CIRINT.NET

Critical Infrastructure Resilience International Network

Good Practices for Critical Infrastructure Resilience: a classification and assessment framework

Paolo Trucco
Giada Feletti
Boris Petrenj
Mariachiara Piraina

Executive summary

The increasing number of accidents and disasters over the last decade has highlighted the lack of structured approaches for dealing with events where Critical Infrastructure (CI) systems are directly or indirectly involved. Despite the existence of a large number of practices in use, these have often proved to be insufficient to cover the wide spectrum of Emergency Management (EM) capabilities required to successfully cope with disruptive events. Over the years, organizations have increasingly understood the importance of expanding from an approach based mainly on the Protection of CIs to an approach that places Resilience at the core. However, the lack of common approaches among different organizations and across governance levels (company, local, national, multi-national), as well as very limited operational cooperation among partners, have revealed a still unstructured and poorly integrated framework for CI-related Emergency Management.

The scientific state-of-the-art calls for the adoption of collaborative approaches to managing interdependencies, as the main cause of *domino effects,* which amplify impacts of disruptions, over space, time and social functions.

The goal of this report is to present an integrated framework for the assessment and comparison of Good Practices (GPs) in the Critical Infrastructure Resilience domain, in the perspective of collaborative Emergency Management capacity building. The GPs mainly come from local and national levels actions and programmes, emphasising the importance of fostering collaborative processes among stakeholders.

Besides the framework itself, the reader can find the list of 53 Good Practices mapped so far. The reader is warmly invited to reach out to us and point at any additional GPs that would fit here.

The framework was completed and validated through a questionnaire distributed to Critical Infrastructure Resilience experts, as a way to integrate theory-based and expert/practitioner-based knowledge.

The assessment framework enables the profiling of GPs, showing their strengths and weaknesses when used to build Emergency Management capabilities. The mapping of GPs against EM capabilities supports a better informed selection of an "optimal bundle" of GPs making sure all the EM phases and requirements are well covered.

Keywords: Critical Infrastructure, Resilience, Good Practice, Emergency Management capability

Table of Contents

Table of Figures

1. Introduction

The concept of Critical Infrastructure is related to assets or systems that are vital for the health, safety, security, economy and well-being of a society (European Commission, 2008). In particular, an infrastructure system can be defined as "a network of independent, mostly privately-owned, manmade systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services" (U.S. President‘s Commission on Critical Infrastructure Protection, 1997). Among all infrastructure systems, those systems "whose incapacity or destruction would have a debilitating impact on the defence and economic security" are regarded as critical (U.S. President‘s Commission on Critical Infrastructure Protection, 1997). Therefore, CI systems include energy supply, communications, IT networks, financial networks, food and water supply, health protection, transport, public administration operations and pipelines of dangerous substances (Wrobel, 2019).

Due to their multiple connections and interactions, CI systems are more and more susceptible to the occurrence of unexpected disasters and emergency events, highlighting the need of enhancing organizational awareness and of improving the ability to efficiently respond to unforeseen events (Tinmannsvik, et al., 2011; Colten, et al., 2012). The presence of interdependencies could undermine the safe, stable and uninterrupted functioning of CI systems, but it determines also the efficiency of the entire network. Indeed, even though the increasing complexity of CI systems and the subsequent growth of interdependencies have shown an increase in their efficiency, this large number of connections implies that CI systems are exposed to various types of interference, which in consequence may lead to the damage or complete destruction of the system components (Skolimowska, 2013). Moreover, an event affecting a CI can produce cascading failures, sending ripple or domino effects throughout regional or national CI systems (Wrobel, 2019). The presence of interdependencies has stressed the need of adopting collaborative efforts among different organizations and has supported a progressive shift from an approach purely based on the protection of CIs to one which places Resilience at the core. This new approach based on Critical Infrastructure Resilience is focused on guaranteeing functional continuity of the services when stress occurs, limiting the extent of losses and impacts and ensuring a fast recovery of normal service conditions even when the infrastructure is severely damaged (Trucco & Petrenj, 2015).

A system can be considered resilient if it embeds "abilities to prevent disruptions, absorb disruption consequences, restore lost performance, adapt to different possible scenarios (short-term) and circumstances (long-term), and overall, prepare to achieve those goals and develop those abilities" (Kozine, Petrenj & Trucco, 2018). In order to reach these abilities, Resilience management guidelines are needed to support stakeholders in making strategic decisions to guarantee continuity of operations, effectively respond and recover from failures and adaptively meet unpredictable demands. In this way, the actors involved have a clear understanding of their responsibilities and shared knowledge about Resilience management (Adini, 2017).

Effective Critical Infrastructure Resilience strategies require approaches and Good Practices based on the collaboration of numerous stakeholders, at different institutional and operational levels, that exchange information by means of a variety of channels (Trucco & Petrenj, 2015). Good Practices are generally defined as methods or techniques that are applied to solve existing problems producing effective results and bringing benefits to the users (Trucco & Petrenj, 2015). Among the GPs, a Best

Practice can be defined as “a method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark” (Trucco & Petrenj, 2015). Firms and organizations rely on Best Practices, since they have proved to be effective in addressing similar past problems. However, Best Practices are not static instruments, they have to be adjusted according to the new emerging applications and adapted to the specific needs of practitioners. For this reason, they are continuously improved and updated versions are released as soon as the conditions in the real application field evolve. By collecting evidence about the practices used in a particular context, it is possible to identify the one that represents the Best Practice in a given context and scope.

In spite of the presence of a large number of Good Practices in the context of CI Resilience, these have often proved to be insufficient to cover the wide spectrum of needed EM capabilities. The lack of common approaches and poor operational cooperation have resulted in a confusing environment, with an overlapping diversity of concepts, which emphasises the need for a structured and integrated framework for CI-related Emergency Management.

In light of the previous considerations, the aim of this study is to develop a comprehensive framework enabling the classification and comparison of GPs according to their most relevant dimensions, the activities or functionalities supported and the EM capabilities covered.

2. Research approach

In order to identify the approaches and means that practitioners and resilience experts can rely on for the management of CI-related events, the work started from the analysis of the GPs currently used in this domain. The approach used to collect and systematise information consisted of the following four-steps:

1. **Data gathering**, in which all the relevant information coming from literature and projects was collected. In particular, after the study of the existing practices contained in the *Miracle Project*, the research continued by examining the *100 Resilient Cities* project and the *EU Horizon 2020* program, taking into consideration projects such as *Darwin*, *Resiliens*, *Smart Mature Resilience* and *Resolute*. Other practices were identified by consulting scientific literature and institutional websites.
2. **Data analysis and data cleaning**, in which the practices were analysed, verifying that all of them were already consolidated, generalizable and as much consistent as possible. At the end of this step, 53 GPs were selected.
3. **Data presentation**, in which each GP was presented in a standardized way, using a common structure to identify its main features and objectives.
4. **Categorization**, in which each GP was categorized according to its main functionality.

The analysis of the GPs supported the development of three different classification frameworks. Indeed, the collected information enabled the identification of useful dimensions of classification for the GPs, their main activities or functionalities and the capabilities of Emergency Management that they are able to cover. These elements were used to build respectively the *Classification dimensions of GPs*, *Activities and functionalities of GPs* and *Emergency Management capabilities* frameworks.

Once the three different frameworks were developed, the research proceeded with their integration through the distribution of the Critical Infrastructure Resilience Questionnaire. The questionnaire was intended to collect experts' assessment of the importance (i.e. positive contribution) that activities and functionalities provided by GPs may have in building of the EM resilience capabilities.

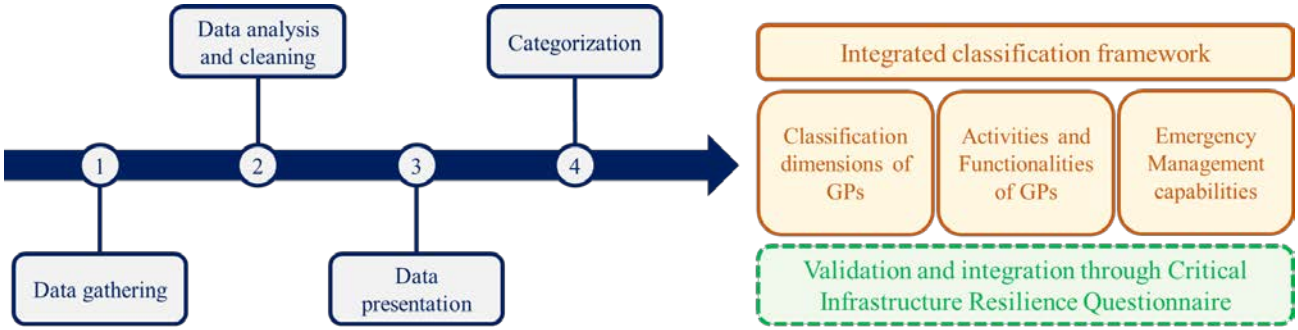

Figure 1: Research approach

The information collected from scientific literature, projects and institutional websites were integrated with the results coming from the questionnaire, and this represented the input for the development of several analyses. The analyses focused on GP's ability to homogeneously cover different capabilities, feasibility to cover a specific capability in a real context, on the potential for improvement of each GP, and on the development of an optimal bundle of GPs.

3. Description of the GPs

The 53 selected GPs have the common aim of supporting institutions and organizations in the management of emergencies affecting CI systems. However, they achieve this goal by adopting different instruments and methodologies. Therefore, after the preliminary analysis of GPs' features, emerged a need of grouping them into *clusters* corresponding to the main functionality covered. The adopted subdivision includes six clusters described below.

Information sharing cluster is composed of GPs which have the main purpose of facilitating the sharing of situational information or knowledge at different levels (e.g. organizational, national, multinational). The Good Practices in this cluster are mainly web-based information-sharing platforms that facilitate collaboration and coordination between public, private and non-profit organizations, providing greater visibility of impacts and strengthening the resilience of communities. The constant collaboration among institutions leads to the development of integrated strategies for the management of CI emergencies which take into consideration the presence of system interdependencies. This strategic alignment can help to avoid delays in the response phase and to better organize resources for rescue and recovery operations. This cluster includes also tools or programs that allow access to researches, knowledge and Best Practices, highlighting what has proved to work well in the implementation of specific policies by other partners. In this way, users can exploit these lessons learned, avoiding mistakes and guiding the implementation of a resilience strategy in a more effective manner, increasing their knowledge expertise about CI Resilience. The list of GPs belonging to the *Information sharing* cluster is provided in Table 1.

Table 1: GPs belonging to Information sharing cluster

INFORMATION SHARING GPs
V-BEOC (Virtual Business Emergency Operations Center)
NWWARN (Northwest Warning, Alert and Response Network)
DARWIN Wiki
Focus on Flows
MATRICS (Multi Actor Threat Recognition, Information and Collaboration System)
SATool (Situational Awareness Tool)
Resilience Building Policies
Multi-State Fleet Response Initiative
Big Business – Small Business
Louisiana Disaster Recovery Alliance

Geographical visualization and information sharing cluster is composed of GPs that have the main purpose of both monitoring the areas of interest through geographical visualization and sharing the needed information within those areas. Most of these practices are tools that allow for a georeferenced visualization of events, strategic places, resources and possible dangerous situations, and provide information for emergency response in relation to different types of disasters. They often include GIS

maps to monitor areas showing emergency situations, or awareness systems to provide information supporting risk management and emergency response. Furthermore, this cluster includes Apps that can provide tailored instructions during emergencies and allow the public to upload contents. The geographical visualization provided by these GPs can support operators by showing the quickest way to reach the affected areas, as well as citizens by diverting traffic towards alternative routings, thus reducing congestions near the location of the emergency event. The list of GPs belonging to the *Geographical visualization and information sharing* cluster is provided in Table 2.

Table 2: GPs belonging to Geographical visualization and information sharing cluster

GEOGRAPHICAL VISUALIZATION AND INFORMATION SHARING GPs
Cruscotto Emergenze
Copernicus Emergency Management Service
GIS Mapping for CI Assets
Resilience Information and Communication Portal
Traffic Scotland Information Service
ESSMA (Emergency Support Smart Mobile App)
CRAMSS (Collaborative Resilience Assessment and Management Support System)

Planning cluster includes practices that provide guidelines to better prepare CI operators and institutions to cope with disruptions. They give ad-hoc instructions, guidance notes, templates or structured steps to support risk and resilience assessment, decision-making and information sharing. In particular, they provide instructions on how to collect data and information about the topic of interest, how to identify relevant stakeholders and interdependencies among systems, how to set priorities and needs for interventions, and finally how to develop and implement a strategic plan. These GPs require a comprehensive and targeted organizational setup which includes the formation of teams, sub-teams and working groups according to experts' background, assigning them well-defined objectives, clear tasks and responsibilities. The continuous communication and engagement with stakeholders, in some cases even including the general public (e.g. citizen associations and activated citizens), provides an important contribution in developing effective plans. The list of GPs belonging to the *Planning* cluster is provided in Table 3.

Table 3: GPs belonging to Planning cluster

PLANNING GPs
PRISM (Performance and Risk-based Integrated Security Methodology)
COLAB
TTF (Thematic Task Forces)
Partnership Alignment for Enhanced Security
European Resilience Management Guideline
Public Safety Canada

Training, exercising and simulations cluster includes practices whose objective is to provide adequate preparedness for CI operators, institutions and experts to deal with all the phases of the Emergency Management. They are applied in different contexts such as interdependence analysis, cyber-attacks prevention and resource allocation efficiency. These GPs can be either in the form of tools (e.g. simulation platforms) or processes (e.g. workshops, exercising programs). Simulations create a virtual environment to test specific tasks or policies adopted during rescue operations, disruptions to resource availability and the consequent effects on CI operations. The results obtained allow to validate the impacts of implementing different policies that could, potentially, be included in the resilience strategy of an area. Users can try different policy options (different scenarios), identifying the implications of each of them in the resilience improvement process. They can, therefore, use simulations as a training environment to find the right path towards improving local resilience. Exercise programs, instead, allow dealing with response, recovery and mitigation activities, trying to guarantee better visibility of available resources and needs in affected areas, and to find ways to guarantee first aid. The analysis of cascading impacts is made through the development of different scenarios aimed at increasing awareness about vulnerabilities and interdependencies of CIs, so that it is possible to identify potential gaps in current plans and intervene to improve them. Indeed, results obtained by exercises offer stakeholders an opportunity to discuss emergency plans and to prioritize the actions needed to update them. Finally, workshops engage stakeholders, experts and sometimes citizens to communicate existing problems, trying to effectively understand their root causes and learn about new ways to solve them. These discussions lead to the identification of challenges and barriers that hinder opportunities, considering existing and needed resources, as well as developing a vision statement and planning the next steps to achieve these opportunities. The list of GPs belonging to the *Training, exercising and simulations* cluster is provided in Table 4.

Risk/Resilience assessment cluster is composed of practices that have the main purpose of supporting the analysis of interdependencies and assessing risk and resilience levels. Tools based on flexible cartography approaches are used for the analysis of the interdependences and the simulation of the domino effects, showing the location sectors where the consequences of the system failures are synthesized. Thanks to constant monitoring of the territory, they are able to assign a risk level to the different areas that could be impacted by an emergency event. Other tools are based on templates that guide users throughout the whole process of risk or resilience assessment. In this regard, they support an assessment of how shocks and stresses in the local area interact to impact specific assets, specific locations, different business sectors, residents and users. This leads to a prioritization of shocks and stresses and to the identification of vulnerable physical assets. Based on the risk level assigned to the key hotspots, some GPs provide access to policies recommendations that may be used to address the most relevant risk scenarios and that can support the identification of measures to mitigate risks within the area. A similar approach is followed to evaluate the resilience levels of a region. Starting from the identification of CI critical functions and system interdependencies, resilience assessment tools generate a quantitative overall resilience score for CIs and individual resilience scores for specific assets, and finally provide guidelines to enhance those resilience levels. The list of GPs belonging to the *Risk/Resilience assessment* cluster is provided in Table 5.

Table 4: GPs belonging to Training, exercising and simulations cluster

TRAINING, EXERCISING AND SIMULATIONS GPs
Blue Cascades Exercise Series
MICC (Major Incident Control Committee)
CATEX (Catastrophic Exercise)
City Resilience Dynamics
SimEnv
Serious Games based on Virtual Reality
GINOM (Global Infrastructure Network Optimization Model)
Opportunity Assessment Tool
Problem Framing
Project Scan Tool
Resilience Accelerator
Resilience Garage
Resilience Value Realization
100 RC Systems Studio
Tactical Urban Resilience

Table 5: GPs belonging to Risk/Resilience assessment cluster

RISK/RESILIENCE ASSESSMENT GPs
DOMINO Tool
GRRASP (Geospatial Risk and Resilience Assessment Platform)
Assets and Risk Tool
Local Area Risk Assessment
Risk Systemicity Questionnaire
THREVI2
CI System Definition Tool
Resilience Management Matrix Tool
GIS based Resilience Mapping Tool
Resilience Management Audit Tool
City Resilience Index
Smart Resilience Indicators
Resilience Maturity Model
Resilience Actions Inventory and Stakeholder Perceptions Review

Business Continuity Management includes programs for embedding business continuity into organizations (BCM of an enterprise) and regions (Area BCM) to help them cope with CI disruptions.

After having defined the purposes and objectives that an organization wants to attain, BCM for an enterprise requires a business impact analysis (BIA) to identify critical operations, processes and resources, and the impact of a disruption on the business. A plan developed and implemented by an enterprise includes strategies and measures for each critical item previously identified. While the traditional BCM system is designed to prevent the company's core business from being suspended in emergency circumstances, Area BCM aims to secure the critical resources, which include external goods and services essential in supporting the business operation in and around an agglomerated area. In particular, the analysis of regional risks and hazards and the evaluation of CI resilience, lead to the development of an Area BCM strategy by preparing disaster risk scenarios and performing a BIA. The resulting Area BC Plan should address various issues, including CI protection, coordinated disaster preparedness and response, quick recovery from damages, supply chain cooperation and monitoring of BCM activities. The list of GPs belonging to the *Business Continuity Management* cluster is provided in Table 6.

Table 6: GPs belonging to Business Continuity Management cluster

BUSINESS CONTINUITY MANAGEMENT GPs
BCM for enterprises
Area BCM

4. Framework for CIR GPs assessment

The aim of this study is to develop a comprehensive framework which allows to effectively compare Good Practices and to choose the most suitable ones ('Best Practices') for a specific context. In this regard, the structured analysis of the GPs allowed identifying the main information required for an effective classification and assessment. In particular, three different frameworks were developed:

- Classification dimensions of GPs;
- Activities and Functionalities of GPs;
- Emergency Management capabilities.

4.1 Classification dimensions of GPs

The *Classification dimensions of GPs* framework includes several dimensions that highlight the relevant characteristics of the different GPs, considering the type of support they are able to provide, the stakeholders that have to be involved and their context of application.

First of all, ***Good practice type*** dimension classifies the GPs according to their nature (Trucco & Petrenj, 2015):

- Tools and Technologies: GPs achieve their specific goals through a set of means, instruments, methods and techniques.
- Processes: GPs achieve their specific goals through actions, tasks, arrangements and procedures.

The second dimension included within the framework is the ***Emergency Management Phase*** (Trucco & Petrenj, 2015), which identifies the phases of EM supported by a specific GP. EM is the discipline of coping with and avoiding disasters. Following the classification and the definitions provided by FEMA, it involves the phases of Preparedness, Mitigation, Response and Recovery in order to lessen the impact of disasters:

- Preparedness: it is the state of being prepared in order to act during a disaster or emergency. It includes emergency plans, training and exercises that individuals, communities and first responders perform with a pre-defined frequency. It requires a continuous cycle of planning, organizing, training, equipping, exercising, evaluating and taking corrective actions. This phase takes place before a disaster happens.
- Mitigation: it is the ability to prevent damages by reducing the impact of disasters and their related consequences. It is primarily focused on risk assessment, prevention, protection and reduction of the impact of future emergencies. This phase can take place both before and after an emergency happens.
- Response: it includes actions and activities undertaken to address the decision-making process for coping with a hazard. It consists of putting the preparedness phase into actionable plans. This phase takes place during an emergency.
- Recovery: it is the ability to come back to the initial conditions with limited suffering after a disaster. The process is a long-term action of restoring the community back to pre-disaster conditions. This phase takes place following a disaster.

The ***Project Phase*** dimension aims at identifying the stage at which the GP is used, it explains is a practice is implemented before, during or after a disruption. This dimension should not be confused

with the previous one. Indeed, *Emergency Management Phase* indicates which phases are supported by the GPs, while *Project Phase* indicates when a GP is used in a given timeline.

Another dimension taken into consideration is ***Partnership type***, which concerns the type of organizations involved in the partnership: public organizations, private ones or both. According to FEMA (2014), the requirement of protection of national infrastructures is growing more and more. Therefore, governmental agencies are establishing partnerships with private-sector organizations to improve resilience during all the phases of Emergency Management. In this regard, partnerships are collaborative relationships built on needs (each member of a partnership receives resources or support from other partners), capabilities (each member of the partnership can leverage on its own set of capabilities) and two-way communication (partners are required to communicate their needs and their capabilities to all the other members). Through public-private collaboration, resilience can be improved thanks to an enhancement of situational awareness, a better decision-making process, an easier access to more resources and capabilities, an improvement of coordination and an increase in the effectiveness of the EM efforts.

To further detail the *Partnership Type*, the ***Key partners*** dimension is used to specify the different stakeholders involved, (i.e. public institutions, CI operators, universities, CI Experts, communities, public and private companies and resilience experts).

Moreover, the ***Organizational Interdependence*** dimension has been introduced to understand if the practice can be adopted by a unique institution or requires collaboration among different organizations. As explained by Cipsec (2018), interdependencies generally increase the vulnerability of the CIs even if their integration can provide valuable benefits in terms of efficiency, service quality and cost reduction. In order to protect a globally interconnected CI system, according to Abou El Kalam (2015), it is necessary to secure cooperation between different organizations with different features, functioning rules and policies. In this context, it is important to secure not only intra-organizational workflows, but also inter-organizational ones through audit and assessment.

Another relevant dimension is the ***Data Type***, which indicates if the GP is able to provide real-time support during a crisis or disruption, by showing real-time situational information. In this regard, according to Kostopoulos (2013), the use of real-time GPs could guarantee effective and timely protection of CIs, keeping their performances high even in presence of interconnections.

Extension is a dimension concerned with the geographical area of application of practice (i.e. city, region, country or more countries). According to the flexibility of the GP, it may be possible to start using it for a limited area just as a pilot test and then extend it to a larger area of application.

Finally, the last dimension taken into consideration is ***Applicability***. In particular, it indicates if a GP can be applied only within a specific context or it can be flexibly and broadly applied in different cases.

Table 7 summarizes the dimensions and the related categories that compose the first classification framework.

Table 7: Classification dimensions of GPs

DIMENSIONS	CATEGORIES

GP Type	Tool and Technologies Processes
Emergency Management Phase	Preparation Mitigation Response Recovery
Project Phase Partnership Type	Before During After Public Private
Key Partners	Public Institutions CI Operators Universities CI Experts Communities Public and Private Companies Resilience Experts
Organizational Interdependence Data Type	Intra-organizational Inter-organizational Real-Time Deferred
Extension	City Region State Neighbouring Countries
Applicability	Broad Specific

The *Classification dimensions of GPs* framework was built using the information coming from the GPs description. The framework allows visualizing the nature of the practices and the context of their use, highlighting their similarities and differences.

4.2 Activities and Functionalities of GPs

The *Activities and Functionalities of GPs* framework is intended to identify the different operations and tasks that the GPs are able to support. From the analysis of the GPs features, the need of making a distinction between *Processes* and *Tools and Technologies* emerged. Due to their different nature, *Processes* can be described through actions and tasks performed by an organization or a group of them to achieve an aim and therefore they can be associated with a set of activities. On the other hand, *Tools and Technologies* can be described through the operations performed by a piece of equipment or software to fulfil an objective and therefore they can be associated with a set of functionalities (Cambridge dictionary). For this reason, on the basis of the *GP Type* of the first classification, the *Activities and Functionalities of GPs* framework identifies the functionalities or activities supported respectively by tools or processes.

The functionalities of *Tools and Technologies* are included in Table 8 (Shannon, 1948; MacEachren, Kraak, 1997, Cambridge dictionary; NIMSAT; CCOHS).

Table 8: Functionalities of Tools and Technologies

FUNCTIONALITIES	DESCRIPTION
Communication channel	It allows exchanging information among entities (organizations, people and technologies). It refers either to a physical transmission medium or to a logical connection. A channel is used to convey an information signal from one or several senders to one or several receivers.
Geographical visualization	It refers to a set of tools and techniques supporting the analysis of geospatial data through the use of interactive visualization.
Alerting/warning	In the context of CIs, it represents a signal that makes you understand if there is a possible danger or problem, especially one in the future.
Training/exercising	It allows to improve all-hazard incident management capabilities as well as integration and interoperability, during the preparedness phase of emergency management.
Planning	Planning is the fundamental management function, which involves deciding beforehand, what is to be done, when is it to be done, how it is to be done and who is going to do it. It is an intellectual process that develops various courses of action, by which it is possible to achieve predetermined objectives. It explains how to attain a specific goal.
Coordination	It is the process of allocating and managing all the resources during the response phase of Emergency Management.
Risk assessment	It refers to the overall process or method of hazard identification (identify hazards and risk factors that have the potential to cause harm), risk analysis and risk evaluation (analyze and evaluate the risk associated with that hazard), risk control (determine appropriate ways to eliminate the hazard, or control the risk when the hazard cannot be eliminated).
Knowledge management	It includes the sharing of lessons learned, guidelines and Best Practices for continuous improvement.
Decision support	It is an information system that supports business, organizations or authorities in decision-making activities. It explains how to put in practice the knowledge acquired through knowledge management function.

The activities of Processes are included in Table 9 (NIMSAT; CCOHS; Prevention Consortium; CDC).

Table 9: Processes activities

ACTIVITIES	DESCRIPTION
Communication	It is the activity which allows exchanging information among entities (organizations, people and technologies).
Expert involvement	It includes the involvement of experts to share lessons learned, guidelines and Best Practices for continuous improvement.
Training/exercising	It allows to improve all-hazard incident management capabilities as well as integration and interoperability, during the preparedness phase of Emergency Management.
Planning	Planning is the fundamental management function, which involves deciding beforehand, what is to be done, when is it to be done, how it is to be done and who is going to do it. It is an intellectual process that develops various courses of action, by which it is possible to achieve predetermined objectives. It explains how to attain a specific goal.
Coordination	It is the process of allocating and managing all the resources during the response phase of Emergency Management.
Risk assessment	It refers to the overall process or method of hazard identification (identify hazards and risk factors that have the potential to cause harm), risk analysis and risk evaluation (analyze and evaluate the risk associated with that hazard), risk control (determine appropriate ways to eliminate the hazard, or control the risk when the hazard cannot be eliminated).
Surge management	It involves all the activities that are performed during the response phase of emergency management as a first response to a crisis or disruption.
Decision support	It is the activity which supports business, organizations or authorities in the decision-making process.
Monitoring	It involves the collection of routine data that are used to track changes in the situation over time. It provides regular feedbacks and early indications of possible disruptions. Its purpose is to permit the management and stakeholders to make informed decisions regarding the effectiveness and the efficient use of resources.
Brainstorming/problem solving/lessons learned	Brainstorming is an activity or business method in which a group of people meet to suggest new ideas for possible development. Problem-solving is the process of finding solutions to problems. Lessons learned is knowledge or understanding gained by experience.

The information coming from the GPs description was used to fill the *Activities and Functionalities of GPs* framework. For each GP, a score from zero (activity/functionality not supported) to five (activity/functionality fully supported) is assigned to assess if and how an activity or functionality is covered. The outcome is a framework that allows visualizing which activities/functionalities a GP is able to provide and which level of support it is able to guarantee.

Besides the association of each GP with the correspondent activities/functionalities, the study allowed also to find a link between the activities and the functionalities taken into consideration. In particular, the analysis of *Tools and Technologies* enabled to determine which activities are supported by a

specific functionality of the practices. The results were summarized in an *Aggregate Matrix* and were used to determine if there is a lack of tools that can support a determined activity, or if there is any activity that can be supported by different functionalities at the same time. The cells of the *Aggregate Matrix* represented in Table 10 are coloured in orange if the functionality can be used to support the specific activity.

Table 10: Aggregate Matrix

		ACTIVITY									
		Communication	**Expert Involvement**	**Training/ Exercising**	**Planning**	**Coordination**	**Risk Assessment**	**Surge Management**	**Decision Support**	**Monitoring**	**Brainstorming/ Lessons Learned**
FUNCTIONALITY	**Communication Channel**										
	Geographical Visualization										
	Alerting/ Warning										
	Training/ Exercising										
	Planning										
	Coordination										
	Risk Assessment										
	Knowledge Management										
	Decision Support										

From the analysis of the *Aggregate Matrix*, the following results were obtained:

- Expert involvement and Brainstorming/problem solving/lessons learned activities are not supported by any tool;
- Planning activity is supported by different functionalities, which are Communication channel, Training/exercising, Planning, Risk assessment and Knowledge management;
- Risk assessment activity is supported by different functionalities, which are Geographical visualization and Risk assessment;
- Surge management activity is supported by different functionalities, which are Alerting/warning and Decision support;
- Decision support activity is supported by different functionalities, which are Knowledge management and Decision support;
- Monitoring activity is supported by different functionalities, which are Geographical visualization and Alerting/warning.

4.3 Emergency Management capabilities

Emergency Management Capabilities framework identifies the capabilities that each GP is able to cover. The term *capability* of an entity (e.g. organisation, system, person) can be generally defined as a feature, faculty or process that promotes the achievement of its objectives (Kozine, Petrenj & Trucco, 2018). The capabilities that promote the resilience goals are called *resilience capabilities*. Or differently said, *resilience capabilities* can be understood as enablers of activities and functions that serve the resilience goals (Kozine, Petrenj & Trucco, 2018), so they refer to the ability of an organization to prepare, mitigate, respond and recover from a particular threat or hazard. The areas covered by EM capabilities include resource management for the allocation and deployment of resources, risk management to direct and control an organization with regard to risk, communication and coordination to favour the information exchange outside the boundaries of the organization, emergency management planning for establishing measures and assessing needs, and surge management to provide support to humans and environment.

The capabilities considered for the study are included in Table 11 (FEMA, 2020; ISO 22325, 2016; Centers for Disease Control and Prevention, 2018; Trucco, Petrenj, Di Mauro, 2018).

Table 11: Emergency Management capabilities

CAPABILITY	DESCRIPTION
Access control and identity verification	It concerns the adoption of physical, technological and cyber measures to verify the access to critical locations and systems.
Logistics and transportation services	It is related to the provision of logistics and transportation services in the affected areas to deliver necessary items and services, and to evacuate people and animals.
Community Resilience building	Starting from the identification, communication and planning for risks, it is the ability of organizations to empower communities to withstand and recover from short- and long-term incidents.
Interdiction and disruption	It is the ability to "delay, divert, intercept, halt, apprehend, or secure threats and/or hazards."
Threat and Hazards identification	It is the identification of threats and hazards in a given area (including frequency and magnitude determination) with the aim of understanding the needs on the ground.
Risk assessment	It includes identification, assessment and prioritization of risks in order to implement adequate measures.
Supply chain integrity and security	It is the ability to "strengthen the security and Resilience of the supply chain". It relies on improving the security and Resilience of key nodes and the related movements between these nodes.
Information sharing	It is the exchange of timely and accurate information and data among governments or other organizations to better respond to disruptive events.
Operational coordination	It concerns the presence of a coordinated operational structure and process to integrate emergency responders' operations.
Public information and warning	It is related to the delivery of information to the whole community regarding the threats or hazards, the actions implemented and available assistance.
Planning	It is the ability to "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".

Environment protection services	It includes all the services aimed at protecting and restoring the surrounding environment (e.g. natural and cultural resource protection) from hazards.
Human protection services	It includes all the services (e.g. mass care, emergency medical services, mass search and rescue operations) aimed at providing support to affected populations. For instance, it wants to protect the public and workers delivering emergency supplies as soon as possible.
Cybersecurity	It is related to the adoption of measures to protect (or restore) "electronic communications systems, information, and services from damage, unauthorized use, and exploitation".

The information coming from the GPs description was used to fill the *Emergency Management Capabilities* framework. For each GP, a score from zero (capability not covered) to five (capability fully covered) is assigned to assess if and how a capability is covered. The outcome is a framework that allows visualizing which capabilities a GP is able to provide and which level of coverage it is able to guarantee.

To enable an effective classification and assessment of GPs, the three frameworks needed to be deeply integrated. In this regard, the link between the *Classification dimensions of GPs* and the *Activities and Functionalities of GPs* was done on the basis of the *GP Type* dimension present in the first classification framework; in particular, the GPs characterized as *Tools and Technologies* were associated to the correspondent functionalities, while the ones characterized as *Processes* were associated to the correspondent activities. On the other hand, the link between the *Activities and Functionalities of GPs* and the *Emergency Management capabilities* was done through the submission of the Critical Infrastructure Resilience Questionnaire, whose aim was to understand the importance of each activity and functionality in guaranteeing a specific capability. Figure 2 represents the structure of the integrated classification framework, highlighting its components and their relationship.

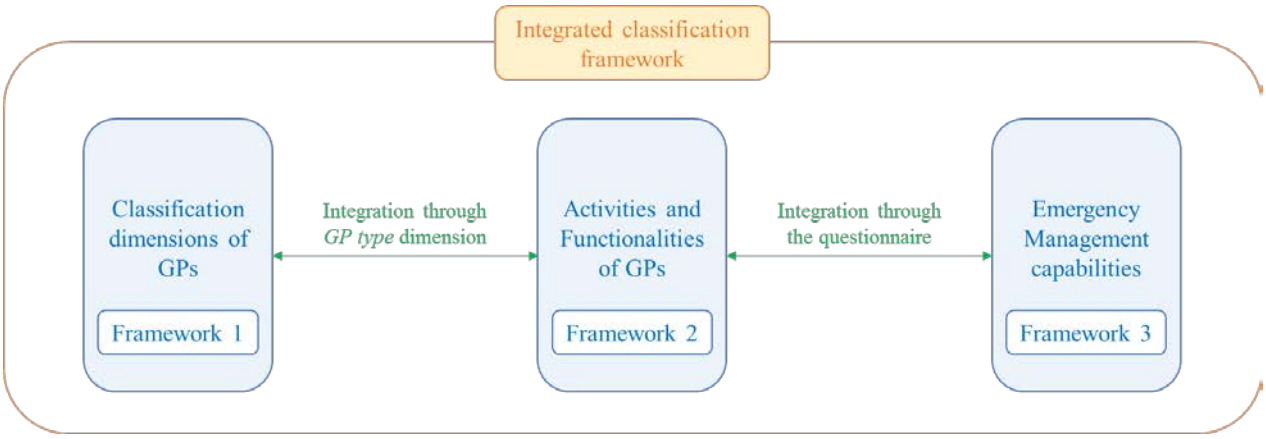

Figure 2. Integrated classification framework

5. Experts' judgement elicitation procedure

The Critical Infrastructure Resilience Questionnaire was intended to collect experts' judgements for linking the list of activities and functionalities with the generalised taxonomy of Emergency Management capabilities (Figure 3). More specifically, the aim was to assess the importance (positive contribution) that activities and functionalities provided by GPs have in the building of the resilience capabilities used in EM.

Functionalities and Activities (F&A) are used in the big framework as an intermediary between GPs and Capabilities. Their goal is to bridge the side of GPs (which are numerous and will further grow in number) with the side of Resilience Capabilities. This approach not only solves the problem of the impracticality of directly assessing GPs against capabilities (requires enormous effort by experts), but ensures the scalability and sustainability of the framework application. Once F&A are mapped against capabilities by experts, the framework is functional and the analysis can be smoothly expanded by adding new GPs which are then easily connected to F&A.

The final result we look at is assessing the contribution of each GP to Resilience capabilities in EM.

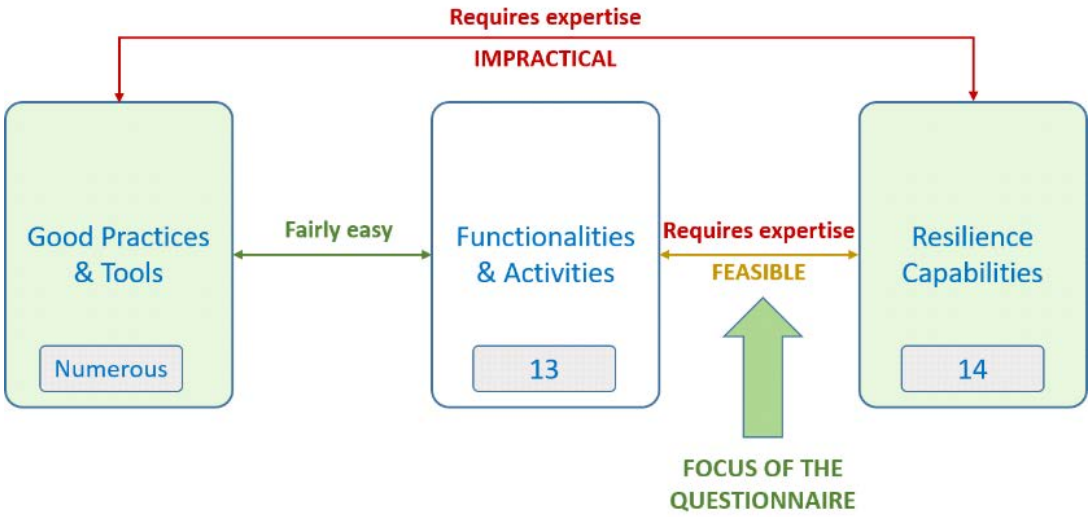

Figure 3. The logic and the need of the questionnaire

The questionnaire was structured in the following way:

- Section 1 – Background Information: it is aimed at knowing the educational background, the current function and the main areas of involvement of the respondent. In this section, questions are in an open form and their answers are mandatory.
- Section 2 – Capabilities & Functionalities/Activities Questionnaire: it is aimed at understanding the importance of each functionality and/or activity in guaranteeing a specific capability. In this section, questions are mandatory and are structured using the Likert scale form, ranging from 1 (low importance of the activity/functionality in guaranteeing the capability) to 5 (high importance of the activity/functionality in guaranteeing the capability). For each capability, experts are required to fill the following table:

	1 Low	**2** Medium Low	**3** Medium	**4** Medium High	**5** High
Communication	○	○	○	○	○
Geographical Visualization	○	○	○	○	○
Alerting/Warning	○	○	○	○	○
Training/Exercising	○	○	○	○	○
Planning	○	○	○	○	○
Coordination	○	○	○	○	○
Risk Assessment	○	○	○	○	○
Knowledge Management	○	○	○	○	○
Decision Support	○	○	○	○	○
Expert Involvement	○	○	○	○	○
Surge Management	○	○	○	○	○
Monitoring	○	○	○	○	○
Brainstorming/Problem Solving/ Lessons Learned	○	○	○	○	○

Table 12. Likert scale questions structure

- Section 3 – Additional Questions: it is aimed at further analysing the classification framework, by increasing its consistency. In this section, questions are in an open form and answering is optional. In particular, the aim is to verify if there are other important capabilities to expand the list of the already mentioned one, to investigate if there are Good Practices for Critical Infrastructure Resilience that could be useful to integrate into the study, and to collect additional suggestions or comments in order to get interesting insights for further analyses.

The experts targeted by the questionnaire were first responders, operators, consultants, researchers or other practitioners active in the CI Resilience domain. The questionnaire was submitted on the 3rd of July 2020 and a recall was made on the 4th of August 2020. The answers included in the analysis are the ones received before the 28th of August 2020, however, the questionnaire was kept open to collect additional feedback from experts. For this reason, this study can be considered as an input for further assessments which could involve a wider spectrum of participants, thus increasing the consistency of the results. During the time frame considered, the questionnaire received 18 responses, 14 of which complete and consistent, coming from 11 different countries.

After having excluded the inconsistent data, the answers provided in Section 2 of the questionnaire were treated by calculating their median, thus assessing the importance of an activity or a functionality in determining a specific capability. An ABC analysis based on the Pareto rule was then applied to prioritize activities and functionalities:

- Class C: low importance (the ones highlighted in red in Table 13);
- Class B: medium importance (the one highlighted in yellow in Table 13);
- Class A: high importance (the ones highlighted in green in Table 13).

The results obtained are summarized in Table 13.

Table 13: Prioritization of activities and functionalities

FUNCTIONALITIES/ACTIVITIES	CAPABILITIES													
	Access Control and Identity Verification	Cybersecurity	Logistics and Transportation Services	Community Resilience Building	Interdiction and Disruption	Risk Assessment	Supply Chain Integrity and Security	Information Sharing	Operational Coordination	Public Information and Warning	Planning	Threat and Hazards Identification	Environment Protection Services	Human Protection Services
Communication	5	5	5	5	3	3	4	5	5	5	3	4	5	5
Geographical Visualization	4	5	4	4	4,5	3,5	4	3	4,5	3	3	4,5	4,5	2,5
Alerting/Warning	5	3,5	4	5	4,5	3	4	3	4	5	2,5	4	4,5	5
Training/Exercising	4,5	4	5	4	3,5	3	4	4	5	4	4	4	5	4
Planning	4	5	5	4,5	4	4	5	4	4,5	3,5	5	4,5	4,5	4
Coordination	5	5	5	5	4	3,5	5	5	5	4,5	5	5	5	5
Risk Assessment	4	4	3	4,5	5	5	4,5	3,5	3	3	4	4	4	4
Knowledge Management	3	3,5	4,5	3,5	4	5	4,5	4,5	4	4	4,5	4	4,5	4
Decision Support	3	4	3,5	4	3,5	4	4	3,5	4	3,5	4	3,5	4,5	4
Expert Involvement	4	4	4	5	5	5	4,5	3	4	4	4	5	4,5	5
Surge Management	3	4	3	4	3	3	3	2,5	3,5	3	3	3	4,5	3
Monitoring	5	4	3	4,5	4,5	3,5	4	3,5	4	4	3	4	4	5
Brainstorming/ Lessons Learned	4	4	4	4	4	3,5	4	3	3,5	3	4,5	4	4	4

6. Prioritization and assessment of GPs

Starting from the results of the questionnaire, which allowed to assess the importance of an activity or a functionality in supporting a specific EM capability, several analyses were carried out.

Firstly, the analysis of **EM Capabilities covered by each GP** was performed by combing the values of Table 13 with the *Activities and Functionalities of GPs* framework. In particular, for each GP, the scores associated with activities/functionalities were multiplied by the scores attributed by experts related to the importance of that activity/functionality in determining an EM capability. This resulted in the development of a table, for each GP, like the one reported below (Table 9), where the value of each cell corresponds to:

*Score of Functionality$_i$ of the GP under investigation * Score of Functionality$_i$ to guarantee Capability$_j$.*

Finally, for each capability, the maximum value was selected in order to obtain the final score which links the practice with the single EM capabilities. A range of colors was then adopted, from red (low score) to green (high score), to show the level of coverage of the different capabilities that the GP under investigation should guarantee.

Table 14 shows an example of this procedure for a GP, particularly a Tool, included in the classification framework.

Table 14: Example of the procedure for a generic GP included in the framework

	GP under investigation	CAPABILITIES													
		Access Control and Identity Verification	Cybersecurity	Logistics and Transportation Services	Community Resilience Building	Interdiction and Disruption	Risk Assessment	Supply Chain Integrity and Security	Information Sharing	Operational Coordination	Public Information and Warning	Planning	Threat and Hazards Identification	Environment Protection Services	Human Protection Services
FUNCTIONALITIES/ACTIVITIES	Communication	25	25	25	25	15	15	20	25	25	25	15	20	25	25
	Geographical Visualization	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Alerting/Warning	25	17,5	20	25	22,5	15	20	15	20	25	12,5	20	22,5	25
	Training/Exercising	9	8	10	8	7	6	8	8	10	8	8	8	10	8
	Planning	12	15	15	13,5	12	12	15	12	13,5	10,5	15	13,5	13,5	12
	Coordination	25	25	25	25	20	17,5	25	25	25	22,5	25	25	25	25
	Risk Assessment	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Knowledge Management	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Decision Support	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Expert Involvement	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	MAX VALUE	**25**	**25**	**25**	**25**	**22,5**	**17,5**	**25**	**25**	**25**	**25**	**25**	**25**	**25**	**25**

This led to the development of a new *Emergency Management Capabilities* framework filled based on the results of the questionnaire. This allowed for the identification of capabilities that a GP should cover with a high level of importance according to experts' judgement, given the activities or functionalities supported by the practice itself.

The comparison between this new framework and the one completed using the information collected from scientific literature, project deliverables and institutional websites, enabled the identification of the gap between the two worlds. The gap points at the capabilities that could be further extended, since the practice is already endowed with functionalities/activities that could support them (Figure 4). In this regard, the different GPs were analysed in order to verify if the potential for improvement revealed by experts' judgement was feasible in a real context of application or if there were some limitations in the coverage of specific capabilities.

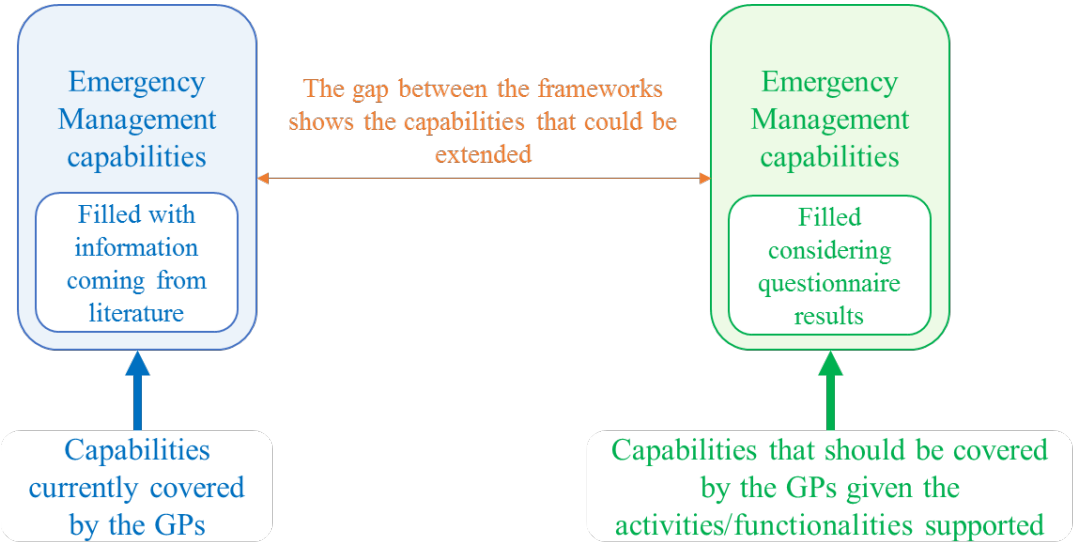

Figure 4. EM capabilities covered by GPs

In light of the previous considerations, the research proceeded with an analysis of the different GPs, which revealed which instruments or methodologies are needed to cover a specific capability. This enabled investigation of how the GPs with a potential for improvement may be further developed, thus aligning the capabilities actually covered with the ones resulting from the questionnaire. Therefore, the analysis conducted for each GP highlighted the capabilities currently covered, but also the instruments or methodologies that may be used to improve the EM.

The most interesting findings resulting from this analysis were:

- GPs belonging to the *Information sharing* cluster include instruments and approaches aimed mainly at enabling information sharing among different institutions and operators. It resulted that these GPs could contribute to community resilience-building by introducing instruments accessible by citizens, thus involving them in the sharing of information with operators. Moreover, it emerged the importance of adopting these practices involving all the actors of the supply chain in order to guarantee its integrity and security.
- GPs belonging to the *Geographical visualization and information sharing* cluster include instruments aimed mainly at enabling information sharing among institutions and operators and at detecting interdictions and disruptions. The study showed that these practices could facilitate the coordination of response operations by integrating their current map visualization tools with

instruments able to support resource deployment during emergencies. Another extension that may be adopted by these GPs concerns the possibility to represent on the maps the location of potential threats and hazards. A further contribution coming from experts' judgements highlighted the importance of involving the community in the resilience-building process and warning citizens in case of threats or emergencies to provide guidelines and support. However, the effective possibility of involving the community depends on the specific purpose of the different practices; indeed, if on the one hand there are GPs developed to support citizens in dealing with emergencies, on the other hand there are others specifically developed to be used by CI experts and operators.

- GPs belonging to the *Planning* cluster include instructions aimed mainly at guiding the development of plans and at providing methodologies for a prompt identification of threat and hazards. It emerged that these practices should guarantee the integrity and security of the supply chain by fostering collaboration among actors and developing common strategies.
- GPs belonging to the *Training, exercises and simulations* cluster include platforms and training programs aimed mainly at supporting planning. This cluster can be better discussed by introducing a distinction between workshops and simulation platforms. The former could support community resilience-building by involving citizens in the discussions, thus having the opportunity to develop better integrated solutions in line with the expectations and the needs of the whole community. Moreover, besides the identification of threats and hazards, these GPs might be extended by introducing an evaluation of the risk level of the area. Concerning simulations platforms, instead, the results of the questionnaire highlighted the importance of supporting operational coordination. In this regard, it could be possible to extend the usage of these tools also throughout an emergency event, by performing real-time simulations to support the resource deployment during the response phase.
- GPs belonging to the *Risk/Resilience assessment* cluster include instruments and templates aimed mainly at identifying threat and hazards and assessing risk or resilience. In some cases, the GPs provide instructions to develop strategic planning starting from the risk or resilience scores obtained.
- GPs belonging to the *Business Continuity Management* cluster include steps and activities aimed mainly at supporting planning activities, in order to avoid the suspension of critical systems or recover them as soon as possible in case of interruption.

The research proceeded with the **Assessment of a single Good Practice**, the analysis related to the degree of comprehensiveness of the GPs, which corresponds to the range of capabilities covered. The purpose was to assess if a GP is able to cover different capabilities homogeneously, or if it focuses on a narrow range. It means: the higher the range of capabilities covered by a GP - the higher is the degree of its comprehensiveness. This enabled to make a comparison between the percentage of capabilities covered according to literature and the percentage of capabilities covered according to experts' judgement. The difference between these two values allowed to identify, for each cluster, the GPs with the highest potential for improvement and to discuss how they could expand, considering also the possible limitations of the practice extension in a real context of application.

The final objective of the study was to achieve an **Overall mapping and prioritization of Good Practices**. In this regard, the degree of comprehensiveness based on the study of literature enabled to recognize, for each cluster, the Best Practices, namely the GPs which currently cover the widest

spectrum of EM capabilities. The most interesting findings resulting from this analysis were:

- V-BEOC and SATool are the Best Practices within the *Information sharing* cluster. Both are web-based platforms with a unique source of information enabling real-time communication among public and private institutions. Information sharing is guaranteed before, during and after an emergency, in order to collect inputs to support decision-making in all the phases of the EM cycle. Meetings and conferences organized by partners allow developing a common and integrated strategic planning, while the constant operating status updates provide a complete situational awareness. These platforms are endowed with components useful to manage resource deployment during emergencies and are publicly accessible to warn and inform the community.
- CRAMSS is the Best Practice within the *Geographical visualization and information sharing* cluster, followed by ESSMA and Cruscotto Emergenze. They all provide a georeferenced visualization of strategic places, resources and possible dangerous situations. This supports a promptly identification of emergencies, thus giving the possibility to intervene immediately in the affected area. Cruscotto Emergenze, differently from ESSMA and CRAMSS, allows identification of threats and hazards. Since it is applied to the management of different types of emergency events, it is focused not only on the protection of humans, but also on the protection of the environment. ESSMA and CRAMSS, instead, are applications available also for the public, therefore they are able to warn citizens and to support them in dealing with emergencies. Moreover, they provide instructions and guidelines to the operators that have to intervene in the affected area, showing the routings to reach the location and suggesting evacuation procedures to be followed.
- Public Safety Canada is the Best Practice within the *Planning* cluster, followed by Partnership Alignment for Enhanced Security. Both provide a set of guidelines to develop strategic plans, in the first case to manage insider risks that could affect CI systems, while in the second one to guarantee alignment among partners in the management of different types of risk.
- MICC and GINOM are the Best Practices within the *Training, exercising and simulations* cluster. The first one is a program which gathers CI operators and the community with the aim of training and exercising them to be prepared to manage an emergency, whilst the second one is a simulation platform fed by real-time data which provides decision support during crises. Data collected during simulations and exercises support the development and the testing of procedures and plans.
- DOMINO and Smart Resilience Indicators are the Best Practices within the *Risk/Resilience assessment* cluster. DOMINO is a tool based on a cartography approach used to locate system infrastructures and simulate domino effects; by analysing situational information of CIs, it assigns a risk level to the different areas that could be impacted by the emergency event. Smart Resilience Indicators, instead, includes a set of indicators suitable for assessing the resilience of Smart CIs, developing a new advanced resilience assessment methodology; based on the type of system considered, this tool suggests the most important indicators that institutions have to focus on in order to increase their resilience levels.

From the previous analyses it emerged that none of the GPs is able to cover all the capabilities for an effective EM. For this reason, the study proceeded with the identification of an **optimal bundle** composed by the minimum number of GPs that, combined together, are able to cover all the EM capabilities. Starting from the *Emergency Management Capabilities* framework filled with the information coming from the study of literature, the practices belonging to the bundle were selected with the support of the Excel Solver, by setting an objective function able to minimize the number of

GPs and by adding constraints implying that the scores assigned to the capabilities were at least equal or higher than 3 (out of a maximum of 5). To summarize, the optimization problem is:

$$Xi = EMCapabilityScore \qquad i = [1,2, \dots 14]$$

$$Yj = GP \begin{cases} 0 \\ 1 \end{cases} \qquad j = [1,2, \dots 53]$$

$$min \sum_{1}^{53} Yj$$

Subject to: $max(Xi * Yj) \geq 3 \qquad \forall i$

The results obtained are summarized in Table 15, which shows the four GPs belonging to the optimal bundle and the capabilities they are able to cover respecting the requirements imposed.

Table 15: GPs belonging to the optimal bundle

	CAPABILITIES													
	Access Control and Identity Verification	Cybersecurity	Logistics and Transportation Services	Community Resilience Building	Interdiction and Disruption	Risk Assessment	Supply Chain Integrity and Security	Information Sharing	Operational Coordination	Public Information and Warning	Planning	Threat and Hazards Identification	Environment Protection Services	Human Protection Services
V-BEOC	5	0	4	0	5	0	0	5	5	5	3	0	5	3
SATool	5	3	0	0	5	0	0	5	5	5	3	0	5	3
CRAMSS	5	0	0	5	5	2	0	5	5	5	0	4	0	5
PRISM	0	0	0	0	0	5	3	0	0	0	5	2	0	0

It resulted that V-BEOC, SATool, CRAMSS and PRISM are the practices that allow covering all the EM capabilities with a score higher than three. V-BEOC and SATool belong to the *Information sharing* cluster, CRAMSS to the *Geographical visualization and information sharing* cluster, while PRISM to the *Planning* one. The fact that these GPs come from different clusters indicates that the subdivision in groups according to the main functionality facilitates the selection of a bundle able to cover all the capabilities of the EM.

To better understand how each GP contributes to effective management of emergencies, a brief description of each of them is provided below.

V-BEOC is a web-based information sharing platform of the National Business Emergency Operations Center (NBEOC) that facilitates collaboration and coordination between public and private institutions, providing greater visibility of impacts and strengthening resilience of local communities. It was created to enhance communication among partners that can share information on impacts, operating status and recovery challenges, as well as information to support business continuity decisions and integration into planning, training and exercises. The main instruments

included in V-BEOC are: a Dashboard that provides real-time information on the latest incident updates, preparedness messaging and response and recovery resources; a Service Desk that allows NBEOC members to communicate, share status updates, track requests for information and meetings and submit offers; a Businesses Preparedness module that provides tools and resources for business preparedness; a Training webpage that provides an overview of emergency management training programs and opportunities available. Moreover, among its activities, NBEOC is charged with supporting local companies within the disaster area providing goods and services, performing disaster response and recovery work, procuring transportation needs and providing temporary lodging assistance to disaster evacuees.

SATool is an online Situation Center that provides operators with a centralized portal to communicate during critical events and share day to day information. The aim is to strengthen the region's collective capacity to prevent, respond to and recover from disasters through effective public-private collaboration and communication. Moreover, it allows to mitigate the impact of catastrophic events and ensure the safety of citizens and the resilience of the economy. It is integrated with social media therefore it enables to post video feeds, blogs and tweets, and it can host documents, message boards and chat groups. The tool includes also a voluntary registry of private sector business resources (e.g. trucks, equipment, skilled personnel and power) that can be called upon by emergency management organizations during disasters. SATool is part of a long-term strategy that leads partners to enhance their capabilities in the five mission areas of prevention, protection, mitigation, response and recovery, as well as the four additional functional areas of training and exercise, planning, cybersecurity and preparedness through an integrated and actionable plan.

CRAMSS is an application whose purpose is to support reference stakeholders of the Urban Transport System (UTS), such as infrastructure managers, in their choices also during emergency conditions. It integrates information from different sources (e.g. data management layer, application framework, actuation channels), providing decision support services and information to Urban Transport authorities via the front-end applications, thus facilitating efficient management of the UTS and real-time applicable countermeasures in critical situations (e.g. evacuation planning). The system can be adapted to real-time according to the needs of each emergent event; for instance, it excludes a particular road from the calculation of the evacuation routings, in order to avoid possible congestions in the affected road. Data collected from the city's sensors and the ones retrieved by the application framework are used to perform a real-time risk assessment and, once an emergency event is detected, CRAMSS identifies individuals as rescuers or to-be-rescued. It proceeds by alerting the operators about the event, supporting them in the definition of the areas that have to be evacuated and providing useful information about the location of users that have to be rescued. Moreover, it allows communicating with those users providing guidance to exit the hazardous areas.

PRISM is a modular risk management tool composed of four phases. It was designed to support the user in the implementation of the risk management process related to CIs, providing guidance notes and templates for each step that has to be undertaken. The first step, Strategy & Planning, is aimed at characterizing the external and organizational environment that influences the security of the assets. The plan can be developed after identifying, for each organizational area, possible issues with the correspondent impacts and after prioritizing the main stakeholders involved. The second step, Risk Assessment, determines the type, nature and severity of risks, following an all-risks approach (i.e. terrorism, natural, consequential and accidental hazards). The identification of the most critical assets,

their critical points and their external interdependences allow to rank assets based on their criticality level, considering specific parameters. The different risk scenarios are ranked based on the consequences they have on the asset and, if necessary, the mitigation actions are planned taking into account the protection objectives fixed by the organization. Those ones can be taken forward into the third phase of Design, where the requirements of the security system are established, leveraging on physical security, process control and IT security, procedural security and personnel security. Finally, the fourth phase, Implementation & Review, focuses on good principles of performance auditing, monitoring and reporting. Once PRISM is embedded, it can be updated and can evolve as an organization evolves and grows. In addition, it can also be applied to a supply chain, addressing interdependencies as they are identified in the second phase.

In line with the previous considerations, the identified bundle allows to cover all the EM capabilities in the following way:

- Access control and identity verification is covered by V-BEOC, SaTool and CRAMSS since all these GPs are platforms that require an authentication procedure.
- Cybersecurity is guaranteed by SaTool since it includes procedural guidelines to be protected from cyber-attacks.
- Logistics and transportation services are covered by V-BEOC. Indeed, it is used also to support response and recovery works in the affected area.
- Community Resilience building is supported by CRAMSS. Indeed, in the response phase, citizens can communicate and collaborate with operators through the app.
- Interdiction and disruption is covered by V-BEOC, SaTool and CRAMSS since they are all able to detect real-time emergencies through the monitoring of the territory, supported by the sharing of situational information or by data collection through sensors.
- Risk assessment is supported by PRISM. Indeed, it includes guidelines to support organizations in the definition of a strategy to incorporate risk management, in the assessment of risks and in the design of mitigation strategies.
- Supply chain integrity and security is covered by PRISM since it includes guidelines to manage risk at a supply chain level.
- Information sharing is covered by V-BEOC, SaTool and CRAMSS through a platform used to communicate and post real-time situational information.
- Operational coordination is covered by V-BEOC, SaTool and CRAMSS supporting a real-time deployment of resources during the response phase.
- Public information and warning is covered by V-BEOC, SaTool and CRAMSS since the platforms are accessible by the community and enable to inform citizens about the emergency events in progress.
- Planning is covered by V-BEOC, SaTool and PRISM. Indeed, through V-BEOC and SaTool, operators can exchange information and use it for planning activities, while PRISM includes guidelines useful to develop a strategic plan for risk management.
- Threats and Hazards identification is covered by CRAMSS. Indeed, the real-time data collected are used by CRAMSS components to evaluate the level of risk and warn operators about the emerging threats.
- Environment protection services are covered by V-BEOC and SaTool that work in the phase of recovery to re-establish the initial conditions of the environment.

- Human protection services are covered by V-BEOC, SaTool and CRAMSS which intervene in the first response to make rescue operations.

7. Conclusions

This research had the objective of developing a comprehensive classification framework composed by consistent and generalizable dimensions which allow an efficient comparison among GPs considering their main dimensions and applicability, the functionalities and activities supported, and the EM capabilities covered. Within this framework, the GPs were grouped by clusters, thus making a subdivision which considers the main functionality covered. The submission of the Critical Infrastructure Resilience Questionnaire to CI experts enabled to link the activities/functionalities to the capabilities that they can support. The results of the questionnaire allowed to make a comparison among the EM capabilities that should be covered given the activities or functionalities supported by a GP, and the ones that are actually covered in a real context. In particular, the analysis enabled to understand the ability of a GP to homogeneously cover the different capabilities and the possible limitations of a GP in the coverage of a specific capability in a real context.

Practitioners can use the comprehensive framework of classification to efficiently compare GPs and select the most suitable ones according to the context of application and the requirements that have to be respected. Indeed, the dimensions introduced in the integrated framework are intended to classify the GPs according to the most relevant needs of CI experts in a real context, thus supporting their selection. In this regard, the main contribution is given by the *Emergency Management capabilities* framework which allows practitioners to select the Best Practices, given the range of capabilities covered. From the analyses carried out, it is possible not only to identify the Best Practices but also to understand the potential for improvements of each GP already in place, thus enabling an expansion of the current practice taking the best ones as a reference. The identification of the different clusters in order to group the GPs has proven to be effective. Indeed, considering the composition of the optimal bundle, in order to cover all the capabilities with the lowest number of GPs, it was necessary to gather practices coming from different clusters. Finally, the generalizable dimensions of the GPs adopted in the frameworks can support practitioners in the understanding of the GPs determinants, enabling exploitation of synergies to cover effectively all the capabilities of the EM cycle. Besides this, practitioners can exploit the results coming from the *Aggregate Matrix*, which provides a link between the different activities and functionalities considered in the study. In particular, this matrix shows the functionalities that must be embedded in a tool in order to support a particular activity; therefore, given a set of activities, the matrix can guide the selection of the most suitable tool in order to support all of them.

Concerning the limits that need to be considered for further improvements of the work, most of them are coming from the questionnaire submission. Indeed, the number of feedbacks received was limited due to time constraints, and involving a higher number of CI experts could have guaranteed a greater consistency of the research. Moreover, an issue stressed by one of the experts was the lack of an orthogonal taxonomy between the activities/functionalities and the EM capabilities.

In order to solve these limitations and increase the consistency of the results, the research could proceed by submitting the questionnaire to a higher number of CI experts. Finally, a further improvement to the comprehensive classification framework can be to group the EM capabilities according to the respective phases of the EM, as suggested by an expert through the questionnaire. In this way, by associating the capabilities to a GP, it is also possible to verify the EM phases covered, thus developing a direct link between the first and the third frameworks.

References

Abou El Kalam, A., Deswarte, Y., Baïna, A., & Kaâniche, M. (2009). PolyOrBAC: A security framework for Critical Infrastructures. *Int. J. of Critical Infrastructure Protection*, *2*(4), 154-169.

Adini, B., Cohen, O., Eide, A. W., Nilsson, S., Aharonson-Daniel, L., & Herrera, I. A. (2017). Striving to be resilient: What concepts, approaches and practices should be incorporated in resilience management guidelines?. *Technological Forecasting and Social Change*, *121*, 39-49.

Cambridge Dictionary (online) https://dictionary.cambridge.org/dictionary/english/functionality

Cambridge Dictionary (online) https://dictionary.cambridge.org/dictionary/english/warning

Cambridge Dictionary (online) https://dictionary.cambridge.org/us/dictionary/english/activity

CCOHS (2020). OSH Answers Fact Sheets https://www.ccohs.ca/oshanswers/hsprograms/risk_assessment.html

European Commission, DIRECTIVE 2008/114/EC, article 2a, 2008.

FEMA (2020) Core Capabilities. https://www.fema.gov/core-capabilities

FEMA (2020) Emergency Management in the United States. https://training.fema.gov/emiweb/downloads/is111_unit%204.pdf

Hollnagel, E. (2015). Disaster management, control, and resilience. In *Disaster management: Enabling resilience* (pp. 21-36). Springer, Cham.

ISO 22325 (2016)

MacEachren, A. M., & Kraak, M. J. (1997). Exploratory cartographic visualization: advancing the agenda.

NIMSAT Institute (2020) Next Generation Business Emergency Operations Center (Next Gen BEOC). https://nimsat.louisiana.edu/resources/virtual-business-emergency-operations-center

Shannon, C. E. (2001). A mathematical theory of communication. *ACM SIGMOBILE mobile computing and communications review*, *5*(1), 3-55.

Skolimowska A, (2013), “Interdependence of Critical Infrastructure”.

Tinmannsvik, R. K., Albrechtsen, E., Bråtveit, M., Carlsen, I. M., Fylling, I. M., Hauge, S., ... & Øien, K. (2011). Deepwater Horizon-ulykken: Årsaker, lærepunkter og forbedrings-tiltak for norsk sokkel. *SINTEF report A*, *19148*.

Trucco, P., Petrenj, B., (2015), “MIRACLE Project Deliverable 2.2”.

Trucco, P., Petrenj, B., (2015), “MIRACLE Project Deliverable 2.3”.

Trucco, P., Petrenj, B., Di Mauro, C., (2018), “Resilience capacities assessment for Critical Infrastructures disruption: READ pilot applications (part 2)”, Int. J. Crit. Infrastructures 14, 221.

U.S. President′s Commission on Critical Infrastructure Protection (PCCIP), (1997), “Critical Foundations: Protecting America’s Infrastructures” report.

Wróbel, R. (2019). Dependencies of elements recognized as critical infrastructure of the state. *Transportation Research Procedia*, *40*, 1625-1632.

Table 16: GPs included in the analysis

GPs list		
GP name	**Developer Organization**	**References**
V-BEOC (Virtual Business Emergency Operations Center)	Louisiana Business Emergency Operations Center	Next Generation Business Emergency Operations Center (Next Gen BEOC) | National Incident Management Systems & Advanced Technologies (louisiana.edu)
NWWARN (Northwest Warning, Alert and Response Network)	Pacific Northwest Economic Region	Home (regionalresilience.org)
DARWIN Wiki	DARWIN project, by European Union	DARWIN-Project-Concluding-Paper.pdf (h2020darwin.eu)
Focus on Flows	Swedish Resilient Regions Association	ENGLISH - Resilient Regions
MATRICS (Multi Actor Threat Recognition, Information and Collaboration System)	Astir in collaboration with Polytechnic of Milan	Astir Progetto: Matrics - Astir S.R.L.
SATool (Situational Awareness Tool)	Colorado Emergency Preparedness Partnership	Colorado Emergency Preparedness Partnership - CEPP's Mission and Projects (thecepp.org)
Resilience Building Policies	Smart Mature Resilience Project, by European Union.	SMR :: SMR (smr-project.eu)
Multi-State Fleet Response Initiative	Multi-State Fleet Response Working Group	https://www.ahcusa.org/fleet-response.html
Big Business – Small Business	Louisiana Business Emergency Operations Center	Hazards risk mgmt - session 10 - handout - nimstat iaem press release.pdf (fema.gov)
Louisiana Disaster Recovery Alliance	Agencies of the State of Louisiana and federal government agencies	Louisiana Disaster Recovery Alliance (louisianarecoveryalliance.org)
Cruscotto Emergenze	Lombardy Region	Cruscotto emergenze (servizirl.it)
Copernicus Emergency Management Service	European Commission	Copernicus Emergency Management Service
GIS Mapping for CI Assets	Scottish Government with Scottish CI operators	Trucco, P., Petrenj, B., (2015), "Miracle Deliverable 2.2"; Abdalla et Al., (2017), "Web-Based Geographical Information System for Urban Emergency Management Decision-Making Support"
Resilience Information and Communication Portal	Smart Mature Resilience Project, by European Union	SMR :: SMR (smr-project.eu)
Traffic Scotland Information Service	Transport Scotland	Traffic Scotland > Media
ESSMA (Emergency Support Smart Mobile App)	RESOLUTE project, by European Union	RESOLUTE D5.4 Mobile-Emergency-Support-App-v6-1.pdf (resolute-eu.org)
CRAMSS (Collaborative Resilience Assessment and Management Support System)	RESOLUTE project, by European Union	RESOLUTE D5.3 CRAMSS application_v9-1-1.pdf (resolute-eu.org)

PRISM (Performance and Risk-based Integrated Security Methodology)	Harnser Risk Group	The_Financial_Aspects_of_the_Security_of_Assets_and_Infrastructure_in_the_Energy_Sector.pdf (ab.gov.tr)
COLAB	100 Resilient Cities	http://www.100resilientcities.org/
TTF (Thematic Task Forces)	Lombardy Region	Microsoft Word - Sintesi (regione.lombardia.it)
Partnership Alignment for Enhanced Security	Netherlands Safety regions	Trucco, P., Petrenj, B., (2015), "Miracle Deliverable 2.2"
European Resilience Management Guideline	Smart Mature Resilience Project, by European Union	SMR-EMRG-handbook-WWW-compressed.pdf (smr-project.eu)
Public Safety Canada	Public Safety and Emergency Preparedness Canada	Enhancing Canada's Critical Infrastructure Resilience to Insider Risk (publicsafety.gc.ca)
Blue Cascades Exercise Series	Pacific Northwest Economic Region	blue_cascades_vii_final_report.pdf (regionalresilience.org)
MICC (Major Incident Control Committee)	Operators within the Grangemouth industrial complex area	MICC – MICC Grangemouth Community (ineos.com)
CATEX (Catastrophic Exercise)	All Hazards Consortium	CATEX 2017 Exercise (ahcusa.org) VEM 2019 Statewide Catastrophic Recovery Exercise | Vermont League of Cities and Towns (vlct.org)
City Resilience Dynamics	Smart Mature Resilience Project, by European Union	SMR :: Tools (smr-project.eu)
SimEnv	DARWIN project, by European Union	DARWIN-Project-Concluding-Paper.pdf (h2020darwin.eu)
Serious Games based on Virtual Reality	DARWIN project, by European Union	DARWIN-Project-Concluding-Paper.pdf (h2020darwin.eu)
GINOM (Global Infrastructure Network Optimization Model)	Electric Infrastructure Security council	EIS Council, (2020), "GINOM The Global Infrastructure Network Optimization Model"; EIS Council, (2020), "The GINOM Simulation"
Opportunity Assessment Tool	100 Resilient Cities	http://www.100resilientcities.org/
Problem Framing	100 Resilient Cities and Citymart	http://www.100resilientcities.org/
Project Scan Tool	100 Resilient Cities and Resilient Rotterdam team	http://www.100resilientcities.org/
Resilience Accelerator	100 Resilient Cities and Center for Resilient Cities and Landscapes at Columbia University	http://www.100resilientcities.org/
Resilience Garage	100 Resilient Cities	http://www.100resilientcities.org/
Resilience Value Realization	Rockefeller Foundation	http://www.100resilientcities.org/
100 RC Systems Studio	100 Resilient Cities	http://www.100resilientcities.org/
Tactical Urban Resilience	100 Resilient Cities	http://www.100resilientcities.org/

DOMINO Tool	Centre Risque & Performance of École Polytechnique de Montréal	Trucco, P., Petrenj, B., (2015), "Miracle Deliverable 2.2"; Tilmann Gramß et Al., (2006), "Domino 7 Performance Tuning, Best Practices to Get the Most Out of Your Domino Infrastructure"
GRRASP (Geospatial Risk and Resilience Assessment Platform)	Joint Research Centre	Geospatial Risk and Resilience Assessment Platform | EU Science Hub (europa.eu) GRRASP-DMCI-manual.pdf (europa.eu)
Assets and Risk Tool	100 Resilient Cities	http://www.100resilientcities.org/
Local Area Risk Assessment	100 Resilient Cities and Next Practice Ltd.	http://www.100resilientcities.org/
Risk Systemicity Questionnaire	Smart Mature Resilience Project, by European Union	SMR :: Tools (smr-project.eu)
THREVI2	Biomedical Campus of Rome University	Critical Infrastructure | Risk & Resilience of Complex Systems (r2macs.com)
CI System Definition Tool	Resilens Project, by European Union	D2.3-Resilience-Management-Matrix-and-Audit-Toolkit.pdf (resilens.eu)
Resilience Management Matrix Tool	Resilens Project, by European Union	D2.3-Resilience-Management-Matrix-and-Audit-Toolkit.pdf (resilens.eu)
GIS based Resilience Mapping Tool	Resilens Project, by European Union	D2.3-Resilience-Management-Matrix-and-Audit-Toolkit.pdf (resilens.eu)
Resilience Management Audit Tool	Resilens Project, by European Union	D2.3-Resilience-Management-Matrix-and-Audit-Toolkit.pdf (resilens.eu)
City Resilience Index	100 Resilient and Arup	http://www.100resilientcities.org/
Smart Resilience Indicators	European Union	Periodic Reporting for period 2 - SmartResilience (Smart Resilience Indicators for Smart Critical Infrastructures) | Report Summary | SmartResilience | H2020 | CORDIS | European Commission (europa.eu) Report on Challenges for SCIs | Zenodo
Resilience Maturity Model	Smart Mature Resilience Project, by European Union	SMR :: Tools (smr-project.eu)
Resilience Actions Inventory and Stakeholder Perceptions Review	100 Resilient and Arup	http://www.100resilientcities.org/
Business Continuity Management for enterprises	Cabinet Office, Government of Japan	Cabinet Office, Government of Japan, (2005), "Reducing the Impact of Disasters and Improving Responses to Disasters by Japanese Companies", Business Continuity Guidelines 1st ed.
Area Business Continuity Management	Japan International Cooperation Agency and Association of Southeast Asian Nations	Hitoshi Baba et Al., (2014), "Area Business Continuity Management, a new opportunity for building economic Resilience"