have proposed considers a combination of its coverage of different H&T on one side, and the complexity of the accident in can cope with on the other (Figure 14).

For an existing Capability there are five possible levels: *Very Low* (1), *Low* (2), *Medium* (3), *High* (4) and *Very High* (5), distributed according to the explained criteria (Figure 14). The scale is not strict and can be adjusted to any particular case.

		Capability coverage of hazards and threats		
		Single or few	Several	All-hazard
Type of accident event	Simple	1 - Very low	2 - Low	3 - Medium
	Complex	2 - Low	3 - Medium	4 - High
	With cross-border effects	3 - Medium	4 - High	5 - Very High

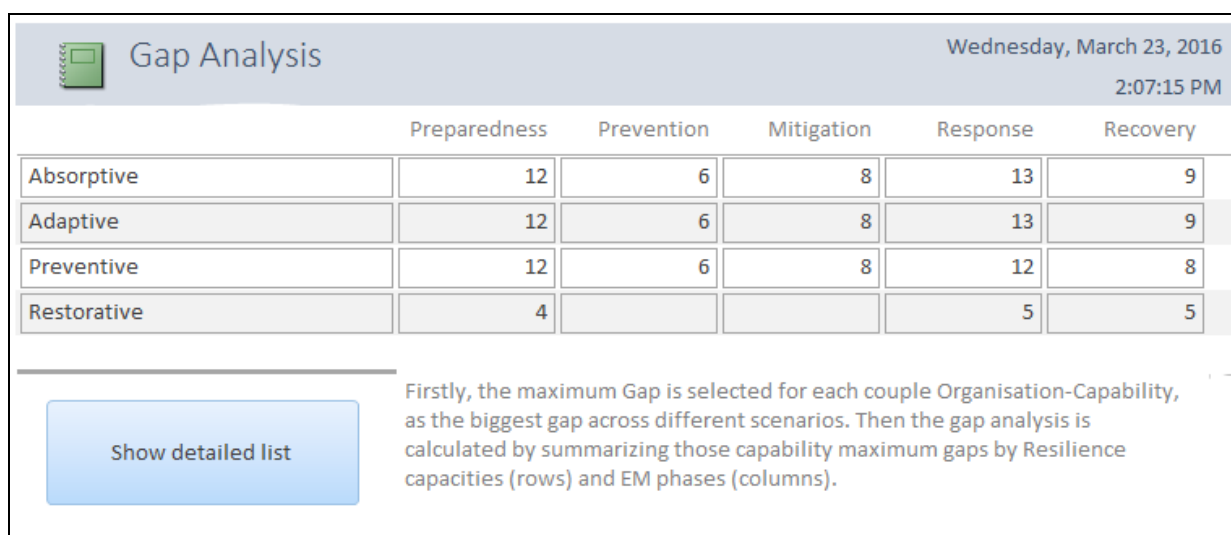
**Figure 14: Proposed assessment scale**

## 6. Outputs

By choosing a scenario (Figure 12) and clicking on “**Show Capability Analysis**” user will get a list of available capabilities listed by organisations, in a table form, for the selected accident event. The function shows the distribution of capabilities as well as their compounds.

“**Show Gap Analysis**” presents an overall capability gap matrix (Resilience Goals vs. EM phases) – Figure 15.

The gap analysis is not tied to a specific accident but to the overall EM and resilience state, based on capabilities, and it includes all organizations. In the gap analysis, the maximum gap is selected for each Organization-Capability couple, as the biggest gap across different scenarios. The gap is then calculated by summarizing the capability gap by Resilience Capacities (rows) and EM phases (columns). The Gap is added to the matrix for each Capability referring to the Capability classification. The Gap Analysis shows a comprehensive picture giving quantitative indicators, enabling analyst to easily identify weak points. It also gives a clear clue about where the future improvements will be focused.



**Figure 15: Gap Analysis**

“Show detailed list” button shows full details of all the Organisation-Capability couples (Figure 16). Using filtering and sorting in columns, user can get a deeper analysis.



D 2.1 READ Preparedness Tool Material and User Guide

Classification co

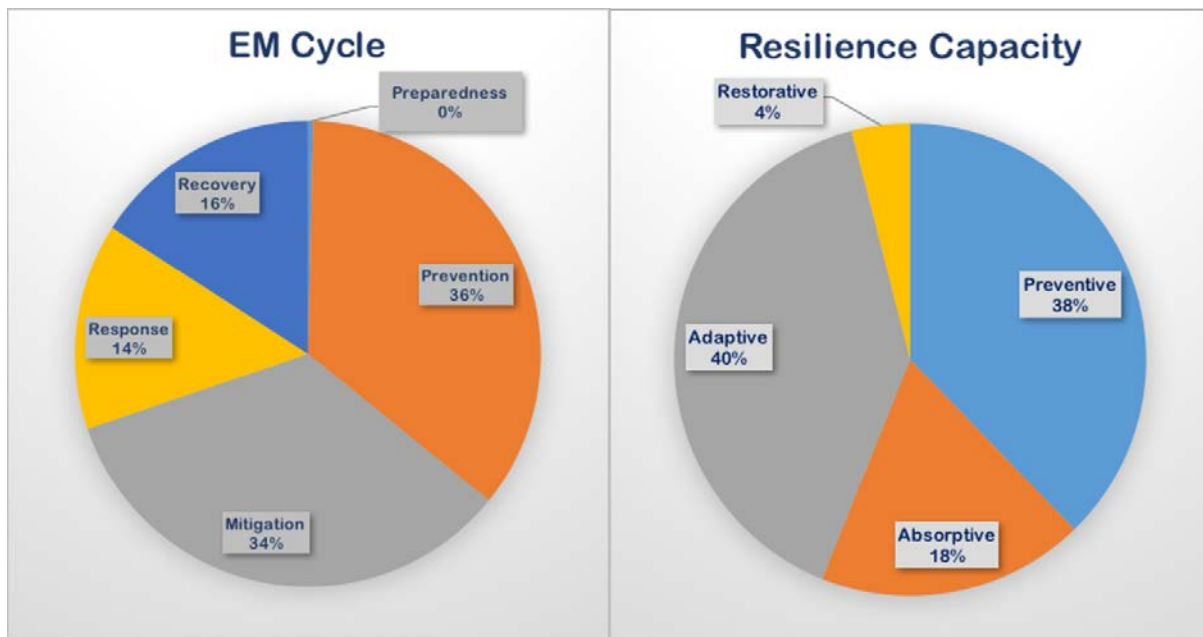
Organisation Name	Accident Name	Capability Name	Resilience Capacity	EM phase	Current Level	Target Level	Gap
ATM	Blackout	Logistics and Transporta	Adaptive, Restorative	Response	Medium	High	1
Autostrade per l'italia	Blackout	Public Information and V	Absorptive, Adaptive, Pre	Mitigation, Preparedness, Prevention, Re	Medium	High	1
Ferrovie dello Stato	Blackout	Risk (& Resilience) Asses	Absorptive, Adaptive, Pre	Mitigation, Prevention	Low	High	2
Ferrovie dello Stato	Blackout	Threats and Hazards Ide	Absorptive, Adaptive, Pre	Mitigation	Low	High	2
Ferrovie dello Stato	Blackout	Public Information and V	Absorptive, Adaptive, Pre	Mitigation, Preparedness, Prevention, Re	Medium	High	1
Ferrovie dello Stato	Blackout	Logistics and Transporta	Adaptive, Restorative	Response	Medium	Very High	2
Ferrovie Nord	Blackout	Logistics and Transporta	Adaptive, Restorative	Response	Low	High	2
REGLOM	Blackout	Intelligence and Informa	Absorptive, Adaptive, Pre	Preparedness, Prevention	Very Low	Low	1
SEA	Blackout	Public Information and V	Absorptive, Adaptive, Pre	Mitigation, Preparedness, Prevention, Re	Medium	High	1
SEA	Blackout	Planning	Absorptive, Adaptive, Pre	Mitigation, Preparedness, Prevention, Re	Medium	Very High	2
SEA	Blackout	Logistics and Transporta	Adaptive, Restorative	Response	High	Very High	1

Figure 16: Detailed overview

A generic analysis path that we can see useful in each particular case is the Gap analysis, enhanced by conditional formatting (colour codes) to highlight the gap distribution (Figure 17), and the share of total gap spread across EM phases and Resilience Goals (Figure 18).

	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	0	265	284	51	32
Absorptive	3	32	51	120	101
Adaptive	0	265	233	69	101
Restorative	3	32	0	0	32

Figure 17: Colour coded Gap Analysis (example)



**Figure 18: Gap share by EM Cycle (left) and Resilience Capacities (right)**

The next useful step is to allow user to dig deeper into any of the Gap analysis matrix cells. If he would be interested in one of the gaps (for example Absorptive-Recovery, Figure 19), he could see where does it come from, i.e. which capabilities and which organisations contribute to it, and in which amount (Figure 20). This would help refining the effort and identify possible misalignment between the strategic plans and operational capability improvement actions.



	Preparedness	Prevention	Mitigation	Response	Recovery
Preventive	0	265	284	51	32
Absorptive	3	32	51	120	101
Adaptive	0	265	233	69	101
Restorative	3	32	0	0	32

Figure 19: Colour coded Gap Analysis (example)

Capability	Actors								TOTAL per Capability
	Civil Protection	Police	Fire Brigade	Telcom Op.	Electricity Op.	Transp. Op.	Railway Op.	Voluntary Org.	
Community Resilience Building	3		3		3	3	3	3	18
Cybersecurity			2		1	3	2	1	9
Fatality Management Services	1	2		2					5
Logistics and Transportation under EM	3		0	0					3
Natural and Cultural Resources Protection	2	2	2	2	1	2	2	1	14
On-scene Security, Protection and Law Enforcement	3	3	2	2	3	3	2	3	21
Health, Healthcare and Emergency Medical Services					2				2
Public Information and Warning		2	1		2	1	3	2	11
Risk (& Resilience) Assessment	0	0		0					0
Screening, Search and Detection		3	3		3	3	3	3	18
<b>TOTAL per Actor</b>	<b>12</b>	<b>12</b>	<b>13</b>	<b>6</b>	<b>15</b>	<b>15</b>	<b>15</b>	<b>13</b>	<b>101</b>

Figure 20: An example of a more detailed gap analysis (Absorptive-Recovery)

The presented analysis up till this point covers the first and the second step of the **Capability Building Cycle** (Figure 21). In the next (third step), the objectives are set, and the implementation plan is decided upon. The fourth step (which is also the first step of the next planning cycle) is where the resilience capabilities are reassessed and reviewed after a single improvement cycle.

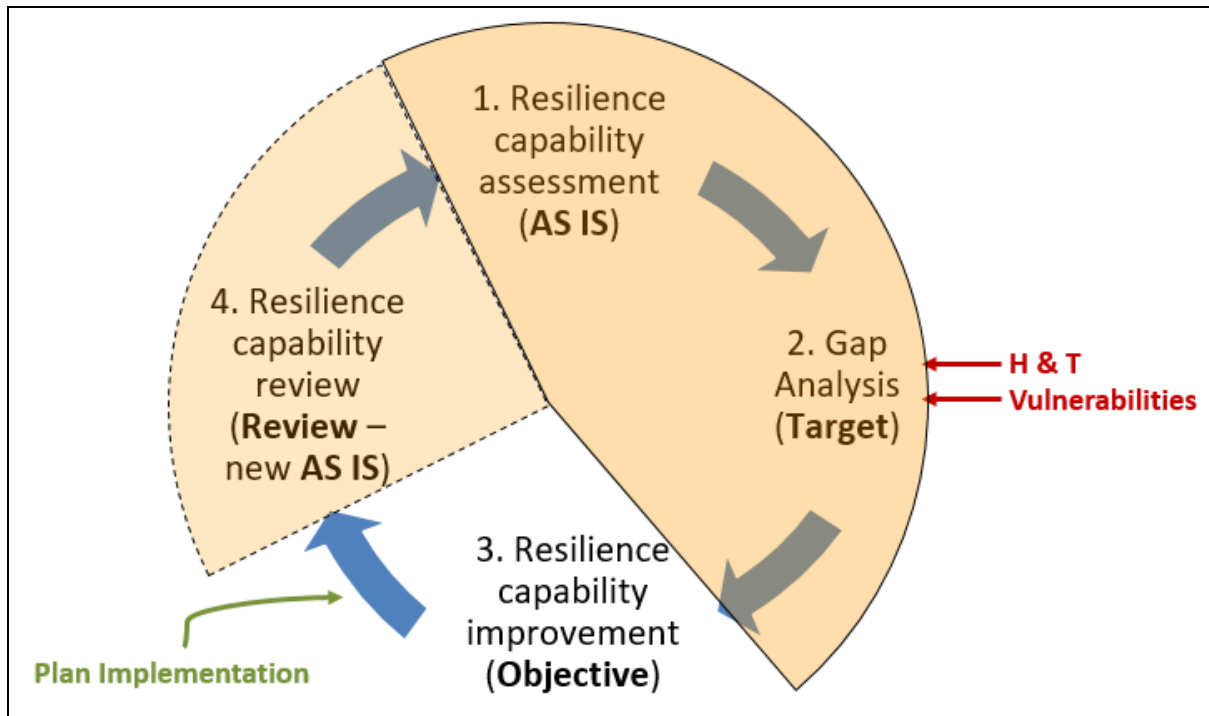


Figure 21: Capability improvement cycle, READ tool coverage



## **ANNEX: List of predefined Capabilities available inside the tool**

<b>Capability</b>	<b>General Description</b>
Planning	Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.
Public Information and Warning	Deliver coordinated, prompt, reliable, and actionable information to the whole community regarding any threat or hazard, as well as the actions being taken and the assistance being made available.
Operational Coordination	Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.
Intelligence and Information Sharing	Provide timely, accurate, and actionable information concerning all hazards and threats. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.
Interdiction and Disruption	Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.
Screening, Search and Detection	Identify, discover, or locate threats and/or hazards through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, bio-surveillance, sensor technologies, or physical investigation and intelligence.
Access Control and Identity Verification	Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.
Cybersecurity	Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.
Physical Protection	Implement and maintain risk-informed countermeasures, and policies protecting people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors.
Risk Assessment	Identify, assess, and prioritize risks to inform Protection activities, countermeasures, and investments.
Supply Chain Integrity and Security	Strengthen the security and resilience of the supply chain.
Community Resilience Building	Enable the recognition, understanding, communication of, and planning for risk and empower individuals and communities to make informed risk management decisions necessary to adapt to, withstand, and quickly recover from future incidents.



Threats and Hazards Identification	Identify the threats and hazards that occur in the geographic area; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of a community or entity.
Logistics and Transportation under EM	Provide transportation (including infrastructure access and accessible transportation services) for the evacuation of people and animals, and the delivery of vital response personnel, equipment, and services into the affected areas. Deliver essential commodities, equipment, and services in support of impacted communities and survivors, to include emergency power and fuel support, as well as the coordination of access to community vital services. Synchronize logistics capabilities and enable the restoration of impacted supply chains.
Environmental Response / Health and Safety	Conduct appropriate measures to ensure the protection of the health and safety of the public and workers, as well as the environment, from all-hazards in support of responder operations and the affected communities.
Fatality Management Services	Provide fatality management services, including decedent remains recovery and victim identification, working with regional and national authorities to provide mortuary processes, temporary storage or permanent internment solutions, sharing information with mass care services for the purpose of reunifying family members and caregivers with missing persons/remains, and providing counseling to the bereaved.
Fire Fighting	Provide structural, wildland, and specialized firefighting capabilities to manage and suppress fires of all types while protecting the lives, property, and the environment in the affected area.
Mass Care	Provide life-sustaining and human services to the affected population, to include hydration, feeding, sheltering, temporary housing, evacuee support, reunification, and distribution of emergency supplies.
Mass Search and Rescue Operations	Deliver search and rescue capabilities, including personnel, services, animals, and assets to survivors in need, with the goal of saving the greatest number of endangered lives in the shortest time possible.
On-scene Security, Protection and Law Enforcement	Ensure a safe and secure environment through law enforcement and related security and protection operations for people and communities located within affected areas and also for response personnel engaged in lifesaving and life-sustaining operations.
Operational Communications	Ensure timely communications in support of security, situational awareness, and operations among and between affected communities in the impact area and all response forces.
Public Health, Healthcare and Emergency Medical Services	Provide lifesaving medical treatment via Emergency Medical Services and related operations and avoid additional disease and injury by providing targeted public health, medical, and psychological support, and products to all affected populations.
Situational Awareness and Decision Making	Provide all decision makers with decision-relevant information regarding the nature and extent of the hazard, any cascading effects, and the status of the response.



**Natural and Cultural  
Resources Protection**

Protect natural and cultural resources and historic properties through appropriate planning, mitigation, response, and recovery actions to preserve, conserve, rehabilitate, and restore them consistent with post-disaster community priorities and best practices and in compliance with applicable environmental and historic preservation laws and executive orders.