D3.1 Contextual factors related to resilience

Report Title:	*D3.1 Contextual factors related to resilience*		
Author(s):	M. Vollmer, G. Walther, A. Choudhary, A. Jovanovic, J. Gehrke, F. Brauner, J. Sanne, L. Bergfors		
Responsible Project Partner:	FhG-INT	Contributing Project Partners:	EU-VRi, IVL, BUW

Document data:	File name / Release:	SmartResilience_D3.1_v23bc31072017		Release No.: 3
	Pages:	67	No. of annexes:	2
	Status:	Final	Dissemination level:	Public
Project title:	**SmartResilience**: Smart Resilience Indicators for Smart Critical Infrastructures		Grant Agreement No.:	700621
			Project No.:	12135
WP title:	WP3. The SmartResilience indicator-based methodology for assessing, predicting & monitoring the resilience of SCIs for optimized multi-criteria decision-making		Deliverable No:	D3.1
Date:	Due date:	July 31, 2017	Submission date:	July 31, 2017
Keywords:	Contextual factors; legal acts; organizational requirements; ethical impacts			
Reviewed by:	Nils Albrecht		Review date:	July 12, 2017
	Dmitry Bezrukov		Review date:	July 17, 2017
Approved by Coordinator:	Aleksandar Jovanovic		Approval date:	July 31, 2017

Euskirchen, July 2017

© 2016-2019 This document and its content are the property of the SmartResilience Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the SmartResilience Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the SmartResilience Partners. Each SmartResilience Partner may use this document in conformity with the SmartResilience Consortium Grant Agreement provisions. The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under the Grant Agreement No 700621.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

Release History

Release No.	Date	Change
1	July 10, 2017	Draft version for internal review
2	July 24, 2017	Revised version for last changes by task partners
3	July 31, 2017	Final version

Project Contact

EU-VRi – European Virtual Institute for Integrated Risk Management
Haus der Wirtschaft, Willi-Bleicher-Straße 19, 70174 Stuttgart, Germany
Visiting/Mailing address: Lange Str. 54, 70174 Stuttgart, Germany
Tel: +49 711 410041 27, Fax: +49 711 410041 24 – www.eu-vri.eu – info@eu-vri.eu
Registered in Stuttgart, Germany under HRA 720578

SmartResilience Project

Modern critical infrastructures are becoming increasingly smarter (e.g. the smart cities). Making the infrastructures smarter usually means making them smarter in the normal operation and use: more adaptive, more intelligent etc. But will these smart critical infrastructures (SCIs) behave smartly and be smartly resilient also when exposed to extreme threats, such as extreme weather disasters or terrorist attacks? If making existing infrastructure smarter is achieved by making it more complex, would it also make it more vulnerable? Would this affect resilience of an SCI as its ability to anticipate, prepare for, adapt and withstand, respond to, and recover? What are the resilience indicators (RIs) which one has to look at?

These are the main questions tackled by SmartResilience project.

The project envisages answering the above questions in several steps (#1) By identifying existing indicators suitable for assessing resilience of SCIs (#2) By identifying new smart resilience indicators including those from Big Data (#3) By developing, a new advanced resilience assessment methodology based on smart RIs and the resilience indicators cube, including the resilience matrix (#4) By developing the interactive SCI Dashboard tool (#5) By applying the methodology/tools in 8 case studies, integrated under one virtual, smart-city-like, European case study. The SCIs considered (in 8 European countries!) deal with energy, transportation, health, and water.

This approach will allow benchmarking the best-practice solutions and identifying the early warnings, improving resilience of SCIs against new threats and cascading and ripple effects. The benefits/savings to be achieved by the project will be assessed by the reinsurance company participant. The consortium involves seven leading end-users/industries in the area, seven leading research organizations, supported by academia and lead by a dedicated European organization. External world leading resilience experts will be included in the Advisory Board.

Executive Summary

This report discusses contextual factors that need to be considered when conducting an indicator-based resilience assessment of smart critical infrastructures (SCIs). It includes legal issues, organizational requirements, as well as ethical considerations.

The analysis of context factors has been part of WP3 "The SmartResilience Indicator-based methodology for assessing, predicting & monitoring the resilience of SCIs for optimized multi-criteria decision making". It sets a frame, and provides information on possible constraints when applying the methodology. The target audience are operators of SCIs and associated stakeholders. Results documented in this report also feed into the guideline as developed in T3.6.

The legal factors firstly concern those that oblige stakeholders to assess resilience of SCIs, and/ or to maintain a certain level of resilience. One of the basic EU Directives is the "Directive 2008/114/EC – identification and designation of European critical infrastructures and assessment of the need to improve their protection". A transfer of relevant EU Directives into national law is exemplified using the fields of energy supply in Germany and drinking water supply in Sweden. Complementing these legal acts, selected support regarding their implementation, especially in terms of guidelines (on national level, plus e.g. ANSI/ API; OECD) is described.

The legal factors secondly concern those that can hinder (or support) an assessment of resilience and/ or measures to increase resilience. Main issue here is data protection. On EU level, the current legal framework of data protection is manifested in Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Member States have implemented it into national data protections laws. However, as a response to challenges from the digital age, a comprehensive reform of data protection rules in the EU will become active in May 2018. It comprises a Regulation (Regulation (EU) 2016/679 – protection of natural persons with regard to the processing of personal data and the free movement of such data) and a Directive (Directive (EU) 2016/680 – protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data).

Both the assessment of resilience and the implementation of measures to increase resilience can only be successful if certain organizational requirements are fulfilled. The identified factors can be classified into "staff/ work process"; "tools"; "cooperation"; and "others".

Finally, possible ethical impacts of indicator-based resilience assessment can be described by phases – the pre-research phase, research phase, and application phase. The examination of respective quality criteria (such as validity, reliability, objectivity, etc.) for each indicator provides a basis for the selection of indicators and their interpretation.

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
BDSG	"Bundesdatenschutzgesetz", German Federal Data Protection Act
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CCPS	Centre for Chemical Process Safety
GDPR	EU General Data Protection Regulation
MS	(EU) Member State
Mts	Meters
SCI	Smart Critical Infrastructure

1 Introduction

The development of an indicator-based resilience assessment method for smart critical infrastructures (SCIs) needs to take into account any contextual factors, e.g. legal issues, organizational requirements, and ethical considerations, in order to be successful. A lack of engagement with these issues may impede the eventual use of the indicators: they may not get used because laws prohibit necessary data acquisition; organizations are unable to use the indicators due to lack of personnel or because they are unable to translate the findings from the indicators into organizational changes, or the public actively works against the measures that are in place in order to collect data (e.g. resistance to surveillance cameras).

Regarding the question, in how far the resilience approach is reflected in the legal and regulatory regimes, it has been found that characteristics of resilience related to "persistence" are quite well addressed by legal systems, while others such as adaptability or transformation are not accounted for in many cases [11] [18]. One explanation for this limited inclusion is that many laws neither sufficiently consider local differences nor allow for reactions to changing circumstances [18]. This report provides an overview in chapter 2 on existing *legal acts that oblige stakeholders* to assess resilience and to maintain a certain level of resilience of SCI. In addition, it identifies supporting tools that assist stakeholders to fulfil their obligations. The deliverable has put a specific focus on two case studies: Energy infrastructure in Germany, and water supply in Sweden, since the number of legal documents and acts that pertain to a single SCI in a country is quite substantial. The amount and variety of supporting documents is even more extensive, thus, the section on guidelines and other support documentation lists the most relevant ones, which have been directly mentioned by stakeholders.

The report will not only provide a basis for the respective cases, but also serve as examples on how to investigate respective legal acts and supporting documents also for other SCI and for other countries.

Of course, *legal acts* do not only play a role in this context because they oblige stakeholders to address resilience. They can also *influence the success of actions to assess or to increase resilience* ("external influencing factors"). In this context, especially the data protection legal framework is important, which is summarized in chapter 3.

Chapter 4 then addresses the question of how *organizational preconditions* ("internal influencing factors"), such as available expertise, training, collaboration traditions, available tools, and others influence the success of resilience measures.

Finally, chapter 5 addresses the issue of ethics. Specifically, what are possible unintentional consequences that the development and use of indicators can have? And how can these issues be addressed beforehand and possible negative results mitigated?

The data in this report are based on desktop research, and consultations with experts and practitioners (SCI operators). The desktop research comprised internet research, but also a revision of related previous work in SmartResilience. For example, D1.3 "End users' needs and requirements" was used to complete the results on internal influencing factors. In addition, a workshop with practitioners (project internal & external) was held[1] to identify and discuss relevant issues, which was supplemented through surveys with practitioners.

The target audience of this report is operators of SCIs who may be unfamiliar with how to identify possible obligations with regard to resilience that they may have. The case studies can help the reader to understand

[1] SmartResilience workshop April 24-26, Budapest

what sort of regulations to look for in their respective countries. In addition, the chapter 4 on organizational setup and chapter 5 on ethics may raise awareness to some of the elements that may be overlooked when discussing resilience from a purely technical point of view. It thus assists in generating debate and highlighting potentially problematic developments early on. This might include highlighting simple issues, which can easily be changed with significant impacts on successful resilience assessments or actions to increase resilience. While some of the results of this deliverable are already available in abridged and adapted form in a first version of deliverable 3.6, which is the "Guideline for assessing, predicting and monitoring resilience of SCIs" (final version to be delivered May 2018), this deliverable provides more background information.

2 Legal acts and supporting tools to assess and ensure resilience

2.1 Legal acts on (S)CI resilience at EU-level

There are different types of legal acts at EU level, which differ on how legally binding they are. The EU describes these different types of legal acts on its official website[2] as follows:

Regulations

A "regulation" is a binding legislative act. It must be applied in its entirety across the EU. For example, when the EU wanted to make sure that there are common safeguards on goods imported from outside the EU, the Council adopted a regulation.

Directives

A "directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. One example is the EU consumer rights directive, which strengthens rights for consumers across the EU, for example by eliminating hidden charges and costs on the internet, and extending the period under which consumers can withdraw from a sales contract.

Decisions

A "decision" is binding on those to whom it is addressed (e.g. an EU country or an individual company) and is directly applicable. For example, the Commission issued a decision on the EU participating in the work of various counter-terrorism organisations. The decision related to these organisations only.

Recommendations

A "recommendation" is not binding. When the Commission issued a recommendation that EU countries' law authorities improve their use of videoconferencing to help judicial services work better across borders, this did not have any legal consequences. A recommendation allows the institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed.

Opinions

An "opinion" is an instrument that allows the institutions to make a statement in a non-binding fashion, in other words without imposing any legal obligation on those to whom it is addressed. An opinion is not binding. It can be issued by the main EU institutions (Commission, Council, Parliament), the Committee of the Regions and the European Economic and Social Committee. While laws are being made, the committees give opinions from their specific regional or economic and social viewpoint. For example, the Committee of the Regions issued an opinion on the clean air policy package for Europe. [38]

Mainly addressed in this report are the binding Regulations and Directives.

The EU's official website further provides summaries of EU legislation, enabling a quick insight into specific legal acts.[3]

[2] https://europa.eu/european-union/

[3] http://eur-lex.europa.eu/browse/summaries.html?locale=en

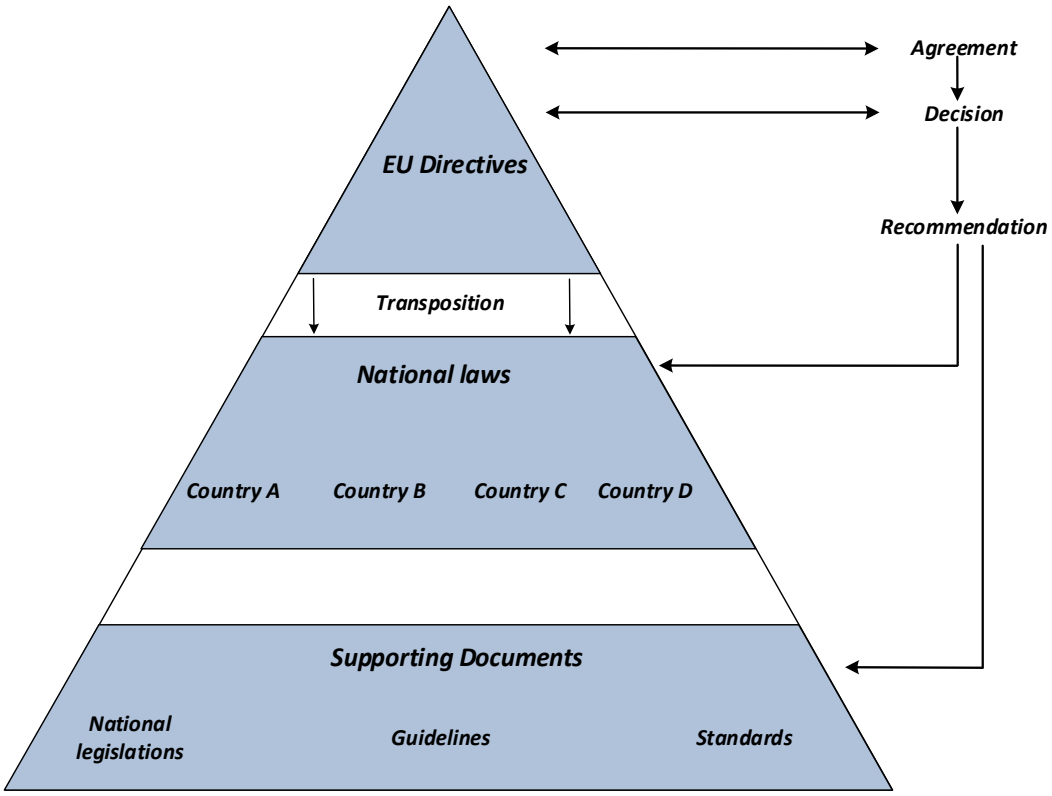

Figure 1: EU Directive transposition into National laws

Selected legal acts

The European Programme for European Critical Infrastructure Protection (EPCIP) provides an overall frame for critical infrastructure protection (energy, transportation, and finance) in the EU. It focuses on the identification and assessment of critical infrastructure in the EU (established in Directive 2008/114/EC, see below), the Critical Infrastructure Warning Information Network (CIWIN), the funding for over 100 critical infrastructure protection projects, as well as international cooperation [33].

In the following, some directives and regulations are described that seem most relevant for SmartResilience. (However, the list cannot be comprehensive.) Some additional directives, plus a list of documents that address relevant topics but that are not binding, or only to a small extent (see above), are listed in Annex 1.

Table 1 summarizes the identified relevant legal acts that are further described below.

Table 1: Overview selected legal acts on EU level obliging stakeholders to assess/ increase resilience

Legal act	Relevant because	CI stakeholders mainly affected	Link
Directive 2008/114/EC – identification and designation of European critical infrastructures and assessment of the need to improve their protection	Member States are requested to identify important assets of critical infrastructures; Requests conduction of risk analysis and threat scenarios; Counter-measures and procedures shall be identified, selected and prioritized.	From energy and transport sectors	http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114
Directive 2013/40/EU – on attacks against information systems	Aims to facilitate the prevention of offences in the area of attacks against information systems and therefore helps in keeping them resilient.	Decision and policy makers who are responsible for the establishment and operation of the national/governmental CERTs (Computer Emergency Response Teams), and the national/governmental CERTs themselves [39]	http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)	Entails a risk assessment plan to identify risks for security of networks and information systems: ‚security of networks' is defined as the ability of network and information systems to resist any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.	All operators of critical infrastructures	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment	Relevant for the "smart" component of the project. Requirements for operators with regard to security and notification are established.	From energy sector	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32005L0089
Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy (Water Framework Directive)	It directly addresses key tasks of water supply operators, and is also relevant for all other infrastructure operations that can affect water quality. Successive amendments have been incorporated in this Directive.	From water supply	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0060

Legal act	Relevant because	CI stakeholders mainly affected	Link
Directive 2007/60/EC *of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks.*	Entails a preliminary assessment of flood risks as well as a risk assessment to reduce consequences.	All operators of critical infrastructures prone to flood risks	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32007L0060
Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC (Seveso III Directive)	Operators using dangerous substances are required to take all necessary measures to prevent major accidents.	From Refinery sector and the ones dependent on it	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012L0018
Regulation (EU) No 994/2010 *concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC*	Aims to ensure both prevention and a coordinated response in the event of a supply disruption.	From natural gas supply	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32010R0994
Regulation (EC) No 300/2008 on common rules in the field of civil aviation security	Lays down rules and basic standards on aviation security.	From civil aviation sector	http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008R0300

Directive 2008/114/EC establishes a procedure for the identification and designation of European critical infrastructures ('ECIs'), and a common approach to the assessment of the need to improve the protection of these infrastructures, in order to contribute to the protection of people. The Directive applies to the energy and transport sectors. Member States (MSs) must regularly review the identification of ECIs, and each ECI has to have an "operator security plan" in place. MSs have to conduct threat assessments and report the types of risks, threats and vulnerabilities every 2 years. Thus, it constitutes one of the basic legal acts in the context of SmartResilience.

Directive 2013/40/EU – on attacks against information systems is relevant especially due to the "smart" character of CIs addressed in SmartResilience. It establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to tackle such offences and to improve cooperation between judicial and other relevant authorities. The Directive introduces new rules harmonizing criminalization and penalties for a number of offences directed against information systems. It also calls for EU countries to use the same contact points used by the Council of Europe and the G8 to react rapidly to threats involving advanced technology. The main types of criminal offences covered by this Directive are attacks against information systems, ranging from denial of service attacks designed to bring down a server to interception of data and botnet attacks.

Also *Directive (EU) 2016/1148* (NIS Directive) seems most relevant in the context of SmartResilience considering the "smart" component of the project. It prescribes measures to achieve a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. It also sets out obligations to all MSs to adopt a national strategy on these matters. The Directive creates a cooperation group as well as a computer security incident response network.

Requirements for operators with regard to security and notification are established. The Directive further lays down obligations for MSs to designate national authorities.

Directive 2005/89/EC aims to ensure the proper functioning of the EU internal market for electricity. It requests from the MSs to define policies on security of electricity supply compatible with the requirements of a competitive single market for electricity. They shall thereby amongst others ensure continuity of electricity supplies, and continuously renew transmission and distribution networks to maintain performance.

The EU Water Framework Directive (*Directive 2000/60/EC*) defines responsibilities for national authorities, who amongst others have to designate authorities to manage river basins in line with EU rules, and monitor their status including the impact of human activity and an economic assessment of water use. Water deterioration shall be prevented, and protected areas that require special attention shall be registered. Successive amendments to the Directive have been incorporated in the original document. This includes the Directive 2006/118/EC on the protection of groundwater against pollution and deterioration; the Directive 2007/60/EC on the assessment and management of flood risks; and the Directive 2008/105/EC on environmental quality standards in the field of water policy.

Directive 2007/60/EC establishes a framework for the assessment and management of flood risks, which aims to reduce their adverse consequences for human health, the environment, cultural heritage and economic activity within affected communities. It is thus relevant for all CIs that are prone to flood events. The Directive prescribes a three-step procedure consisting of a preliminary flood risk assessment, a risk assessment and flood risk management plans. The flood risk management plans are not formally binding but measures are proposed to manage the risks and focus on prevention, protection and preparedness.

The *Seveso III Directive 2012/18/EU* is based on a preventive principle that aims to anticipate possible (probable) negative effects from events involving dangerous substances and uses various instruments to avoid the occurrence of damage. It is achieved by focusing on ways to avoid transboundary pollution, prevent pollution at source, reduce environmental damage and reduce the risk of harm [26]. The Directive covers facilities where dangerous substances may be present (e.g. during processing or storage) in quantities above a certain threshold. Operators of the infrastructures are obliged to take all necessary measures to prevent major accidents and to limit their impact on human health and the environment. The requirements include [29]:

- Notification of all concerned establishments (Article 7);
- Deploying a major accident prevention policy (Article 8);
- Gathering information about the domino effects (Article 9);
- Producing a safety report for upper tier establishments (Article 10). This article specifically, focuses on indicators for monitoring performance;
- Producing internal emergency plans for upper tier establishments (Article 12);
- Providing information in case of accidents (Article 16).

Regulation (EU) No 994/2010 aims to ensure both prevention and a coordinated response in the event of a gas supply disruption, and to secure the proper and continuous functioning of the internal gas market. The regulation provides common standards at EU level. These standards state amongst others that in case of the event of a disruption of the single largest infrastructure, MSs must be able to satisfy total gas demand during a day of exceptional high gas demand. Further, risk assessment and respective preventive action- and emergency plans are requested.

Regulation (EC) No 300/2008 lays down common rules and basic standards on aviation security and on procedures to monitor their implementation. It applies to all civil airports in the EU, as well as to air carriers and entities providing goods or services to or through these airports. It includes obligation for both Member States and on airports and operators. The latter are obliged to define and implement a security programme, and to ensure internal quality control. Successive amendments to the Regulation have been incorporated in the original document. This includes the Commission Regulation (EU) No 72/2010 laying down procedures for conducting Commission inspections in the field of aviation security; the Commission Regulation (EU) No 1254/2009 setting criteria to allow Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures; the Commission Regulation (EC) No 272/2009

supplementing the common basic standards on civil aviation security; and the Commission Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security.

2.2 Case study: Energy supply in Germany

This chapter analyses the current situation of the energy infrastructure in Germany with regard to what sort of regulations, guidelines, and support institutions pertain to resilience initiatives. Of course, this case study is necessarily dependent on the general political, legal and technological landscape in Germany. Yet, this overview might nevertheless be pertinent to other countries as it shows what actors are generally involved in securing energy infrastructure resilience. A similar analysis in other countries can thus draw on these insights and help in the early identification of relevant sources. In addition, the topical focus on the energy is interesting as it will highlight how elements of security and safety are intertwined in efforts to increase resilience. The chapter thus pays particular attention to safety regulations and supporting documentation and institutions.

The chapter is divided into two subsections. The first will discuss relevant laws and regulations whereas the second provides an overview of national and international guidelines and organizations that directly address resilience of energy infrastructure.

While this chapter focuses specifically on the energy infrastructure sector, a short discussion of overall critical infrastructure protection in Germany may prove useful. At the most general level, the national strategy for the protection of critical infrastructure ("KRITIS-Strategie") [8] defines the goals and lays out the strategy for any policies at the federal level. Its guiding principles are a close cooperation between government and industry based on mutual trust. In addition, all efforts should be based on how appropriate and commensurable they are with regard to possible threats and the level of necessary protection. The overall goal is to increase protection by working towards *prevention*, *reaction*, and *sustainability*: All operators of (S)CI are to work on preventing any disruption of their services. These efforts are to include protection in combination with risk and crisis management, all of which shall be subject to continuous training. The response to any disruption should be strengthened by reducing any downtime of the infrastructure. All of the processes and improvements are to be revised continuously and lessons learned from disruptions of infrastructures in other countries included in these revisions. In addition, international efforts should be coordinated by developing common standards.

In 2005, the federal government had already issued a basic guideline for critical infrastructure protection [6]. This publication analyses potential threats to (S)CIs and recommends structural, organizational, personal and technical protections, e.g. how to protect vulnerable areas against intrusions, how to conduct physical access controls, or how to improve crisis management communication. In 2009, and revised in 2011, the government also provided a guideline for operators of CIs on how to conduct risk and crisis management [9]. Given the prominent role and potential vulnerability of IT-systems, the government has also issued specific guidelines for this issue. A publication from 2007 details how to implement the national plan for IT protection for critical infrastructures [7]. This plan initially involved the active cooperation of about 30 companies, which has subsequently increased to more than 150 companies and organizations. The results of this cooperation between government and industry can be found online where companies can also register to participate in the programme [14].

2.2.1 Legal acts

Germany is a Federal Republic, which has legislation on both the federal as well as on state (*Länder*) level. The German constitution, the Basic Law, defines which thematic areas fall under the competence of the national, and which of the state legislation.

Highest legal acts following the constitution are federal laws ("Bundesgesetze"). These are followed by legal decrees ("Rechtsverordnungen"), statutes ("Satzungen"), and general administrative provisions ("allgemeine Verwaltungsvorschriften"). Accordingly, these different levels of legal acts exist within the individual states as well. From the safety perspective, in Germany each state implements its own regulations. Furthermore, each organization implements the procedures which are rooted in technical guidelines outlined in chapter 2.2.2.1

to ensure safety of the infrastructure. Table 2 provides an overview of the relevant laws and regulations, which are discussed in detail below.

Table 2: Overview of selected legal acts in Germany obliging stakeholders to assess/ increase resilience

Legal act	Relevant because	CI stakeholders mainly affected	Link
Gesetz über die Elektrizitäts- und Gasversorgung, July 07, 2005	Regulates the provision of electricity and gas.	All gas and electricity providers	https://www.gesetze-im-internet.de/bundesrecht/enwg_2005/gesamt.pdf
Gesetz zur Sicherung der Energieversorgung, December 12, 1974; latest change on August 31, 2015	Designed to secure the provision of energy.	All energy providers	https://www.gesetze-im-internet.de/ensig_1975/BJNR036810974.html
Verordnung zum Schutz von Übertragungsnetzwerken, January 6, 2012; latest change on August 31, 2015	Regulates the protection of the transmission grid.	Operators of transmission grids	https://www.gesetze-im-internet.de/_nschutzv/%C3%9CNSchutzV.pdf
Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), July 17, 2015	Aims to increase IT security.	Relevant to every organization that uses IT-based systems	http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.html
Bundesdatenschutzgesetz, January 14, 2003	Regulates the protection of data.	Relevant to everyone who collects data	https://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html
Betriebssicherheitsverordnung, February 3, 2015; latest change on March 29, 2017	It aims to ensure good safety and healthy work conditions in Germany.	All operators of critical infrastructures	https://www.gesetze-im-internet.de/betrsichv_2015/BJNR004910015.html

2.2.1.1 "Gesetz über die Elektrizitäts- und Gasversorgung" (Law on electricity and gas provision)

At the most general level, the "Gesetz über die Elektrizitäts- und Gasversorgung" (Law on electricity and gas provision) aims to provide a secure, cheap, customer-friendly, efficient and environmentally safe, grid-bound provision of energy and gas to the public, which increasingly relies on renewable energy. With regard to

resilience and security, paragraphs 11 to 16 of part 1 of the law (Regulation of the Network) mentions the duties of grid operators. In detail, these 6 paragraphs state the following:

§11 Operating power supply grids;

§12 Duties of the operators of electricity power supply grids;

§13 Responsibilities of operators of transmission grids for the energy system;

§14 Duties of operators of distribution grids;

§15 Duties of operators of long-distance line networks;

§16 Responsibilities of operators of long-distance line networks for the energy system.

In addition, part 6 (§ 49 – 53) of the law addresses the security and reliability of the energy provision. These paragraphs pertain to:

§49 Requirements for facilities;

§50 Use of stockpiles for securing energy provision;

§51 Monitoring the security of energy feed-in;

§51a Monitoring load management;

§52 Obligation to report disruptions of the energy feed-in;

§53 Call for bids for new energy capacities in the electricity sector.

2.2.1.2 "Gesetz zur Sicherung der Energieversorgung" (Law on the security of energy supply)

Related to the overall law on electricity and gas provision is the more specific Gesetz zur Sicherung der Energieversorgung ("Law on the security of energy supply") from December 20, 1974, which was last amended by article 324 of the provision from August 31, 2015. Paragraph 1 of the law regulates energy supply security:

In order to protect the vital supply of energy in the case of an emergency and disruption of service when the disruption cannot be overcome by market driven mechanisms, regulation can be put in place with regard to

a. Production, transport, storage, distribution, dissemination, purpose, use, and price of oil and oil products as well as other solid, liquid and gaseous energy sources, electrical energy, and other energy (goods);
b. Legal obligation to keep records, supporting documents, notification duties on the market processes described in section 1 and about volumes and prices as well as other market conditions of these goods and;
c. Production, maintenance, distribution, connection and use of production materials of the market economy if these production materials serve the creation of electrical energy and gas, as well as the services and works of businesses for the maintenance, restoration, production and change of buildings and technical facilities that serve to supply electrical energy and gas.

Vital functions also include the fulfilment of public services and international obligations.

Subsequent paragraphs deal with international obligations, the enactment of regulations, the implementation of the law, and more specific elements, e.g. compensation for losses, or punishments in case violation of the law.

2.2.1.3 "Verordnung zum Schutz von Übertragungsnetzen" (Regulation for the protection of the power transmission grid)

The protection of the transmission grid is regulated in the "Verordnung zum Schutz von Übertragungsnetzen" ("Regulation for the protection of the power transmission grid"), which came into force on January 6, 2012, and was amended on August 31, 2015. The regulation serves to implement the EC directive 2008/114/EG. It contains 7 paragraphs:

§ 1 Report by energy grid providers

a. All operators of transmission grids have to provide a report that explains whose disruption would impact on at least two members of the EU.
b. The risk scenarios prepared by the German Federal Office for Civil Protection and Disaster Assistance (BBK) in conjunction with the Federal Network Agency are to be used as basis for the risk assessment.

§ 2 Definition of European critical facilities

Within two months after the submission of the report, the Federal Network Agency will declare facilities as European critical facilities, i.e. facilities whose disruption have implications for several European countries.

§ 3 Appointment of security manager

a. Within two weeks of being declared a European critical facility, the operators have to announce the nomination of a security officer.
b. The security officer acts as a point of contact and has to be able to provide information about the facilities' security plan.

§ 4 Development of security plans

Within four weeks of being declared a European critical facility, the operator has to develop a security plan that includes the following information:

a. Declaration of the European critical facility.
b. Results of a risk assessment, which is based on risk scenarios mentioned in § 1 section 2, that discusses the weaknesses of the facility and the effects of its disruptions.
c. Development and determination of rank of order of countermeasures and procedures; these have to differentiated according to
    - Permanent security measures, which includes information on
        - Technical measures; in particular early warning systems, access controls as well as protection and preventative measures,
        - Organizational measures, in particular plans for the case of emergency and crisis management,
        - Surveillance and inspection plans,
        - Communication,
        - Raising awareness and education,
        - Securing information systems, and
    - Transitory security measures that can be activated depending on the level of threat and risk.

§ 5 Confirmation and inspection of security plan

a. The security plan will be assessed by the Federal Network Agency after four weeks of its declaration. If the plan is in accordance with §4 the operator will receive an approval of the plan. If it fails to meet the requirement, the operator will be given a time limit to remedy the situation.
b. In case the security officer fails to meet requirements set out in §3, section 2, the Federal Network Agency can request the operator to provide adequate training or announce a new officer.

§ 6 Classification of sensitive information

The Federal Network Agency decides which information, reports and security plans have to be classified.

§ 7 Entry into force

This regulation enters force on the day of its declaration.

2.2.1.4 "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" (Law to enhance the security of information systems)

With regard to the protection of information systems of critical infrastructure, the "Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes" (Law for Strengthening the IT-Security of the Federation) was amended to become the "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" (Law to enhance the security of information systems) in 2015 and now includes specific

provisions for CI. Paragraph 2 has been expanded to specify what facilities or parts thereof are indeed critical infrastructures. They include all facilities (1) in the sectors Energy, IT, Transport and Traffic, Health, Water, Food, Finance and Insurance, (2) which are important for providing public services and whose disruption would threaten public safety and security. Paragraphs §8a through d then outline the duties of operators (§8a), nominate the national contact point (the "Bundesamt für Sicherheit in der Informationstechnik") and list its obligations (§8b), to whom the laws apply (e.g. small businesses are excluded from §8a and §8b) (§8c), and the regulation of what information can be accessed publicly (§8d). Paragraph §14 discusses provisions concerning fines.

2.2.1.5 Betriebssicherheitsverordnung – BetrSichV: Verordnung über Sicherheit und Gesundheitsschutz bei der Verwendung von Arbeitsmittel (Regulation for health and safety at work)

The regulation aims to ensure good safety and healthy work conditions in Germany. It defines requirements in terms of safety measures, the right choice and use of specific means of productions, requirements regarding manufacturing processes as well as personnel qualification and information. Additionally, it defines federal legal penalties regarding the use and management of means of production.

Relevant paragraphs are summarized below:

§11 special events, disturbances, accidents

Here, the document describes requirements regarding special events, disturbances and accidents. This includes: (1) The duty for the employer to act immediately in case of some sort of "instability" and to re-establish a normal and stable functioning of the concerned mean of production. (2) The possibility to rescue and medically treat people. (3) The communication and provision of information related to the specific incidents. (4) The obligation to employ qualified personnel for actions regarding point one and (5) the obligation to define and to properly signal areas of danger.

§12 Briefing of employees

This paragraph defines requirements regarding the briefing of personnel about possible dangers and adequate reactions, which includes oral briefing as well as written documents.

§13 Cooperation between different employers

In case of different employers involved (e.g. due to subcontracting) this paragraph defines the requirements of communication and cooperation of these regarding possible dangers and adequate reactions in case of incidents.

§19 Duty to inform relevant government agencies

This paragraph defines the cases in which an employer needs to inform relevant government agencies (all cases with deaths or major injuries). The employer has the obligation to provide additional information if asked for (especially the reason for the incident and its possible consequences). This duty to report is to help the relevant agency to react immediately (if required) or to improve the overall safety and resilience in the long run.

In summary, these regulations can help to improve the resilience of a given SCI. There are several implications for SmartResilience and CI operators: §12 concerns phase two (Anticipate/prepare); §11 and §13 concern phase three (absorb/withstand) and phase four (respond/recover); §19 could help to improve the response/recover capacity (phase 4) and also to adapt and learn (phase 5) from an incident.

2.2.2 Guidelines and support

The following section contains information about a selected number of international and national guidelines that pertain to a variety of infrastructure systems. The guidelines were identified in discussions with topic experts and operators of energy infrastructures in Germany and EU countries.

These guidelines are supplementary to those projects and guidelines that have provided the basis for the SmartResilience approach, which have been discussed in detail in D1.1 and in D1.2. Besides the discussion of other EU projects on resilience, there is specific information on guidelines and approaches by UNISDR, OECD,

and FEMA in D1.1 and other indicator based approaches to resilience and corresponding guidelines in D1.2. The following guidelines provide information about resilience in specific fields of critical infrastructure or describe interesting regional and local efforts to increase resilience.

2.2.2.1 National (Germany)

Technische Regeln für Betriebssicherheit (TRBS)

The „technical guidelines for industrial safety“ (TRBS) are documents complementing the “BetrSichV”(see chapter 2.2.1.5). While implementing the TRBS, the operator should consider that the facility or infrastructure has “to be in compliance” with the requirements of the BetrSichV. The exact implementation is not legally binding, but in case of non-implementation, the operator has to prove that the “equivalent or better” measures are implemented in the infrastructure to ensure safety and resilience. More than 30 TRBS are currently (June 2017) valid, but only some of them are likely to specifically affect critical infrastructures: This is the case for TRBS 2141 (Gefährdungen durch Dampf und Druck), TRBS 3146 (Ortsfeste Druckanlagen für Gase), TRBS2151 (Gefährliche explosionsfähige Atmosphäre – Allgemeines). It is likely that all three TRBS are relevant for case study ECHO (refinery in the industrial zone) and HOTEL (energy supply). They are briefly summarized below:

TRBS 2141 concerns dangers related to steam and pressure [41].

First, TRBS 2141 provide guidelines about the *determination* of danger. A determination of danger should be done by focusing on the following aspects: shock waves, flying parts and slapping ropes, which originate from explosions as well as dangers of suffocation, poisoning, burning and freezing which originate from leaking elements [41].

Secondly, TRBS 2141 is giving guidelines on the *evaluation* of danger. Dangers should be evaluated using the following indicators: amount of stored energy, access of employees or third persons, location of the device (inside/outside of the facility), characteristics of the pressured elements, nature of the facility/device, technical condition of the facility/device, equipment of the facility/device, usage of the facility/device and damage mechanisms [41].

Finally, the guideline comments on suitable measures to reduce danger: Measures should be based on the determination and evaluation of danger and should be initiated (in case of a critical situation) following a specific order: First technical measures, secondly organizational measures and third personnel measures. External influences (like weather) should be taken into account and it is necessary to comply with any other guidelines given by the manufacturer [41].

TRBS 3146 concerns dangers related to facilities containing gas (as well as hydrogen cyanide) [43].

It defines areas/stages of possible dangers (installation, filling, storage, emptying, maintenance, quiesce i.e. pause or alter a device or application to achieve a consistent state, disassembly) which the owner of the facility should investigate and evaluate possible threats. Once the specific threats are identified, the owner should define appropriate measures to be taken in case of an emergency. In particular, these measures should aim to reduce the likelihood of a gas leak, limit the volume of gas leakage and ensure the safety and security of vulnerable individuals and objects in the vicinity [43].

The document goes then into the details of the measures to be implemented: They are divided into nine categories [43]:

1. Defining the hazard areas,
2. General measures such as installation of leak proof facilities,
3. Signaling units and emergency shut off systems,
4. Requirements for pipes and valves for equipment that contain gas,
5. Requirements for the setup(e.g. emergency exits, ban of traffic areas) of the facilities containing gas,
6. Measures for buried facilities containing gas,
7. Requirements for audit,
8. Requirements for Operation of stationary facilities containing gas and
9. Special security measure.

TRBS2151 concerns the identification and prevention of explosions [40]. According to §5 ArbSchG, every employer is legally bound to assess and identify such threats and to take appropriate measures to prevent any explosion. TRBS2151 provides general guidelines for implementation and the aspects to assess include:

1. The existence of inflammable substances
2. The possible existence of explosive atmospheres by these substances
3. The scale of the danger such atmospheres could reach
4. Measures to contain such atmospheres (see 5 and 7)
5. Possible alternative substances and way to eliminate the explosive atmosphere without danger
6. If elimination is not possible the evaluation of probability and endurance of such an explosive atmosphere, possible ignition sources as well of possible effects of an explosion
7. Measures to avoid the occurrence of explosive atmospheres, measures to avoid ignition of such atmospheres as well as measures to reduce the impact of explosions

Once all these aspects are assessed, an integrated explosion protection plan has to be developed and implemented [40].

To summarize, clearly the technical guidelines summarized above are of significant importance to the infrastructures such as a refinery in Pancevo or the energy supply system in Helsinki. Furthermore, these guidelines could help to improve the resilience of these infrastructures by means of understanding the risks (Phase 1) and preventing the threat scenarios by means of anticipating and planning (Phase 2) of the resilience cycle.

DIN VDE 0105-100

The DIN VDE 0105-100 standard discusses all safety related aspects of working on, with or near any facility or installation, either fixed or movable that produces electrical power. The generated electricity can range from extra-low voltage up to high voltage. The norm lists all of the requirements that are necessary for the safe operation of these facilities and includes best practices for working in the proximity of these installations, e.g. construction work near cables and power lines. It covers all details, including terminology, personnel, operation, equipment and communication.

2.2.2.2 International

ISO Standards

The entire ISO27k standards series pertains to “information technology – security techniques” and is thus highly relevant for any operator of an energy infrastructure. The standards range from terminology to implementation guidelines and risk management. Especially ISO 27001 is widely known, as it sets out the requirements for an information security management system (ISMS). “An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process” [53].

American Petroleum Institute

“The American Petroleum Institute (API) is the only national trade association that represents all aspects of America’s oil and natural gas industry. Its 650 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. They are producers, refiners, suppliers, marketers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry” [1].

“For more than 85 years, API has led the development of petroleum and petrochemical equipment and operating standards. These represent the industry’s collective wisdom on everything from drill bits to environmental protection and embrace proven, sound engineering and operating practices and safe, interchangeable equipment and materials. API maintains 685 standards and recommended practices. Many have been incorporated into state and federal regulations; and increasingly, they’re also being adopted by the International Organization for Standardization, a global federation of more than 100 standards groups”

[1]. One section of its standards focusses on safety and fire protection [2]. Within this section a lot of guidelines are listed that discuss Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries as well as guidelines on fatigue management of personnel and many different diverse guidelines. Only a short description of these guidelines is given.

In specific, API has two standards that might be useful to SmartResilience: Std 780: Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries; RP 754: Process Safety Performance Indicators for the Refining and Petrochemical Industries. Also, API 581 [4] provides a list of indicators which are useful for assessment of resilience of CIs in SmartResilience [55].

API RP 780: Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

API 780 provides a five step Security Risk Assessment (SRA) for the petroleum and petrochemical industries. It covers a wide range of security threats from theft to insider sabotage to terrorism. It can be used for both fixed and mobile applications. "A SRA is a systematic process that evaluates the likelihood that a given threat factor (e.g. activist, criminal, disgruntled insider, terrorist) will be successful in committing an intentional act (e.g. damage, theft) against an asset resulting in a negative consequence (e.g. loss of life, economic loss, or loss of continuity of operations). It can consider the potential severity of consequences and impacts to the facility or company itself, to the surrounding community, and on the supply chain." [24]

The five sequential steps of the SRA are as follows:

"1) *Characterization*-Characterize the facility or operation to understand what critical assets need to be secured, their importance, and their infrastructure dependencies and interdependencies;

2) *Threat Assessment*-Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each threat and the consequences if they are damaged, compromised, or stolen.

3) *Vulnerability Assessment*-Identify potential security vulnerabilities that enhance the probability that the threat will successfully accomplish the act.

4) *Risk Evaluation*-Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the maximum credible consequences of an event if it were to occur; rank the risk of the event occurring and, if it is determined to exceed risk guidelines, make recommendations for lowering the risk.

5) *Risk Treatment*-Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses) and reassess risk to ensure adequate countermeasures are being applied. Evaluate the appropriate response capabilities for security events and the ability of the operation or facility to adjust its operations to meet its goals in recovering from the incident." [24]

API RP 754: Process Safety Performance Indicators for the Refining and Petrochemical Industries

API 754 is a recommended practice (RP) particularly aimed at refineries and chemical industry, providing precise definitions and an indicator classification for benchmark purposes [102]. It identifies leading and lagging process safety indicators useful for driving performance improvement. A distinction is made between four types of process safety events (PSEs) which, in order of decreasing severity, are referred to as tier-1 to tier-4. These are linked to different kind of events, and corresponding indicators Figure 2.

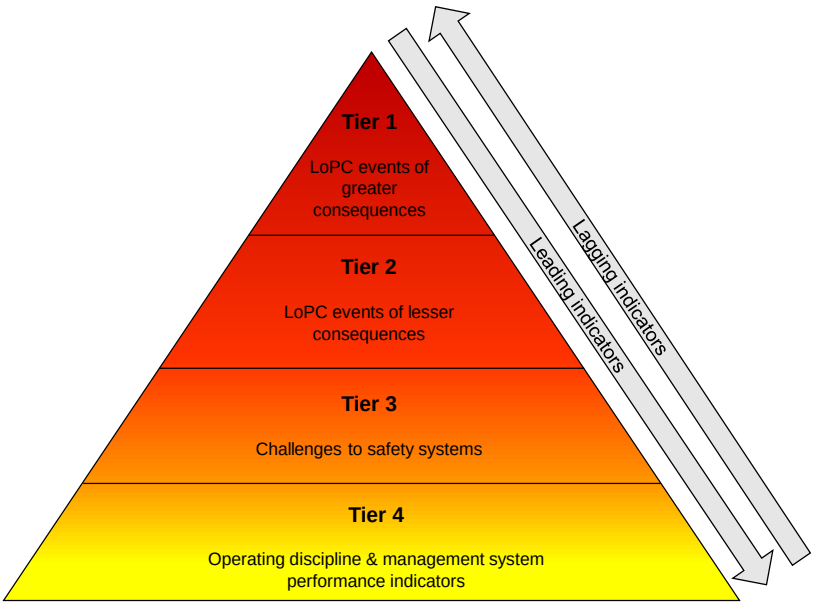

Figure 2: Process safety indicator pyramid

It is an important standard because it has been globally supported and adopted by the oil suppliers and integrated oil companies [50]. It was initially developed for the refining and petrochemical industries, but may also be applicable to other industries with operating systems and processes where loss of containment has the potential to cause harm, hence can be useful for more than one CI.

In terms of its applicability of measuring resilience of the CI, this practice focuses on the understand risk and anticipate/prepare phase by means of leading indicators and also the adapt/learn phase by means of lagging indicators.

Furthermore, API 581 provides a list of indicators such which can be adapted to measure the resilience of the CIs. Some of the indicators useful for the resilience assessment adapted from API581 are presented in Table 3

Table 3: Resilience Indicators adapted from API 581 [4]

Nr.	Reference	Resilience Indicator
1.	API 581	Resilience policy documented and applied?
2.	API 581	Resilience-related responsibilities clearly defined?
3.	API 581	Training for resilience management in place?
4.	API 581	General & specific resilience training procedures exist?
5.	API 581 /ANL [78]	Emergency control center designated & operational?
6.	API 581 & ANL [78]	Personnel assigned to contact for emergency plan?
7.	API 581 /ANL [78]	Incident investigation procedures include?

OECD

In 1971, OECD established a programme to address chemical safety, focusing initially on chemical testing and assessment [54]. It was later expanded to address risk assessment and management, to the testing of certain high-production volume chemicals, and to account for the safety of pesticides, biocides, and products of biotechnology [54]. Following the Bhopal and Basel accidents, the OECD countries decided that the programme should also address the issues related to chemical accident prevention, preparedness, and response and set a new working group to manage these activities. The Working Group on Chemical Accidents has brought together OECD and non-OECD countries, as well as industry, unions, UN bodies, and nongovernmental organizations, to collaborate in addressing issues related to chemical accident prevention, preparedness, and response [54]. One element of its work was to develop the Guidance on Safety Performance Indicators (SPI). The OECD published the 2008 Guide on Developing Safety Performance Indicators in two versions: one for industry and one for public authorities and civic associations [102]. These documents, developed by a group of experts from the public and private sector, are based on 'best practices' of measuring safety performance [102].

The guideline consists of two primary components:

- a step-by-step approach for developing SPI programmes; and
- a menu of possible indicators which addresses the range of issues involved with chemical accident prevention, preparedness, and response.

The Guidance sets out a seven-step process for creating an SPI programme [77], i.e.:

- Step One: Establish the SPI team
- Step Two: Identify the key issues of concern
- Step Three: Define outcome indicator(s) and related metrics
- Step Four: Define activities indicator(s) and related metrics
- Step Five: Collect the data and report indicator results
- Step Six: Act on findings from SPIs
- Step Seven: Evaluate and refine SPIs

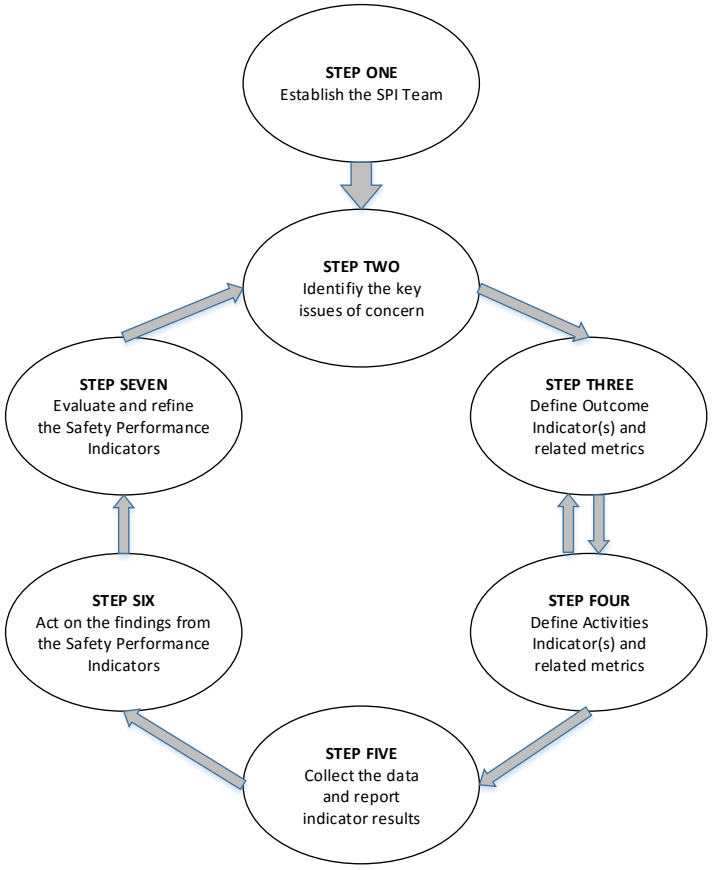

Figure 3: OECD's seven-step process for creating an SPI Program [77]

This guideline also provides a list of possible safety outcome and activities performance indicators for the following topics [77]:

- Prevention of accidents
- Emergency preparedness
- Response and follow-up to accidents

Outcome indicators help in assessing if the safety-related actions (policies, program, procedures and practices) achieve their desired results [77]. Also, they show if the actions reduce the likelihood of an accident and/or less adverse impact on human health, the environment and/or property from an accident. They are reactive, intended to measure the impact of actions that were taken to manage safety and are similar to what are called "lagging indicators" [77], for example, the number of incident resulting from the failure to manage change appropriately. Outcome indicators often measure change in safety performance over time, or failure of performance. Thus, outcome indicators tell you whether you have achieved a desired result (or when a desired safety result has failed). But, unlike activities indicators, they do not tell you why the result was achieved or why it was not [77].

Activities indicators help to identify whether CIs are undertaking measures required to decrease the risks (e.g., the types of policies, program, procedures and practices described in the Guiding Principles). These are proactive measures, and are similar to what are called "leading indicators" [77]. For example, is there a clear definition of a change (modification)? They often measure safety performance against a tolerance or threshold level that shows deviations from safety expectations at a specific point in time. When used in this way, activities indicators highlight the need for action when a threshold level is exceeded. Thus, activities indicators provide organizations with a means of checking, on a regular and systematic basis, whether they are implementing their priority actions in the way they were intended. They can help elaborate the reason for a result (e.g., measured by an outcome indicator) achievement or failure.

From the perspective of CI operators, an SPI may allow to [54]:

- assess whether it is implementing appropriate chemical safety programs and policies,
- evaluate whether these programs and policies are achieving their desired objectives, and
- help determine the extent to which such programs and policies are making a difference.

This allows a CI to identify if there is appropriate emphasis on different aspects of safety management and provide insights on the need for setting priorities for future investment of resources [54]. It can also facilitate communication and cooperation with public authorities, other enterprises, and the local community.

Clearly, this guideline and the possible outcome and activities SPIs can support the CIs resilience assessment in two phases of the resilience cycle i.e. plan/prepare and recover/respond. For the SCIs in SmartResilience project, it could be useful to consider these applicable SPIs to ensure safety of their critical infrastructure for any chemical accident prevention, preparedness, and response.

Centre for Chemical Process Safety (CCPS)

The Centre for Chemical Process Safety (CCPS), provided process safety leading and lagging metrics with the metaphor "You don't improve what you can't measure". CCPS was established in 1985 by the American Institute of Chemical Engineers (AIChE) for the purpose of assisting industry in avoiding or mitigating catastrophic chemical accidents. It aims to achieve its purpose by developing and promoting the use of common metrics across the industry and around the world. Several corporate members around the world drive the activities of CCPS [17].

The CCPS programme is built on three types of metrics [17]:

1. "Lagging" Metrics – a retrospective set of metrics based on incidents that meet the threshold of severity and should be reported as part of the industry-wide process safety metric [17]
2. "Leading" Metrics – a forward looking or proactive set of metrics which indicate the performance of the key work processes, operating discipline, or layers of protection that prevent incidents [17]
3. "Near Miss" and other internal Lagging Metrics – descriptions of less severe incidents (i.e., below the threshold for inclusion in the industry lagging metric), or unsafe conditions which activated one or more layers of protection. Although these events are actual events (i.e., a "lagging" metric), they

are generally considered to be a good indicator of conditions which could ultimately lead to a more severe incident [17]

The programme recommends all companies to incorporate these three types of metrics into their internal process safety management system. Furthermore, it suggests a list of indicators such as number of incidents with (failed) risk assessment as a root cause; inspection, testing and maintenance activities completed on schedule; number of errors during simulation training; Number of drills conducted with local emergency responders etc.

Table 4: Example of the CCPS indicators use for defining resilience indicators [55]

Source	Safety indicator	Resilience indicator	Details of the indicator	Phase
CCPS	Number of incidents with (failed) risk assessment as a root cause of the incident	Number of incidents with (failed) risk assessment as a root cause	Are there incidents with (failed) risk assessment as a root caused recorded? What is the percentage of events with (failed) risk assessment as a root cause? High: less than equal to 39% of the events Medium: between 40-69% of the events Low: between 70-100% of the events No record	Understand risk
CCPS	Percentage of sites that conducted a drill with local emergency responders during the year	Number of drills conducted with local emergency responders	Are the regular drills conducted with local emergency responders? How often the regular drills are conducted to evaluate and reinforce the emergency plan? High: once/ month Medium: once/ 6 months Low: once/ 1 year Never	Anticipate/ Prepare
CCPS	Number of errors during simulation training	Percentage of errors due to deficiency in simulation training?	Are the errors due to deficiency in training recorded? What is the percentage of errors recorded in the simulator? High: less than 5% Medium: between 5-10% Low: more than 20% No record	Anticipate/ Prepare

This programme is of significance to those CIs in the SmartResilience project that deal with chemicals such as the NIS refinery. The process safety indicators once applied can provide significant insights on the resilience of the CI. Also, as stated earlier, according to [55] the preliminary results of the application of the SmartResilience methodology suggest that safety indicators suggested by CCPS can be useful for the first two phases of the resilience cycle.

International Association of Oil & Gas Producers (IOGP)

The International Association of Oil & Gas Producers (IOGP) is the advocacy institution for the global upstream industry for oil and gas. Oil and gas continue to provide a significant proportion of the world's growing energy demands for heat, light and transport. The members produce more than a third of the world's oil and gas. They operate in all producing regions: the Americas, Africa, Europe, the Middle East, the Caspian, Asia and Australia. They aim to serve industry regulators as a global partner for improving safety, environmental and social performance. They also act as a uniquely upstream forum in which members identify and share knowledge and good practices to achieve improvements in health, safety, the environment, security and social responsibility [51].

Since 1985, the OGP has been reporting about the trends in safety in the oil and gas upstream industry (upstream industry means the part of the supply chain that works on crude oil extraction). It is done by means of safety performance indicators such as number of fatalities, fatal accident rate, fatal incident rate, total recordable injury rate, lost time injury frequency, number of lost work days, number of restricted work day cases, etc. The submission of data is voluntary and is used for trend analysis, benchmarking and identification of areas and activities on which efforts should be focused to bring about general improvements in performance. These indicators and trend analysis data provides an understanding of the impact after an incident occurred, thereby giving insights on the response and recovery phase of the resilience cycle [51].

Furthermore, in 2011 the OGP report number 456 detailing the recommended practice (RP) on key performance indicators was issued by the International Association of Oil & Gas Producers (OGP) following the report 415 on asset integrity [50]. It acts as a companion to the report on asset integrity – a key to managing major incident risks and describes practical implementation of KPI system [50]. It refers to UK HSE guidelines, CCPS OECD and the ANSI/API RP754 [50]. OGP links leading indicator to preventive barriers and lagging indicator to de-escalating barriers [102]. For so-called critical barriers a combination of a leading and a lagging indicator is suggested to test the strength of the barrier.

In the guidance, OGP aimed at:

1. Identification of indicators that are reliable, clearly defined, and implementable across the upstream oil & gas industry.
2. "Loss of primary containment (LOPC)" of hazardous material, which is the predominant cause of major process safety incidents in the oil and gas production industry [50]. These LOPC events occur when there is a failure in the prevention barriers of the system. In this context, "Recording the number of LOPC events or actual consequences where one or more barrier fail simultaneously – is a "lagging" indicator" [50]. Also, monitoring the strength of the barrier by measuring the company's performance in maintaining robust risk controls – is a "leading indicator" [50].
3. Furthermore, it suggests that the companies can become aware by looking at some indicators that provide both retrospective and forward-looking insights, for example "near misses" [50]. Analysis of near miss events provides information on the likelihood of an actual incident and also provides lagging information on barrier weaknesses. Investigating near misses can help in continuous improvement of asset integrity and process safety by identification of weaknesses and providing warnings of potential events.

Table 5: Leading and lagging indicators [50]

"Lagging" indicator.	"Leading" indicator
Recording the number of LOPC events or actual consequences where one or more barrier fail simultaneously – is a "lagging" indicator.	Monitoring the strength of the barrier by measuring the company's performance in maintaining robust risk controls – is a "leading" indicator.
Retrospective in nature	Forward-looking nature

Clearly, the recommended practice is applicable to the ECHO (Oil refinery, Serbia) and HOTEL (Energy supply, Finland) case studies in SmartResilience. It can also be applied to the BRAVO case study for electricity supply, where the leading and lagging indicators could be adapted for the analysis of retrospective and future events.

2.3 Case study: Drinking water supply in Sweden

This chapter uses drinking water supply as an example of how the legislative system in Sweden is designed and how it supports and advices the assessment and strengthening of resilience. The analysis further elucidates how end-users (in this case drinking water producers and distributors, that is, municipalities or their companies) adopt legislation and how it shapes their resilience efforts.

2.3.1 Legal acts

The Swedish legislative system can be described as decentralized, with a high degree of power delegated to governmental agencies. The parliament issues acts (Swedish 'lag') on certain issues, such as emergency management and drinking water supply that regulate how various actors should address related issues. The government, as mandated by the parliament, issues regulations (Swedish 'förordning') that outline the work of governmental agencies on various topics, such as emergency management. The agencies run certain activities and they regulate what others do, such as municipalities. Agencies are usually national and sectoral in scope but all counties also have county administrative boards that on a regional basis oversee, coordinate, support and follow up on a large number of issues on behalf of central agencies, including emergency management and drinking water supply. These agencies are mandated to issue rules (Swedish 'föreskrift').

The municipalities are responsible for providing safe water to consumers that are connected to public distribution networks, covering around 90 percent of the population, whereas the rest has access to water through private wells. The regulatory framework encompasses raw water sources, water production and distribution.

To identify relevant legislation, a number of searches were made. The Swedish Water and Wastewater Association (Svenskt Vatten/SWA) advice and guidelines listing various agencies and their roles for drinking water supply were used [88]. Also the Swedish National Food Agency advice for risk and vulnerability analysis, which lists relevant legislation and methods and their applicability, was used [59]. Further, relevant legislation from the Swedish Civil Contingencies Agency (MSB) related to CI protection, emergency management, risk and vulnerability analysis, and information security was identified. In addition, legislation regarding security of certain objects, as regulated by the Swedish Security Service (Säkerhetspolisen), was analysed. In the presentation below (Table 6 and the following description), focus is on the most relevant legislation. A more comprehensive overview is provided in Annex 2.

Table 6: Overview of selected legal acts in Sweden obliging stakeholders to assess/ increase resilience

Legal act	Addressees	Relevant because	Stakeholders mainly affected	Link	Note
Act on Municipal and County Council Measures prior to and during Extraordinary Events in Peacetime and during Periods of Heightened Alert (2006:544)	Municipalities and counties/regions	Regulates the emergency and crisis management of drinking water producers and distributors	Municipalities and counties/regions, as well as others involved	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2006544-om-kommuners-och-landstings_sfs-2006-544	
Rule of municipalities' risk and vulnerability analyses (MSBFS 2015:5)	Municipalities	Regulates what municipalities should investigate and prepare for	All of them	https://www.msb.se/externdata/rs/15e78831-767b-4714-9fa4-3b4fd0df92a8.pdf	Including definitions of terms, checklist/indicators and advice
Rule about national agencies' reporting of IT incidents (MSBFS 2016:2)	National agencies	Regulates what agencies need to report to MSB	A large number of agencies as listed in regulation (2015:1052)	https://www.msb.se/externdata/rs/f21ae5f7-b655-4462-a2e6-9939b952a751.pdf	Includes advice
Rule and advice for protection of certain objects, information and material (PMFS2015:3)	Public agencies that run certain critical activities (need for protection against terrorism, espionage, sabotage and robbery)	Regulates what objects need to be protected, such as drinking water production	The military, municipalities, counties or to organizations otherwise in charge of these activities (referring to law 2010:305)	http://www.sakerhetspolisen.se/download/18.1beef5fc14cb83963e7c8b/1430826384590/Sakerhetspolisens_foreskrifter_allmanna_rad_sakerhetsskydd.pdf	Includes advice
Act on protection of certain objects (2010:305)	Public agencies that run certain critical activities (need for protection against terrorism, espionage, sabotage and robbery)	The military, municipalities, counties or to organizations otherwise in charge of these activities	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/skyddslag-2010305_sfs-2010-305		

Legal act	Addressees	Relevant because	Stakeholders mainly affected	Link	Note
Rule regarding measures to be taken in regard to sabotage and other damage to drinking water facilities (LIVSFS 2008: 13)	Municipalities	Regulate what producers and suppliers need to take into account	Those in charge for drinking water production and supply	https://www.livsmedelsverket.se/globalassets/om-oss/lagstiftning/dricksvatten---naturl-mineralv---kallv/livsfs-2008-13-kons.pdf	The National Food Agency has separate guidelines for SLVFS 2001:30 and LIVSFS 2008:13, encompassing a 158 pages book
Environmental code (1998:888) *Chapter 7*	Public agencies – municipal or regional	Stipulate the need to plan for and protect raw water sources	Protecting raw water sources	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/miljobalk-1998808_sfs-1998-808	
Food Act (2006:804)	Public agencies – municipal or regional – as well as private enterprises	Regulate the need to assess the need for critical supply of drinking water	Municipalities e.g. as drinking water producers and suppliers	http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/livsmedelslag-2006804_sfs-2006-804	
Regulation on food (2006:813)	Public agencies – municipal or regional – as well as private enterprises	Regulate how to secure critical supply of drinking water	Municipalities e.g. as drinking water producers and suppliers	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/livsmedelsforordning-2006813_sfs-2006-813	
Rule on drinking water (SLVFS 2001: 30)	Municipalities	Regulate how to assess safe drinking water	Those in charge for drinking water production and supply	https://www.livsmedelsverket.se/om-oss/lagstiftning1/gallande-lagstiftning/slvfs-200130	Includes 30 pages with detailed advice

Overall emergency management legislation

The Swedish Civil Contingencies Agency (MSB) supports and oversees municipal and regional government activities with respect to crisis and emergency management (CEM), covering measures taken before, during

and after an emergency or crisis. MSB also supports and oversees how other agencies with responsibilities for various critical infrastructures address issues of resilience in its different phases and dimensions. Moreover, MSB is responsible for issues of coordination, i.e. addressing interdependence and mutual support between agencies.

MSB, as part of its assignment to oversee critical infrastructures and crisis and emergency management, regulate municipalities' work to set up, review and revise their overall crisis and emergency management plans. This includes their preparedness according to act 2006: 544 and associated regulations (2006: 942, 2015: 1052), that prescribe a risk and vulnerability analysis and a plan for managing extraordinary events, such as a crisis management committee, training programs and reporting schemes, responsibilities for supplying food including drinking water etc. The rule MSBFS 2015: 5 around risk and vulnerability analysis in municipalities further defines terms such as risk, critical dependencies, critical infrastructures (or activities), vulnerability and crisis preparedness. The actors involved need to identify safety-critical (socially relevant) businesses within their area of responsibility, to run those businesses, to coordinate and support as well as to follow-up, report and learn from their experiences.

Security legislation

Information and IT security falls under *the regulation of national agencies reporting of IT-incidents (MSBFS2016:2)* issued by the Swedish Civil Contingency Agency (MSB) as well as under *the regulation and advice of protection of certain objects, information and material (PMFS 2015:3)* issued by Swedish Security Service (SÄPO). Today, water production facilities are all protected objects, falling under the *Act on protection of certain objects (2010:305)* and related regulation and rule (LIVSFS 2008: 13). These objects should be protected from unauthorized access and unauthorized description, such as photos or drawings. To protect them, one can use police, military forces or other assigned personnel [79]. Organizations falling under this legislation, such as municipalities, are required to investigate what data and what objects needs to be protected in order to uphold national security and protection against terrorism [80]. The regulation also includes the obligation for governmental agencies to report IT-incidents that have occurred in the information system.

Regulatory requirements for drinking water resilience

The Environmental Code (1988: 888) and related legislation prescribes the need to arrange water protection areas and a water provision plan. This legislation is crucial to ensure sufficient raw water supply of sufficient quality.

The Food Act (2006:804) and related legislation (e.g. 2006:813) require producers to make a risk analysis to ensure sufficient barriers towards potential contamination. Water producers need to have equipment that enables a) warning against errors in pH-adjustment and disinfection, b) alarm for increased turbidity, c) a description of the water works and, d) an operational instruction. This legislation also prescribes measures to be taken to ensure distribution. A distribution system needs to be designed, maintained and served so as to ensure the required amount and quality when it reaches the consumers. Moreover, the responsible organization needs to ensure that unauthorized persons cannot access reservoirs, pump stations and the like.

The National Food Agency (NFA) is the central actor in a system comprised of many other actors dealing with drinking water. NFA is only concerned with the quality of the water for drinking purposes. Other actors include municipalities and the county administrative boards. The emergency management rule SLVFS 2001:30 prescribe risk analysis and preparedness for water producers and distributors. For example there is a need to set up, review and revise a) a risk and vulnerability analysis, b) an emergency plan, and c) a crisis management plan with routines for a number of disturbances (such as water borne infection, loss of electric power, major leakage, and contamination with oil or chemicals).

2.3.2 Guidelines and support

To identify what and how elements shape the application of legislation, handbooks and advice were used from the agencies and SWA as well as evaluations, research reports, as well as interviews carried out (in April 2017) with representatives from the Swedish Civil Contingencies Agency (MSB), the SWA, the National Food Agency, the research program DRICKS on drinking water coordinated by Chalmers University of Technology and with the Northern Water Board (Kommunalförbundet Norrvatten), the drinking water producer.

The indicators and checklists provided together with rules should be seen as part of the advice that government agencies are required to provide, as a means to improve compliance. Most of the time, the indicators are on a yes or no basis accompanied with a space for reflection. They are not designed to indicate performance levels for the actual issue being indicated, rather as guidance towards the addressees' own work fulfilling legislative demands. Through posing questions on specific topics they provide food for thought, stressing what the regulators need to do. Taken as a whole, a large number of no-answers or yes-answers will give a rough estimate of the status of a critical infrastructure or various dimensions of it, as a sort of resilience level. Moreover, governmental agencies as well as the Swedish Water and Wastewater Association provides additional guidance, training and arranges seminars and conferences.

Table 7: Overview of selected support for increasing resilience in the drinking water sector, related to the legislation

Legal act	General advice	Other written advice, including checklists, databases, web tools	Training, conferences
Act on Municipal and County Council Measures prior to and during Extraordinary Events in Peacetime and during Periods of Heightened Alert (2006:544)		Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure [69] (MSB) Systematic efforts to protect socially important business – Support for risk management, continuity management and to manage events (MSB) *[73]*	Web support Various conferences and seminars Maps Statistics Major exercises Advice in terms of learning from events, how to conduct a systematic safety work, public procurement
Rule of municipalities' risk and vulnerability analyses (MSBFS 2015:4)	Include general advice	Guide to Risk and Vulnerability Analysis (MSB) [67]	See above
Rule on drinking water (SLVFS 2001:30)	Guidance for drinking water (NFA, 2014)	Risk and vulnerability analysis for drinking water supply (National Food Agency) [60]	Drinking water training – disinfection, hygiene, risk analysis Training for the (SWA)

Legal act	General advice	Other written advice, including checklists, databases, web tools	Training, conferences
Rule regarding measures to be taken in regard to sabotage and other damage to drinking water facilities (LIVSFS 2008: 13)	Guidance for drinking water (NFA, 2014)	Crisis Management for drinking water (National Food Agency) [62] Exercise handbook drinking water producers (National Food Agency) [63] Web based advice in case of an accident at a water source (National Food Agency) www.livsmedelsverket.se	
Rules and advice for protection of certain objects, information and material (PMFS 2015:3)	Include general advice	Checklist for SCADA security (National Food Agency), www.livsmedelsverket.se Guidance to improved safety in industrial information and control systems (MSB) [94]	Training course in information security (MSB)

Increasing resilience: support provided

In the following, focus is on a limited number of the resources mentioned above; resources that briefly describe the support provided in a number of areas that are most relevant to the production and distribution of safe drinking water in sufficient quantities. The first part is on the support provided by MSB, followed by the Security Services and then the specific support provided by the National Food Agency, the County Administrative Boards and the Swedish Water and Wastewater Association.

Overall emergency management support

MSB has identified relevant legislation, sponsored R&D, produced guidance for various assignments and has developed a relevant training concept. MSB has developed a model for sectoral agencies (such as the National Food Agency) assignments with sectoral plans. MSB also, together with sectoral and regional agencies, report the experiences from major disturbances in a number of sectors, such as drinking water. MSB has several activities that support the implementation of related legislation:

1. The agency has an activity relating to information security issues that aims to increase quality and measurability of indicators. Important topics include confidentiality, appropriateness, access, possibility to track disturbances and measurements that are well anchored among actors.
2. MSB provides advice and training for both risk and vulnerability analysis and for information security issues.
3. The agency supports and indicates interorganizational collaboration as a national resource in crisis and emergency management.

In an action plan [69], MSB provides an overview of the emergency management policy arena in Sweden, outlining relevant policy areas, goals, actors and policy instruments (legislation, monetary incentives and knowledge management activities). The overall principles are a) that the same organizations that are responsible for a critical infrastructure in normal operations are also responsible for managing the infrastructure in crisis situations and b) that crisis preparedness and management needs to be integrated in existing management processes. Emergency preparedness should use a systematic perspective, encompassing the whole life cycle of events and all kinds of events. The agency suggests using ISO 31000 for risk management and ISO 22301 for continuity management. MSB has also developed a guide to risk and

vulnerability analyses [67] for both municipalities and county councils. In the guide, MSB has listed the most commonly used methods for risk analysis, both quantitative and qualitative. Some of them are listed in Table 13 in Annex 2.

In a handbook [73], MSB provides concepts, terminology, checklists, and standards for the different functions as well as how various components in the systematic work towards increased resilience are related to standards, regulations and rules (Regulation 2015: 1052, MSBFS 2015:3, 4 and 5) and indicators used to assess and stimulate their application.

In cooperation with sectoral agencies, MSB has begun to develop a model with performance goals for various CIs, including drinking water supply [93]. The intention is that goals should stimulate actors to provide means to increase emergency preparedness. So far, the performance goals are vague and related to customer supply, not to production or distribution.

- Taking measures to reduce the risk for major disturbances in drinking water supply
- Those disturbances that do occur do not influence other CIs such as healthcare, sewage etc.
- Minimum levels of supply for individuals

In 2015, MSB suggested that the performance levels could be supplemented with "temperature meters", which could be used for a continuous assessment and evaluation of different actors' capacities and efforts in order to reach the performance levels [97]. For example:

- If there is emergency water and how much in relation to users' needs
- The proportion of households who in case of a disturbance has received potable drinking water within 24 hours
- The capacity for emergency water per person within the municipality

It seems that the performance levels could be compared to the SmartResilience "issues", and the "temperature meters" to indicators to be developed in SmartResilience.

The drinking water sector

In a handbook for risk and vulnerability analysis [60] the Food Agency has compiled advice and guidance for responsible bodies within drinking water production [65] as well as rules and methods for analysis and operational planning regarding water distribution. The methods include HACCP (Hazard Analysis and Critical Control Points), Water Safety Plans (WSP), risk and vulnerability analysis and security analysis. Moreover, the Food Agency has produced several brochures and handbooks that provide detailed advice for both risk and vulnerability analyses as well as emergency preparedness, emergency management and exercise. The Food Agency also publishes a climate adaptation handbook or drinking water producers, municipalities and county administrative boards regarding how to plan with regard to risks due to e.g. flooding. The agency provides emergency preparedness training.

The Food Agency coordinates VAKA, the national water catastrophe group, composed of personnel from the areas of drinking water production, environmental protection, laboratories and rescue services. The group supports cities and regions that have or might have urgent problems with (safe) drinking water supply. A network of experts within and outside of agencies continually advice and train the members of the group.

The Swedish Water & Wastewater Association (Svenskt Vatten, SWA) represents the interests of the municipalities in the whole field of municipal water and wastewater. The association's work includes:

- Compiling recommendations and guidelines for risk and vulnerability analysis for water protection areas,
- Arrange seminars and courses, such as in Microbial Barrier Analysis,
- Publish a journal, newsletter and reports,
- Initiate and sponsor research and development within the field.

The Swedish Water and Wastewater Association also compiles a database (VASS) related to the water utility sector. Using VASS, Bondelind et al. (2013) [13] developed performance indicators (PI) for water works, focusing on safe drinking water and present a method for evaluating drinking water safety.

Moreover, SWA has utilized the VASS database to construct an index, the Sustainability Index, as a means to assess the long-term sustainability of the water production facilities, primarily focused on the projected needs due to challenges that arise from climate change. The Sustainability Index is an expert/research based

approach, aimed at supporting municipalities with their work to secure safe drinking water. The experts have been developing the indicators during several years and a large number of municipalities have used it from 2014 onwards (124 municipalities participated in the survey for the Sustainability Index 2015).

A high rating on the Sustainability Index requires a documented knowledge of vulnerabilities and strategies and plans to secure sustainability in a longer term. The indicators include: healthy and safe water; water quality; supply assurance; water and waste water planning; climate change adaptation and flooding safety; high customer satisfaction; communication; economizing with non-renewable resources; energy savings; environmental demands; water availability; water and waste water equipment status; operational stability and; personnel resources and competences. According to an expert at SWA, the Sustainability index is intended as a tool for the members to use in respect to politics: explaining why they get a poor record, arguing for the need to increase capacity etc.

International guidelines and support documents are often taken into account and incorporated in the Swedish documents when found relevant. Since the quality of raw water source has historically been very good in Sweden and the load on the source relatively small, many of the problems faced by drinking water producers in other countries has not been an issue in Sweden. However, climate change and further urbanization may change this in the future.

Table 8: Overview of selected risk assessment techniques for drinking water in Sweden, provided by SWA and the Food Agency

Supporting method	Type of method	Source	Description	Comment
Microbial Barrier Assessment (MBA)	Method to assess the hygienic safety of the drinking water	(Bondelind et al., 2013) [13]	A simplified method that makes it easy for water and wastewater operators to evaluate their drinking water safety level	A good example of how to make user-friendly indication techniques
Quantitative Microbial Risk Assessment (QMRA)	Tool used to assess microbiological risks	www.dricks.chalmers.se	Used by Swedish water treatment facilities In Sweden, normally, a combination of local data, data from literature and a calculation tool developed for Swedish water facilities (QMRA-tool) is used.	Advocated by WHO, using combined data, including scientific data
Microbiological Barrier Analysis (MBA)	Tool used to assess microbiological risks	www.svensktvatten.se		Used by Swedish water treatment facilities
Water Safety Plans (WSP)	Work plan/Management system	www.svensktvatten.se (Davison et al., 2005) [21]	Developed by WHO Managing drinking-water quality from catchment to consumer	Developed by international experts Written for practitioners
HACCP (Hazard Analysis and Critical Control Point)	Management system	www.slv.se (Swedish National Food Agency, 2007)	Originally developed by NASA Well accepted within the Food Industry Included in SLVFS 2001:30 (Swedish drinking Water Rules)	Useful to look at because of its inclusion into rules

Sustainability Index	Assessment system	www.svensktvatten.se	A survey directed to municipalities	Designed by experts Using existing data A means to argue for investments and attention
Climate adaptation handbook	Handbook	www.slv.se Swedish National Food Agency	Guidance for how to plan for risks of flooding and contamination	Written by experts For non-experts

Support for security protection

MSB has an assigned role to support and coordinate IT-security work and to clarify how actors should follow-up, report and improve it. The Security Services has issued a guidance [82] related to legislation on protection against threats to national security, confidential information regarding national security and terrorism, see Act 2010:305 and related legislation. The legislation essentially aims to restrict unauthorized access. The guidance stresses the uncertainty and unpredictability of the causes and timing behind attempts to unauthorized access and therefore the need to focus preventive work on identifying and reducing vulnerabilities as well as continuously updating the actual threat scenarios. Thus, preparation requires an analysis of the probable ability and course of actions that a potential perpetrator might use and to establish a defence that is capable of withstanding these. The Security Services also provides personal advice regarding legislation; responsibilities as well as methods for security analysis, internal control, to increase security awareness and for personnel security screening.

MSB, NFA and SWA are the main actors providing support to the drinking water producers and suppliers on how to comply with the regulations even though the regulation from Security Services also gives advice on how to treat information security. The support provided by MSB, SWA and NFA is distributed as guidance documents and handbooks on how to organize the information and IT-security work giving written advice on procedures and structures to ensure that all important aspects are covered. NFA and MSB also engage in and organize exercises as a manner of supporting and pushing the concerned organizations to improve in this area.

The recommendations in these guides can be divided into categories handling organizational aspects, operating procedures and increasing technical system security. A majority of the recommendations are focused on precautionary actions.

Concerning ICT-security the most extensive support document provided by the Swedish authorities is the *Guide to Increased Security in Industrial Information and Control Systems* published by MSB in 2010 [94]. It contains 17 recommendations mainly based on international guidelines, standards and instructions from organizations such as North American Electric Reliability Council (NERC), National Institute for Standards and Technology (NIST), Centre for the Protection of National Infrastructure (CPNI) and International Atomic Energy Agency (IAEA). Each recommendation has a detailed description and the users are given further recommendations on how to work with all aspects within the recommendation as well as information on further reading.

SWA has also distributed a checklist to assess the work with industrial control systems security. It was released in 2012 and has a lot of similarities with the document from MSB. By answering questions concerning 64 control system security related actions the user gains an overview of the security work status.

In the document *Crisis management for drinking water* by NFA there is an entire section devoted to secure information giving advice on handling confidential information, security in office IT-systems and security in the industrial control system. It contains guidance on how to work with these issues and stresses the need for clear responsibility, requirements on procurements and to have standardised procedures and protocols for security when updating and restructuring the systems.

3 External influencing factors (legal acts) on assessing and increasing resilience

When assessing resilience or conducting measures to increase resilience, specific legal acts can influence the success of these actions. In specific, data protection rights are an important issue in all countries and can have crucial impact on the ability to collect data for assessing resilience.

Data protection legislation

Data protection legislation was also mentioned by SmartResilience practitioners regarding the question, which kind of legislation can be an obstacle for resilience assessments[4]. This includes confidentiality (e.g. assessment results cannot be shared with others), and freedom of information – for example, an energy provider who wants to collect data on energy consumption of households has to respect data protection regulations; or, if mass movements shall be monitored, the privacy rights of individuals have to be respected. Also (the avoidance of) classified information was mentioned as obstacle, when using data to assess resilience.

Further, on a higher level, platforms, centers, etc. for critical infrastructure protection that imply extensive sharing of data (e.g. EU-wide), require careful consideration of data protection rules. For example, the EU-FP7 project ECOSSIAN[5], which aimed at an Operator Security Operation Centre, has elaborated on data protection issues in detail.

On ***EU level***, current legal framework of data protection is laid out in Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 95/46/EC seeks a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the EU. It sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data. The Directive defines cases when data processing is lawful, including for example the cases that the data subject has unambiguously given his consent, or that processing is necessary, e.g. for the performance of a contract or for the performance of a task carried out in the public interest. When data is processed, this has to be done “fairly and lawfully”, and it is forbidden to process personal data revealing issues such as political opinions or sex life. Exemptions and restrictions to a data subject’s rights can exist in certain cases, e.g. in order to safeguard national security or the prosecution of criminal offences. Regarding the transfer of personal data from a Member State to a third country, the Directive defines respective cases when and how this is allowed or not [26].

The full text (as well as a summary) is available on the EU’s official website [26].

Further, *Directive 2002/58/EC* on privacy and electronic communications of 12 July 2002 addresses the processing of personal data and the protection of privacy in the electronic sector. It defines requirements for service providers to secure their services protecting personal data [27].

This legal framework of data protection is currently in a process of change: A comprehensive reform of data protection rules in the EU was proposed in January 2012 by the European Commission. It comprises a Regulation (Regulation (EU) 2016/679 – protection of natural persons with regard to the processing of personal data and the free movement of such data) and a Directive (Directive (EU) 2016/680 – protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data), which have entered into force in May 2016, while the Regulation shall apply from May 25, 2018, and the Directive is to be transposed into national law by the EU Member States by May 6, 2018. These new legal acts are a response to challenges from the digital age. They shall strengthen

[4] SmartResilience workshop April 24-26, Budapest

[5] ECOSSIAN - European COntrol System Security Incident Analysis Network, June 2014 – May 2017, http://ecossian.eu/

citizens' control over their personal data, and simplify the regulatory environment for business – and thus support the "Digital Single Market Strategy", which the European Commission has prioritized [34]:

Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), defines citizen's rights such as an easier access to their data that is processed, or a "right to be forgotten", i.e. the data shall be deleted when there is no longer a need to keep it. It further details rules for businesses, e.g. a guarantee that data protection safeguards are built into products and services from the earliest stage (innovation-friendly rules), or removal of notification obligations [31].

Directive (EU) 2016/680 aims to better protect individuals' personal data when their data is being processed by police and criminal justice authorities. It also aims to improve cooperation in the fight against terrorism and cross-border crime in the EU by enabling police and criminal justice authorities in EU countries to more effectively exchange information necessary for investigations. It includes key points on how the data is to be collected and processed (e.g. "lawfully and fairly", "adequate, relevant and not excessive", or "appropriately secured"). EU countries shall define time limits for erasing the personal data. Further, national authorities must take technical and organizational measures to ensure a level of security for personal data that is appropriate to the risk. Where data processing is automated, a number of respective measures must be put in place [32].

The new Regulation and Directive will repeal Directive 95/46/EC.

The use of data is crucial to assess resilience, and to identify gaps that require an improvement of CI resilience. Looking at the resilience cycle and its phases (see e.g. D1.2), this would affect the phases "understand risk" and "prepare". However, the identified gaps can belong to all phases of the resilience cycle. Hence, the availability of data is a crucial aspect for the resilience assessment and improvement of the CIs. Especially in cases of public infrastructures such as airports, where video surveillance is pertinent, the desired data basis can be restricted due to data protection regulation.

The new regulatory tool GDPR both strengthens the control of citizens over their personal data and simplifies the regulation environment for business, in order to support the "Digital Single Market Strategy" [34]. These two aspects need a balancing act to be able to ensure the objective of both, the support of resilience, safety, security on the one side, and privacy, protection of individual data on the other side. The commercial use of data has to be regulated, requiring consent of individuals. However, to get the consent of the public at large, for safety and security assessments, is a difficult aspect to address.

The EU-FP7 project CRISP[6] for example, has attempted to address this issue by means of a "Security, Trust, Efficiency and Freedom infringement (S-T-E-Fi)" method [20]. It proposes certification as an instrument to address security-related and societal needs. The certification is based on conformity assessment, which aims at overcoming the market imperfections [57]. Advantages of conformity assessment include for example preservation of quality, avoidance of damage and injuries, and reduction of risks [105]. Furthermore, it fosters trust [105]. However, this solution is not without challenges of fragmented markets within the EU [105]. The GDPR has addressed the issue of data protection certification mechanism in its articles 42 and 43 [34]. This could promote better compliance with legal obligations and promote transparency [20]. Similar instruments could bridge the gap between the individuals' data protection and resilience efforts for safe and secure CIs.

Regarding further effects of the (new) GDPR on the SmartResilience methodology, the case studies in WP5 might reveal additional issues to be considered and addressed. These issues will be included in the update of the SmartResilience Guideline (D3.6).

The ***German data protection law*** shall serve as an example for data protection legislation on national level:

Basic element of German data protection law is the *Federal Data Protection Act*, which entered into force in 1977, and has been updated several times since then. An update in 1990 included the right of individuals to decide on their personal data to be used, which means that it is up to each individual to determine what and

[6] CRISP - Evaluation and Certification Schemes for Security Products, April 2014 – March 2017, http://crispproject.eu/

how much personal information he or she would like to reveal. In 2001, the Federal Data Protection Act was revised in line with Directive 95/46/EC facilitating the exchange of data within the European Community [46].

Furthermore, on April 27, 2017 the German Federal Parliament adopted the new German Federal Data Protection Act (Bundesdatenschutzgesetz) ("new BDSG") to replace the existing Federal Data Protection Act of 2003. The new BDSG intends to adapt the current German data protection law to the EU General Data Protection Regulation (GDPR), which will become effective on May 25, 2018.

The Federal Data Protection Act is complemented by laws covering specific areas of data processing, such as the telecommunications industry and the activities of security authorities, and data protection laws on state ("Bundesländer") level. Besides the EC Data Protection Directive, other international data protection provisions have been incorporated into German data protection law, such as the Council of Europe Data Protection Convention and Art. 8 of the European Convention on Human Rights.

Objective of the BDSG is "to protect the individuals against his/her right to privacy being impaired through the handling of his/her personal data" [46].

The act applies to the collection, processing and use of personal data by

1. Public bodies of the Federation,
2. Public bodies of the states in so far as data protection is not governed by state legislation and in so far as they
   a. execute federal law or,
   b. act as bodies of the judicature and are not dealing with administrative matters,
3. Private bodies in so far as they process or use data by means of data processing systems or collect data for such systems, process or use data in or from non-automated filing systems or collect data for such systems, except where the collection, processing or use of such data is effected solely for personal or family activities [46].

The aspects from the act that are of consideration for SmartResilience are:

- For a CI operator, it is mandatory to get the consent from the data subject (i.e. the individuals) before collecting, processing or using the data.
- It states in Section 14 that the storage, modification or use of personal data shall be admissible where it is necessary for the performance of the duties of the controller, which can be a CI operator. In addition, clause 9 in this section states: "the data can be used if it is necessary for the conduct of scientific research, as long as the scientific merit of the research project substantially outweighs the interest of the data subject and when the research purpose cannot be attained by other means or thus can be attained only with disproportionate effort".
- The collection, storage, modification or transfer of personal data or their use by means of fulfilling one's own business (commercial purpose) shall be admissible. This can be the case when the need arises to safeguard the justified interest of the controller (i.e. the CI operator) of the filing systems and there is no reason to assume that the data subject has an overriding legitimate interest in his/her data being excluded from processing or use.

In general, the act protects the digital privacy of individual citizens, which may impede resilience assessment in real time if data about individuals is required. However, with the consent of the data subject or user, the data can be used for research and commercial purposes.

The *"technical and organizational checklist"* (German "Checkliste Technische und organisatorische Maßnahmen nach §9 BDSG, Annexe 1-3 – TOM") is one of three checklists which are used to evaluate the compliance with the BDSG. The checklists aim to implement and guarantee a good and legal data protection practice. Using these checklists, the appointed authority can evaluate the vulnerability of any specific facility regarding data protection. They can also be used in order to find ways for safety and resilience improvement. The "TOM-checklist" is attached to § 9 phrase 1 of the German federal data protection act (BDSG) [44] and is subdivided into 14 checklists, out of which three are seen relevant in this context. These checklists are regularly updated by the German "society for data protection and data security" (GDD e.V.) [67]. It follows a summary of these three checklists:

a. Checklist: physical access control (Zutrittskontrolle) [67]

The checklist physical access control concerns the physical location of areas, buildings and rooms, as well as the physical access by persons to these facilities. It addresses several issues of which the following are relevant to SmartResilience:

i. The possibilities to restrict physical access to specific areas, buildings or departments.
ii. The possibility of physical separation of specific departments (server-rooms, IT-departments etc.).
iii. The different possible weaknesses regarding physical entrance and their securitization (doors, windows, ventilation shafts, fire ladder etc.).
iv. The different possibilities of closing and opening regulation (Who has the keys, where are the keys, do backup-keys exist etc.).
v. Possible surveillance devices (audio video surveillance etc.).
vi. Definition and recording of physical access control (visitor or customer management etc.).

b. Checklist: entry control (Zugangskontrolle) [67]

This protocol aims to prevent the (electronic) access to data systems by unauthorized persons. It includes the following points (most relevant points have been chosen):

i. Password proceedings (minimal requirements, regular change, bios and boot passwords etc.).
ii. Other authentication measures (biometrics, chip cards etc.).
iii. Recording of login.
iv. Encryption.
v. Access from outside the intranet.
vi. Access to the internet.
vii. Used technology.
viii. Firewall.
ix. Use and frequency of penetration tests.
x. Admins (Who are admins, How do they work etc.).

c. Checklist: access control (Zugriffskontrolle) [67]

This protocol aims to guarantee that personnel can only access data that they are authorized to use and to avoid unauthorized reading, use, or copying of data. The protocol includes following points (most relevant points have been chosen):

i. Existence and application of a user access rights concept (concept, role attributions, differential access to data, applications, operational systems etc.).
ii. Data carrier administration (which and how much data carrier exists, how they are administrated).
iii. Data carrier destruction.
iv. Rules regarding data copying.
v. Bag search.
vi. Control of external maintenance.

Overall, the "TOM-checklists" provide detailed information on how to evaluate resilience and safety of SCIs regarding data protection. Furthermore, it helps to improve safety and resilience of the SCIs. The checklists have been developed based on known risks, safety concepts and experiences. Therefore, most of the points concern the second (anticipate/prepare) and third (absorb/withstand) phase, for example they are useful in order to be prepared for a wide range of possible incidents and helps the SCIs to be more robust. However, some of the content can also be useful in the fourth (recover/respond) and fifths (adapt/learn) phase, for example the recording of relevant information (possible surveillance devices; definition and recording of physical access control; recording of login or the use and frequency of penetration tests) can help to adapt and learn.

Even though data protection seems to dominate external influencing factors on assessing and increasing resilience, a few other aspects need to be mentioned:

While ***environmental legislation*** can encompass obligations regarding the resilience of specific critical infrastructure (cf. chapter 2), it can also hinder actions intended to enhance resilience of specific critical infrastructure. For example, an infrastructure that is not resilient can have negative impacts on the environment such as water contamination, which environmental laws try to avoid. On the other hand, actions that are actually meant to avoid negative impacts on the functioning of infrastructure, and thus to increase resilience, can also implicate negative impacts on the environment. As an example, non-renewable energy sources might be more resilient regarding a secure energy supply also during specific hazards events, but do more harm to their environment. Thus, respective environmental legislation has to be considered. Environmental legislation has also been mentioned by SmartResilience end-user partners[7] as being a possible hurdle when implementing actions to increase resilience.

[7] SmartResilience workshop April 24-26, Budapest

4 Internal influencing factors on assessing and increasing resilience (organizational requirements)

The success of resilience assessments and/or the implementation of resilience measures strongly depend on factors and structures within an organization, which can be supportive or obstructive.

The checklist in Table 9 does not claim to be exhaustive and most useful implications of its results can only be identified on a case by case basis. However, it can help to identify factors that can be improved in order to enhance the possibilities to successfully conduct resilience assessments and/or to successfully implement measures to increase resilience.

Respective issues are partly also represented in specific resilience indicators (WP4). However, representing required context factors for successful resilience assessment and actions, those issues that were described by practitioners are listed here. They can be grouped into topics on “staff + work process”, “tools”, “cooperation”, and “others”.

Table 9: Overview influencing organizational structures

Question	If Yes, the positive effect can be	Source
Staff + work process		
Is there specialized staff and/ or even a dedicated unit within the organization?	Dedicated place for knowledge, expertise, resources, and tools can ensure that the required resources are available	SmartResilience T3.1 workshop; Written feedback by SmartResilience End-User
Is there any training for responsible staff members on ▪ How to conduct resilience assessments? ▪ How to report assessment results? ▪ How to implement actions to increase resilience?	Improved abilities to conduct resilience assessments and to implement actions to enhance resilience	SmartResilience T3.1 workshop; Written feedback by SmartResilience End-User
Is there sufficient knowledge about realistic risks, criticality of infrastructure, and possible cascading effects?	Improved awareness	Written feedback by SmartResilience End-User
Do responsible staff members have expertise in the application of indicators?	Increased feasibility of resilience assessments	D1.3/ case study ECHO, p.38
Are resilience assessments integrated into company processes/ daily work?	Enhanced possibilities for assessments	D1.3/ case study HOTEL, p.54
Tools		
Is there a useful Decision Support System in place?	Improved abilities to implement actions to enhance resilience	SmartResilience T3.1 workshop
Are clear, practical and easy to use methodologies for resilience assessments known and available?	Improved abilities to conduct resilience assessments	SmartResilience T3.1 workshop; Written feedback by SmartResilience End-User
Are specific guidelines for specific areas known and available)	Improved abilities to implement actions to enhance resilience	SmartResilience T3.1 workshop
Do the existent IT systems allow to efficiently extract required data for resilience assessments?	Feasibility to gain relevant data without using too much time and man-power	D1.3/ SWH, p.25
Cooperation		

Question	If Yes, the positive effect can be	Source
Do confidentiality rules allow to share assessment results with other stakeholders	Improved possibilities of learning from each other	SmartResilience T3.1 workshop
Is the cooperation with other relevant stakeholders (e.g. police, fire brigade, armed forces) sufficiently in place?	Improved motivation; improved abilities to implement actions to enhance resilience	Written feedback by SmartResilience End-User
Does any exchange of experiences with similar actors take place?	Improved sharing of knowledge + increased motivation	D1.3/ case study ECHO, p.39
Others		
Can the resilience assessment be conducted without using sensitive data?	Enhanced possibilities to use available data	D1.3, p. 63,66
Is the amount of available data manageable?	Enhanced possibilities to select relevant data	D1.3, p. 63,66

Resilience assessment results included in regular reports of SCI operators

If results of resilience assessments are included in regular report of an SCI operator, this can serve as an indication of resilience assessments integrated in the daily work of SCI operators is in how far assessments are included in regular reports of the organization. Results of respective information provided by SCI operators[8] are summarized as follows.

Operator 1:

Resilience assessments are included in safety reports, which are reviewed once in 3 years.

Operator 2:

The “Major Emergency Management readiness” is appraised once in a year.

Operator 3:

The safety and security activities by clients are audited/ supervised once in a year by the operator, based on EU directives.

Operator 4:

Exercises are conducted, but a follow up leading to improvements is not undertaken. Looking at these exercises from the resilience perspective is seen as useful to address these issues. Thus, a regular system is not yet 100% developed, while real events are used to implement actions and assess improvements.

Operator 5:

Regular assessments are conducted, while TSM (“Technische Sicherheit Management”) certification and ISMS (Information Security Management System) certification are used as a basis. Further, a follow-up of exercises is planned, and assessments of real events take place.

[8] SmartResilience workshop April 24-26, Budapest

5 Ethical aspects of indicator-based resilience assessment

5.1 Introduction - unintended consequences of a resilience indicator

Unintended consequences caused by the application of resilience indicators can always occur and can hardly be anticipated. Nevertheless, some factors foster the chance of unintended consequences and, therefore, the knowledge of these factors raises awareness. Furthermore, taking into consideration the knowledge of different potential problems and having a continuing assessment / evaluation management cycle, the occurrence of unintended consequences can be reduced.

These considerations do not guarantee the "absolute absence" of unintended consequences caused by the application of resilience indicators, but do limit the unexpected consequences and their negative impacts. The following recommendations help to identify unintended consequences and to preclude their impacts. The fusion of science and application bridges the gap of misunderstanding and increases the quality of the Smart Resilience research and the resilience indicators created. According to the ethical standard (protocol) of this project, this has to be addressed as an ethical demand. In fact, the quality of resilience indicators is a requirement of an appropriate ethical standard as well. The ethical standard of Smart Resilience mainly focuses on the prevention of ethical issues before they can have their unintended impact. Therefore, an unqualified set of resilience indicators and/or their unqualified application and assessment have to be prohibited.

In this section, the different "*dimensions of resilience indicator quality*" are displayed and how they can influence the implications. All the factors introduced are unwanted and, consequently, threaten the values of knowledge [47]. This is not only because of the mere fact that incorrect data is taken for knowledge, but also for all the consequences entailed and further actions related to this misjudgment. Goode and Hatt stated: "An ethic is more than a presence of a basic value or values. It is also an injunction to action" ([47], p.21). What does this mean for the project Smart Resilience? This quote implies that ethic consists of two major components: (1) the presence of common quality values and procedures (such as explained in the ethics protocol of Smart Resilience) and (2) the keeping of the values in all actions & phases of research. According the quote, the researchers of Smart Resilience strive for high quality in research practice. To apply this theoretical "demand of quality" a certain number of actions and research practices are required in context of indicator-based resilience assessment. In this section, the authors will discuss the great relevance of indicator problems, which can cause ethical issues. This implies not only the already mentioned dimension of the quality of resilience indicators, but also the inaccurate application or use of it.

In section 5.2, the authors outline the benefits of resilience indicator research to introduce the positive effects of this methodology and introduce also negative side-effects. In section 5.3 diverse indicator problems are demonstrated as well as their ethical implications. The knowledge of these unintended ethical implications leads to a set of countermeasures (quality requirements) that are developed and explained at the end of this section. The quality requirements of resilience indicator assessment will help to reduce unintended indicator problems and prevent ethical implications.

5.2 Benefits of resilience indicators

Although, this section is focussing on ethical aspects and consequences caused by indicator-based resilience assessment, a short discourse of the benefits of resilience indicators shall increase the understanding of the use of this methodology, the understanding of the purpose of resilience indicators, and what they are describing. At the same time, the information about the benefits offers first insights of possible ethical concerns due to the methodology ("nature") of building indicators.

The benefits and negative ethical effects are linked in a combination of circumstances, which every user has to be aware of. Negative impacts of indicators narrow the benefits of indicators or even turn them into the opposite direction. However, the benefits of indicator-based resilience assessment are crucial for a better understanding of resilience.

As resilience can be characterized as a vague and multidimensional concept ([19], [81]), developing an indicator means creating "a measure for resilience [that] can be a step towards characterizing resilience in a particular context" ([81], p.4). In other words "creating an indicator" is an attempt to describe a "part of a complex system" in manner to derive conclusions about the status of this part; in this case, deriving a statement about the skill "resilience". *The main benefit is to make resilience measurable, therefore analyzable for developments, and further comparable among different risks but also as benchmark among different critical infrastructure.*

Another benefit of resilience indicators is to raise awareness about resilience in general and about which risk entities suffer a lack of resilience in particular (ibid). In context of e.g. urban areas and their critical infrastructures, this plays an important role due to the dependency of population on the services and products of critical infrastructure. The awareness and analysis of rather vulnerable parts are used to implement countermeasures and protect/mitigate disruptions. Therefore, current research allocates resources and knowledge to progress and to compare these to further research in future. The accomplished knowledge leads to improve or build resilience at best. In addition, this knowledge enables to monitor and evaluate performance, which is crucial to secure the social benefits for politics [81].

5.3 Factors of resilience indicator implication and their potential ethical implications

In context of the briefly introduction of the benefits (for further information see D1.1, chapter 2.2 Preliminary definition & concept of resilience), the potential problems arising with this methodology are discussed in the following section according three stages of the Smart Resilience research:

I. 5.3.1 Pre-research phase (preparation phase): addressing all stakeholders involved in the Smart Resilience research project
II. 5.3.2 Research phase: addressing all involved projects partners in the development of resilience indicators
III. 5.3.3 Application phase of resilience indicators: addressing all users of resilience indicators

In a last section 5.3.4 countermeasures are introduced to ensure the quality of resilience indicators and prevent misleading measurement of resilience causing severe ethical consequences by wrong basis of decisions.

5.3.1 Pre research phase: Conflict of interests and intentions of a resilience indicator

Scientific research is powered by a certain intention, usually depending on where it originates from, the research programme, involved partners and funding parties. In this sense, there is no objective research because already the choosing of the research scope implies a purpose and therefore a judgment of what is worth and what is not worth to be investigated [81].

The agreed and conducted type of research has a direct influence on how resilience can and is being understood. With regard to ethical aspects, intentions of the research need to be reviewed iteratively to understand the research process with its stakeholders. A key question, which one has to be aware of, is: Who initiated a research project and who benefits from the research regarding resilience indicators? If there is a political background, the research should lead to the ideal of social benefits and a maximised benefit for the society.

Additionally, the intention can also influence the process of creating a resilience indicator as well. Certain interests influence the availability of data sets, which are needed for the application of the resilience assessment. The researches can face two possible challenges: Firstly, data sets which are needed are hidden or inaccessible through mislead intentions. Secondly, the choice of data can be limited to certain interests and therefore influences the outcome of the research of resilience indicators. In the Smart Resilience project, different groups (of project partners) and therefore also different interests are coming together. Besides partners of academia, different research organizations, industrial partners and public bodies are working together on the research topic of smart resilience indicators. The expectations are concluded in nine case studies, which represent different critical infrastructures and the application and evaluation of smart resilience indicators in context of resilience decision making processes. Therefore, the interests (research goals) are described in a transparent manner. Nevertheless, the application of Smart Resilience developed

resilience indicators needs an open access to the data sets of the industrial partners. The success of the application will be dependent on the interests of the industrial partners, the availability of date, and the arrangement of the stress framework of the case studies. The amendment of partners in the project is an example of different incompatible interests.

The above mentioned interest "to raise awareness" can also function as an intention of a resilience indicator. However, in this case it needs to be considered that awareness of resilience as a preventive function of endangerments can lead to not intended inverted effects. This is termed as iatrogenic potential or iatrogenic consequences in the sense that "a preventive technique actually harms treated subjects" ([56], p.114). This label is primarily used in the context of medicine or psychology; however, connections can be derived to the concept of resilience as well. Questions can be asked like: Does an increased awareness of resilience emerge emotions of fear and insecurity in the population? In different studies, Wurtzbacher researched the correlation between objective and subjective security. He found out that there is no explicit correlation, in many cases, the evaluation of objective and subjective security even does not lead to similar results [106]. Therefore, "resilience awareness" should be part of operators and decision makers of smart critical infrastructures, who know about the methodology and benefits. To publish resilience indicator values requires additional explanation for non-professionals.

5.3.2 Research phase: Inaccurate resilience indicator methodology

Ethical concerns can also arise due to an inaccurate developed indicator or a lack of quality (see section 0.). Ethical impacts might consist of unintended consequences such as a loss of time and money because resilience indicator research implies high efforts of resources. If an inaccurate resilience indicator is not recognized as an inaccurate one, it leads to misinterpretation of the real situation and the investigated subject. Depending on the users *trust value of resilience indicators* in the decision-making process, wrong measures can be implemented and lead to a wrong policy application with more unintended consequences.

An inaccurate indicator can occur due to many reasons, such as *complexity*. Transferring a theoretical concept into an operational variable, an indicator, usually already implies simplifying the complexity of reality in order to make the subject measurable. This is especially the case with the concept of resilience as "resilience is inherently complex and with increasing complexity comes greater difficulties in establishing measures and interpreting results" ([81], p.13).

It becomes even more complex and fuzzy, because there is *no universally accepted definition of resilience*. The findings and results of diverse research studies are often not comparable or the comparison limited. Research studies need to clarify their (used) definition of the resilience concept and justify their way of operationalizing resilience through an indicator to counteract misunderstandings and their unintended consequences. Prior and Hagmann ([81], p.15) propose three considerations from a policy perspective to gain clarity of the resilience concept in a research study:

(1) A sound definition;

(2) explicit policy linked to the definition; and

(3) explicit articulation of scale and context.

The intentions, which influence what is being investigated, have to be put aside during the research process. This means a resilience indicator has to show the characteristic of being researcher *independent* in the sense of research results not being influenced by a researcher's preferences. Otherwise, research results are distorted by subjective preferences.

An inaccurate resilience indicator can also emerge due to research limitations. On the one hand, there is the complexity of resilience; on the other hand external circumstances are framing the research process. "Achieving the right balance" of the complexity of resilience and the given resources for the investigation, is a challenge, which has to be addressed in a specific research design. Nevertheless, resilience and its complexity are difficult to measure that can cause diverse indexes of an indicator (multiple indicators) [15].

Another issue of operationalizing resilience is *generalizability*, also referred as external validity. This term refers to "the assumption that the research can be transferred to other business contexts and situations" ([45], p.184). In general, research results depend on the specific context in which they were collected, so it is not possible to generalize them. To enable a higher degree of generalizability, researchers have to take care

to collect data in a most likely real context. This has to be considered as well as the fact that the constitution of resilience also "var(ies) dramatically between places and with respect to the events they are examined in relation to" ([81], p.14). As the concept of resilience is more understood as a *dynamic* process than a constitution with fixed features, measurement results can also differ at the same place over time. Consequently, a once accurate indicator measurement can turn into an inaccurate one through time and context differences. The degree of generalizability can be increased by the number of research replications conducted [22]. An example for a rather quick changing indicator is performance indicators of operating systems such as production lines. Due to different influencing factors (e.g. crisis event), these indicators can change quickly, while indicators about e.g. educational training of staff change rather slowly.

The fundament of resilience research (and research in general) is the data set (information) that the indicator reveals/concludes. If a resilience indicator is based on *wrong data sets*, the indicator itself will be inaccurate consequently and further all the assessment based on the indicator (*chain of failure*). For that reason, *credibility* of the used information needs to be guaranteed. *The credibility can be ensured by checking the data fundament for completeness, correctness, consistency and traceability*. In this context, the UN list refers to the aspect of completeness as "the data should be complete and free of missing values" ([103], p.7), whereas correctness means the data is free from error or fault. The term of consistency describes the data of being free from contradictions or convention breaks. Traceability as a sub-criterion of credibility ensures the possibility to trace back the whole research process and to check on its trustworthiness. To gain a high quality of data, it is presupposed that data is available and suitable (see section 0).

5.3.3 Application phase: No application possibility of the indicator

It can also be the case that according to circumstances a developed resilience indicator is accurate, but *no application* is conducted. This occurs for instance when there is no current need of it or the user does not see any relevance of it. If a decision maker does not know about the indicators relevance, there will be no application of the indicator although it might be accurate and relevant.

As a research study takes time to be executed, a future perspective has to be taken into account if the researched scope will remain crucial. The concept of resilience (e.g. in urban areas the increasing population numbers has become more and more relevant or certain threats like global warming or terrorisms [19]) has to be reflected in the manner of which aspects of resilience might be more urgent and therefore of more interest than others. This choice of relevance (prioritization) is part of all stakeholders dealing with resilience, such as research level (Smart Resilience), SCI operators or governmental agencies.

In addition, an application is also disabled if a developed indicator cannot be used by others due to a *lack of understanding*. This can be the case if researchers did not present their developed resilience indicator in a comprehensive way, or if the needed competence of researchers is not provided.

In a complex resilience system, there also might be no data available to execute the application of resilience indicators in such a way, that the results are sufficient. The *missing data* lead to a deconstruction of application possibilities.

5.3.4 Research and Application phase: Countermeasures to avoid unqualified indicator-based resilience assessment

In the following section, a set of countermeasures are provided to avoid the development of unqualified resilience indicators. "Unqualified" means in this context that the developed resilience indicators cause minor to major ethical consequences by the use in a smart critical infrastructure system. Although, the quality of research and its processes in Smart Resilience and in general are described in the Ethics Protocol, the following descriptions are focusing especially on indicator-based resilience assessment according to the project.

The Smart Resilience project uses a multi-layer approach to combine separated indicators according to issues which are clustered in dimensions, resilience phases, threats, and the critical infrastructure system (see D3.2). The quality requirements presented in this section are necessary to avoid unintended ethical implications. Although, the indicator requirements are also termed as quality criteria, they function also as a guideline to check on.

The Figure 1 outlines a set of indicator requirements, which can be used to evaluate the quality of a resilience indicator in the phase of indicator development and/or indicator application. To some extent, the listed indicator requirements correspond to a list of the UN ([103], p.7). The authors added other relevant criteria due to the specific demands of addressing "resilience indicators" and structured them as an overview. With the help of this quality criteria catalogue, the above discussed potential indicator problems can be encountered within the three dimensions:

(A) Intention of a resilience indicator,
(B) inaccurate resilience indicator and
(C) inapplicable resilience indicators.

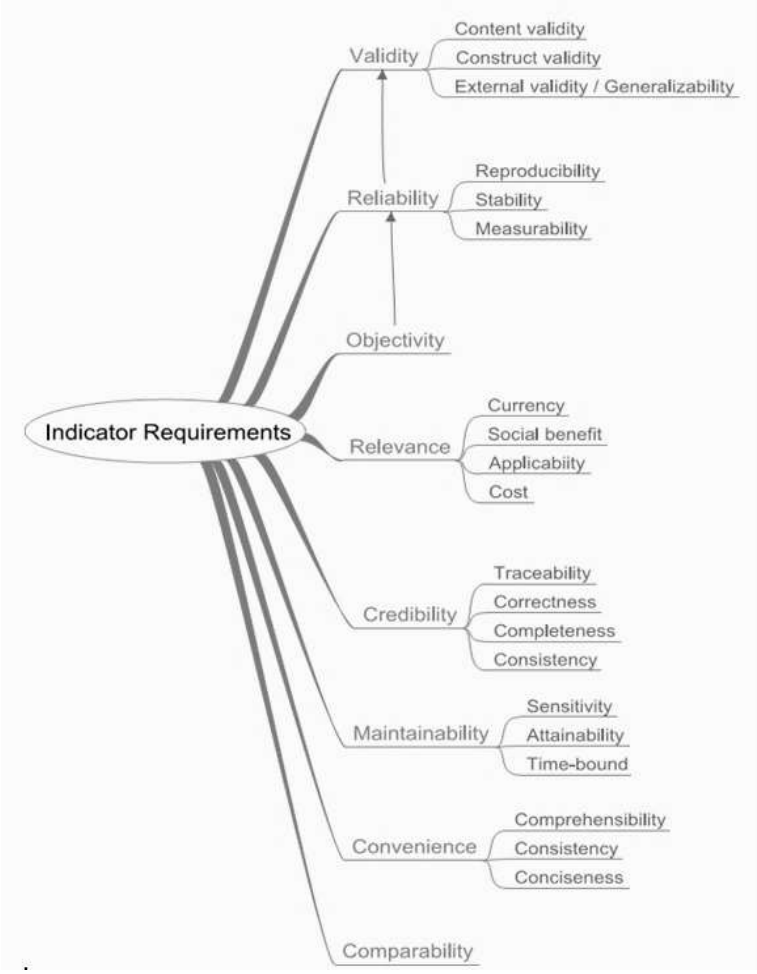

Figure 4: Quality criteria of resilience indicators (source: authors referring to [10])

The two dimensions of the intention behind a resilience indicator based research and inapplicable resilience indicators can be reviewed through the requirement of *relevance*. The authors define relevance by the sub-criteria *currency*, *social benefit*, *applicability* and *cost*. Social benefit refers to the outlined dimension of intention, as it is the ideal of a social benefit deriving from research. As mentioned above the question has to be answered, who will profit from a research project and by whom it is financially supported? The criterion of cost of the research has to be seen in relation to the expected benefit of the strived findings.

The two sub-criteria of relevance, *applicability* as "the characteristic […] to be directly useful in a given context" [25] and *currency* of the addressed research manner, help to ensure the effective utilization of a developed resilience indicator.

The criterion of *maintainability* also enables to lengthen the usability of a resilience indicator. Maintainability is consisting of *sensitivity*, *attainability* and *time-boundness*. Sensitivity refers to the aspect that "indicators should be able to reflect small changes in the things that the actions intend to change" ([103], p.7). In

addition, the criterion of *attainability* as "the measurement of the indicator which should be achievable by the policy or project and thus should be sensitive to the improvements the project/policy wishes to achieve" (ibid.) allow a broader scope of application. As *time-boundness* comes along with any resilience indicator, the time interval needs to be appropriate and clearly stated [103].

To avoid inapplicable resilience indicators due to a lack of understanding of a third party, *usability* has to be ensured by the criterion of *convenience* in context of the ease-of-use for others not involved of the research process. It is important that the data about a resilience indicator is comprehensive, consistent and concise. The description of a resilience indicator therefore needs to be expressed understandable, clearly and succinctly, free of contradiction and convention breaks.

The third problematic dimension referring to inaccurate resilience indicators can be addressed by the criteria of *objectivity, reliability, validity* and *credibility*. Objectivity, reliability and validity are fundamental of every research and probably the best-known quality criteria in the literature. These three quality criteria are hierarchically arranged [23] as shown in Figure 4.

Validity as the overall indicator requirement is preconditioned by *objectivity* and *reliability*. Validity can be defined "in a very general sense, that our propositions describe and explain the empirical world in a correct way; in a stricter sense: that they are free from random as well as systematic errors" ([92], p.22). This means in other words, the resilience indicator measures what it is supposed to measure. A distinction can be drawn between different types of validity. Objectivity and reliability as preconditions of validity ensure that research results are independent of the researcher and the research methods. An independence of research methods implies that the results are reproducible, stable and continued measurable.

The basis for every research project is the current *available data*. If the data consists of inferior quality or is even inconsistent, the resilience indicator will be inaccurate and misleading. Therefore, to ensure credibility of the data sources the characteristics of *traceability*, *correctness, completeness* and *consistency* have to be provided.

The listed quality criterion of *comparability* is not directly referring to one of the three dimensions of resilience indicator problems. Nevertheless, it is crucial for the progress in the field of resilience as it is defined by the UN as follows: "the indicator measurement should enable comparison over the different lifecycle stages of the policy or project as well as between different policies or projects" ([103], p.7). This criterion accelerates progress in research because outcomes of diverse research can be aligned, which generates a further understanding of the research matter.

5.4 Guideline and support

In the previous section 5, a range of indicator problems has been discussed as well as their ethical implications within the three dimensions: *intention of the resilience research, inaccurate resilience indicator and the case of no application*. The overall challenge of "*misjudgment*" causes consequences like wrong resilience policy. The separately outlined indicator problems constitute the diverse origins, from which this misjudgment arises. To avoid misjudgment of resilience indicators and ensure ethical standards, it is important to take potential indicator problems into account and to pursue a *high quality of research*. The quality of indicator-based resilience assessment can be enabled by indicator requirements. Indicator requirements serve as a basis of quality control, which should be followed to maintain the scientific character of a research process. Lastly, unintended consequences cannot all be predicted and/or prevented, nevertheless with the knowledge of potential indicator problems and indicator quality criteria, negative impacts of resilience indicator research can be reduced and limited.

A brief abstract of these quality criteria are provided in a checklist, which have been included in a first version of the SmartResilience Guideline.

6 Conclusion

Contextual factors are manifold and it is challenging to identify those that are “most relevant”. Especially when considering the legal background, the amount of legal acts with its different types, different sources, different addressees, different sectors targeted, is huge. The goal was to provide an overview of the existing legal framework without claiming to be comprehensive. However, it can serve as starting point and especially invites stakeholders from other countries and other sectors to use the provided description as starting point and motivation to check their respective legal framework.

Also the legal acts as “external influencing factors” on the assessment of resilience and/ or the implementation of measures to increase resilience might be extended, since the variety of possible measures is large.

The “internal influencing factors”, i.e. the organizational requirements, are mainly based on experience by practitioners involved in SmartResilience. However, other stakeholders might have different experience, and other factors might be added to the ones described.

Further, the described ethical considerations are seen as crucial for a valid resilience assessment, even though there is no overall rule on what to do if one or the other quality criterion is not fully met. It can only serve as basis for decision making – which indicators to take up, which not, and how to interpret the results.

First results of this report have already been summarized and transferred to the first version of the D3.6 “Guideline for assessing, predicting and monitoring resilience of SCIs”.

References

[1] American Petroleum Institute (2017). About API, http://www.api.org/about, accessed July 28, 2017.

[2] American Petroleum Institute (2016). Safety and Fire Protection, http://www.api.org/~/media/Files/Publications/Catalog/2016_catalog/07%20Safety%20and%20Fire%20Protection.pdf, accessed July 28, 2017.

[3] American Petroleum Institute (2010). API 754 – Factsheet for Process Safety Performance Indicators for the Refining and Petrochemical Industries

[4] American Petroleum Institute (2000). API RP 581 – Risk-Based Inspection Technology

[5] Barnett, J.; Lambert, S. & Fry, I. (2008). The Hazards of Indicators: Insights from the Environmental Vulnerability Index. In: Annals of the Association of American Geographers, Vol. 98 No.1, pp.102-119

[6] BMI – German Federal Ministry of the Interior (2005). Schutz Kritischer Infrastruktur – Basisschutz, available at http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2005/Basisschutzkonzept_kritische_Infrastrukturen.html?nn=3314962

[7] BMI (2007). Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen, available at http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.html?nn=3314962

[8] BMI (2009). Nationale Strategie zum Schutz Kritischer Infrastrukturen, available at http://www.bmi.bund.de/DE/Themen/Bevoelkerungsschutz/Schutz-Kritischer-Infrastrukturen/schutz-kritischer-infrastrukturen_node.html

[9] BMI (2011). Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, available at http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2011/leitfaden_schutz-kritischer-infrastrukturen.html?nn=3314962

[10] Brauner, F.; Claßen, M. & Fiedrich, F. (2017). Knowledge as enabler of urban infrastructure resilience. In: Fekete, A; Fiedrich, F. (Eds.) Urban Disaster Resilience and Security – Novel Approaches for Dealing with Risks in Societies, Springer (unpublished exsp. 2017)

[11] Barnes, R. A. (2013). The Capacity of Property Rights to Accommodate Social-Ecological Resilience, in: Ecology and Society, Volume 18, Issue 4.

[12] Bellamy. L. J. (2012). A literature review on safety performance indicators supporting the control of major hazards RIVM Report 620089001/2012, National Institute for Public Health and Environment, www.rivm.nl/bibliotheek/rapporten/620089001.pdf, accessed April 20, 2017.

[13] Bondelind, M., Pettersson, T., Malm, A., Bergstedt, O., Lindgren, J. (2013). VASS Dricksvatten - uppgifter, nyckeltal och modell för säkert dricksvatten för vattenverk (VASS Drinking water – data, performance indicators and a safe drinking water model for water works), SVU Rapport Nr 2013-15.

[14] Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2017). Internetplattform zum Schutz Kritischer Infrastrukturen, available at http://www.kritis.bund.de/SubSites/Kritis/DE/Home/home_node.html

[15] Cardona, O. D. (2005). Indicators of Disaster Risk and Risk Management. Summary Report, p.2-3. Washington D.C.: Inter-American Development Bank.

[16] Centre for Chemical Process Safety (2010). Guidelines for Process Safety Metrics. New Jersey: John Wiley & Sons, Inc.

[17] Centre for Chemical Process Safety (2011). Process Safety leading and lagging metrics, New York https://www.aiche.org/sites/default/files/docs/pages/CCPS_ProcessSafety_Lagging_2011_2-24.pdf accessed on 20.04.2017

[18] Clarke, J. et al. (2015). RESILENS – Realising European ReSILiencE for Critical INfraStructure. D1.1 Resilience Evaluation and SOTA Summary Report. http://resilens.eu/wp-content/uploads/2016/08/D1.1-Resilience-Evaluation-and-SOTA-Summary-Report.pdf, accessed June 08, 2017.

[19] Coaffee, J.; Clarke, J. & Rowlands, R. (2013). HARMONISE - A Holistic Approach to Resilience and Systematic Actions to make Large Scale Urban Built Infrastructure Se-cure. Deliverable D1.1 / Thematic findings report on state of current practice and state of the art, p.7-30.

[20] CRISP project (2014). Briefing paper for End-users, Netherlands, http://crispproject.eu/wp-content/uploads/2016/09/CRISP-End-users-FINAL-.pdf

[21] Davison, A., Howard, G., Stevens, M., Callan, P., Fewtrell, L., Deere, D., Bartram, J. (2005) Safety Plans: Managing drinking-water quality from catchment to consumer. WHO/SDE/WSH/05.06. World Health Organization, Geneva.

[22] Diaz-Bone/ Weischer (2015). Validität. Methoden-Lexikon für die Sozialwissenschaften. Springer, p. 421.

[23] Diekmann, A. (2012). Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen, p.247-261. Hamburg: Rowohlt Verlag GmbH.

[24] Engineering 360, Standard: ANSI/API STD 780, http://standards.globalspec.com/std/1603209/api-ansi-api-std-780.

[25] Eppler, M. J. (2006). A Framework for Information Quality Management. In: Managing Information Quality, 69-85. Berlin und Heidelberg: Springer.

[26] European Commission (1995). European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046, accessed July 24, 2017.

[27] European Commission (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058&qid=1496931684434, accessed July 24, 2017.

[28] European Commission (2012). Principles pf EU Environmental Law, Workshop on EU Environmental Legislations. Brussels, http://ec.europa.eu/environment/legal/law/pdf/principles/6%20Prevention_Precaution%20in%20other%20areas_revised.pdf, accessed March 08, 2017

[29] European Commission (2012). Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/ECText with EEA relevance, Brussels, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012L0018, accessed March 06, 2017

[30] European Commission (2014). Communication from the commission to the European parliament, the council, the European Economic and Social committee and the committee of the regions on an EU Strategic Framework on Health and Safety at Work 2014-2020, Brussels, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0332&from=EN, accessed March 09, 2017

[31] European Commission (2016a). Regulation (EU) 2016/679 — protection of natural persons with regard to the processing of personal data and the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG, accessed July 24, 2017.

[32] European Commission (2016b). Directive (EU) 2016/680 — protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG, accessed July 24, 2017.

[33] European Commission (2017a). Protection of critical infrastructure. http://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure, accessed July 31, 2017.

[34] European Commission (2017b). Protection of personal data. http://ec.europa.eu/justice/data-protection, accessed June 12, 2017.

[35] European Union (2006) Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH), http://ec.europa.eu/environment/chemicals/reach/reach_en.htm, accessed April 18, 2017.

[36] European Union (2008) Regulation (EC) No 1272/2008 of the European Parliament and of the Council of 18 December 2006 on classification, labelling and packaging of substances and mixtures, https://osha.europa.eu/en/themes/dangerous-substances/clp-classification-labelling-and-packaging-of-substances-and-mixtures, accessed April 18, 2017.

[37] European Union (2017) Regulations, Directives and other acts. Brussels, https://europa.eu/european-union/eu-law/legal-acts_en, accessed April 19, 2017.

[38] European Union (2017): Regulations, Directives and other acts. https://europa.eu/european-union/eu-law/legal-acts_en, accessed March 13, 2017.

[39] European Union Agency for Network and Information Security – ENISA (2013): The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems. ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013.

[40] Federal Republic of Germany (2006). TRBS 2152 - Technische Regel für Betriebssicherheit, Gefährliche explosionsfähige Atmosphäre – Allgemeines (technical rules concerning dangers related to explosions), BAnz. Nr. 103a; BArbBl. 8/9-2006, S. 36 ff., https://www.baua.de/DE/Angebote/Rechtstexte-und-Technische-Regeln/Regelwerk/TRBS/TRBS-2152.html

[41] Federal Republic of Germany (2007). TRBS 2141 - Technische Regel für Betriebssicherheit, Gefährdungen durch Dampf und Druck - Allgemeine Anforderungen (technical rules concerning dangers related to steam and pressure)., GMBl. Nr. 15 vom 23. März 2007, S. 327, https://www.baua.de/DE/Angebote/Rechtstexte-und-Technische-Regeln/Regelwerk/TRBS/TRBS-2141.html

[42] Federal Republic of Germany (2015). Verordnung über Sicherheit und Gesundheitsschutz bei der Verwendung von Arbeitsmitteln (Betriebssicherheitsverordnung - BetrSichV), 2015, https://www.gesetze-im-internet.de/bundesrecht/betrsichv_2015/gesamt.pdf, accessed April 21, 2017.

[43] Federal Republic of Germany (2016). TRBS 3146 - Technische Regel für Betriebssicherheit, Ortsfeste Druckanlagen für Gase (technical rules concerning dangers related to facilities containing gas) (2016), GMBl 2016 S. 854-880 [Nr. 44], https://www.baua.de/DE/Angebote/Rechtstexte-und-Technische-Regeln/Regelwerk/TRBS/TRBS-3146.html

[44] Federal Republic of Germany. Anlage (zu § 9 Satz 1), Bundesdatenschutzgesetz (BDSG).

[45] Frauendorf, J. (2006). Methodology. In: Customer Processes in Business-to-Business Service Transactions. Wiesbaden: Deutscher Universitäts-Verlag.

[46] German Federal Ministry of the Interior (2017). National data protection law. http://www.bmi.bund.de/EN/Topics/Society-Constitution/Data-Protection/data-protection_node.html, accessed June 13, 2017.

[47] Goode, W. & Hatt, P. (1952): Methods in Social Research, p.21-23. McGraw-Hill Book Company:

[48] Health and Safety Executive (2017), Control Of Major Accident Hazards Regulations 2015 (COMAH), UK, http://www.hse.gov.uk/comah/background/comah15.htm, accessed March 09, 2017.

[49] HSE (2006). Process Safety Indicators, A step-by-step guide for the chemical and major hazards industries, HSG 254. The Office of Public Sector Information, Information Policy Team, Kew, Richmond, Surrey http://www.hse.gov.uk/pUbns/priced/hsg254.pdf accessed on 13.04.2017 https://www.gesetze-im-internet.de/bdsg_1990/anlage.html

[50] International Association of Oil& Gas Producers (2011) Process Safety- Recommended Practice on Key Performance Indicators, Report 456 http://www.learnfromaccidents.com.gridhosted.co.uk/images/uploads/OGP_456_KPIs_for_Process_safety.pdf, accessed June 06, 2017.

[51] International Association of Oil& Gas Producers (2017). About us, http://www.iogp.org/about-us/, accessed July 28, 2017.

[52] International Association of Oil& Gas Producers (2015) Safety performance indicators-2015 data, http://www.iogp.org/bookstore/wp-content/uploads/sites/2/2016/10/2015se.pdf, accessed June 26, 2017.

[53] International Organization for Standardization (2017). ISO/IEC 27000 family – Information Security Management Systems, https://www.iso.org/isoiec-27001-information-security.html

[54] Jennings, K., & Schulberg, F. (2009). Guidance on developing safety performance indicators. Process Safety Progress, 28(4), 362-366. http://onlinelibrary.wiley.com/doi/10.1002/prs.10343/full, accessed April 20, 2017.

[55] Jovanovic, A., Quintero, F. and Choudhary, A. (2017). Use of safety-related indicators in resilience assessment of Smart Critical Infrastructures (SCIs). Submitted to ESREL 2017 - European Safety and Reliability Conference, June 18-22, 2017, Portoroz, Slovenia.

[56] Kimmel, A. (1998). Ethics and values in applied social research. California: SAGE Publications.

[57] Kamara. I. et. al. (2014). D4.1 Legal Analysis of Existing Schemes, Brussels, http://crispproject.eu/wp-content/uploads/2015/05/CRISP_WP4_D.4.1._Legal-analysis-of-schemes-30-April_.compressed.pdf

[58] Livsmedelsverket (2007). Operativa åtgärder vid vattenkris med nödvattenförsörjning – För insatspersonal (Operational measures in a water crisis with reserve water – for emergency personnel), Livsmedelsverket, Uppsala.

[59] Livsmedelsverket (2007). Risk- och sårbarhetsanalys för dricksvattenförsörjning (Risk and vulnerability analysis for drinking water supply), Livsmedelsverket, Uppsala.

[60] Livsmedelsverket (2007). Risk- och sårbarhetsanalys för dricksvattenförsörjning (Risk and vulnerability analysis for drinking water supply), Livsmedelsverket, Uppsala.

[61] Livsmedelsverket (2007). Strategi vid vattenkris med nödvattenförsörjning - För krisledningen (Strategy in a water crisis with reserve water– to crisis management), Livsmedelsverket, Uppsala.

[62] Livsmedelsverket (2008). Krishantering för dricksvatten (Crisis Management for drinking water) , Livsmedelsverket, Uppsala.

[63] Livsmedelsverket (2008). Övningshandbok för dricksvattenproducenter (Exercize handbook for drinking water producers), Livsmedelsverket, Uppsala.

[64] Livsmedelsverket (2014). Vägledning dricksvatten (Guidance – drinking water), Livsmedelsverket, Uppsala.

[65] Livsmedelsverket (2016). Information och råd till dig som är ansvarig för dricksvattenförsörjning (Information and advice to you as responsible for drinking water), Livsmedelsverket, Uppsala.

[66] Livsmedelsverket (2016). Nödvatten storstad.

[67] Münch, P. (2006), Checklisten zur Betriebsprüfung gem. § 38 BDSG, RDV 2006, 272, 280; Coaching Workshop Datenschutzpraxis, https://www.datenschutz-wiki.de/Kategorie:Checklisten, accessed April 21, 2017)

[68] Myndigheten för samhällskydd och Beredskap (2012). Guide to Risk and vulnerability analyses, MSB, Stockholm/Karlstad.

[69] Myndigheten för samhällskydd och Beredskap (2014). Action Plan for the Protection of Vital Societial Functions & Critical Infrastructure, MSB, Stockholm/Karlstad.

[70] Myndigheten för samhällskydd och Beredskap (2014). Övergripande inriktning för samhällsskydd och beredskap (Overall orientation for emergency preparedness), MSB, Stockholm/Karlstad.

[71] Myndigheten för samhällskydd och Beredskap (2014). Vägledning för samhällsviktig verksamhet. Att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid (Guidance for socially important business. Identifying socially important business and critical dependencies as well as acceptable recess time), MSB, Stockholm/Karlstad.

[72] Myndigheten för samhällskydd och Beredskap (2015). Processbeskrivning för uppföljning av kommunernas krisberedskap (Process description to follow up on municipal emergency preparedness), Dnr 2015-1370, MSB, Stockholm/Karlstad.

[73] Myndigheten för samhällskydd och Beredskap (2016). Systematiskt arbete med skydd av samhällsviktig verksamhet – Stöd för arbete med riskhantering, kontinuitetshantering och hantera händelser (Systematic efforts to protect socially important business – Support for risk management, continuity management and to manage events), MSB, Stockholm/Karlstad.

[74] Myndigheten för samhällskydd och Beredskap (n.d.). Öva krishantering: en handbook i att planera, genomföra och återkoppla övningar (Practicing crisis management: a handbook in planning, conducting and feedback exercises), MSB, Stockholm/Karlstad.

[75] Myndigheten för samhällskydd och Beredskap/Sveriges Kommuner och Landsting (2013). Ta ett samlat grepp – om trygghet och säkerhet (Make an overall concept – about safety and security). MSB and SKL, Stockholm/Karlstad.

[76] Naturvårdsverket (2003). Water protection areas – Handbook 2003:6 with general guidelines, Naturvårdsverket, Stockholm.

[77] OECD (2008). Guidance on Developing Safety Performance related to Chemical Accident Prevention, Preparedness and Response, Organization for Co-operation and Development, 2008, available at: http://www.oecd.org/dataoecd/6/57/41269710.pdf

[78] Petit et al. (2013). Resilience Measurement Index - An Indicator of Critical Infrastructure Resilience, Argonne, Argonne National Laboratory (ANL), http://www.ipd.anl.gov/anlpubs/2013/07/76797.pdf

[79] Polismyndigheten (2015). Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd, PMFS 2015:3 (Security Services rules and general advice), Polismyndigheten, Stockholm.

[80] Polismyndigheten (2015). Säkerhetsskydd – en vägledning (Security protection – a guidance), Polismyndigheten, Stockholm.

[81] Prior, T. & Hagmann, T. (2013). Measuring resilience: methodological and political challenges of a trend security concept. In: Journal of Risk Research

[82] Säkerhetspolisen (2010). Säkerhetsskydd – en vägledning (Guidance to security protection), Säkerhetspolisen, Stockholm.

[83] Säkerhetspolisen (2010). Säkerhetsskyddad upphandling – en vägledning (Security informed procurement), Säkerhetspolisen, Stockholm.

[84] SOU 2016:32 (2016). En trygg dricksvattenförsörjning – bakgrund, överväganden och förslag (A secure drinking water supply – background, deliberations and suggestions), Statens offentliga utredningar, Stockholm.

[85] Svenskt Vatten (2011). Råd och riktlinjer. Fysiskt och tekniskt skydd för dricksvatten (Advice and guidance on physical and technical protection for drinking water), Svenskt Vatten, Stockholm.

[86] Svenskt Vatten (2012). Säkerhetshandbok för dricksvattenproducenter (Safety handbook for drinking water producers), Svenskt Vatten, Stockholm.

[87] Svenskt Vatten (2013). Mikrobiologiska risker vid dricksvattendistribution - översikt av händelser, driftstörningar, problem och rutiner (Microbiological risks in drinking water distribution – overview of events, operational disturbances, problems and routines), Research report, Svenskt Vatten, Stockholm.

[88] Svenskt Vatten (2016). Råd och riktlinjer för ansvariga inom dricksvattenproduktion (Advice and regulations for responsible persons within drinking water production), Svenskt Vatten, Stockholm.

[89] Svenskt Vatten (2016). Råd och riktlinjer för ansvariga inom dricksvattenproduktionen (Advice and guidance for responsible persons within drinking water production), Svenskt Vatten, Stockholm.

[90] Svenskt Vatten (2016). Resultatrapport för hållbarhetsindex 2016 (Results for the Sustainability Index in 2016), Svenskt Vatten, Stockholm.

[91] Svenskt Vatten et al. (n.d.). Planera för dricksvatten – vårt viktigaste livsmedel (Planning for drinking water – our most important foodstuff), Livsmedelsverket, Uppsala.

[92] Swanborn, P. G. (1996). A common base for quality control criteria in quantitative and qualitative research. In: Quality and Quantity. International Journal of Methodology, 30, p.19-35. Netherlands: Kluwer Academic Publishers.

[93] Swedish Civil Contingencies Agency (2010). Förslag till resultatmål för samhällets krisberedskap för försörjningen av dricksvatten, livsmedel och värme (Suggested performance goals for public crisis management with respect to the supply of drinking water, food stuff and heating),), Swedish Civil Contingencies Agency, Karlstad.

[94] Swedish Civil Contingencies Agency (2014). Guide to Increased Security in Industrial Information and Control Systems, Swedish Civil Contingencies Agency, Karlstad.

[95] Swedish Civil Contingencies Agency (2014). Handlingsplan för skydd av samhällsviktig verksamhet (Action plan for protection of societal critical businesses), Swedish Civil Contingencies Agency, Karlstad.

[96] Swedish Civil Contingencies Agency (2014). *Nationell risk- och förmågebedömning 2016* (National risk and capacity assessment 2016), Swedish Civil Contingencies Agency, Karlstad.

[97] Swedish Civil Contingencies Agency (2015). Resultatmål. Förslag till målstruktur och mål inom fem områden (Performance goals. Suggested goal structure and goals within five areas). Swedish Civil Contingencies Agency, Karlstad.

[98] Swedish Civil Contingencies Agency (2016). A summary of risk areas and scenario analyses 2012–2015, Swedish Civil Contingencies Agency, Karlstad.

[99] Swedish Civil Contingencies Agency (2016). Kritiska beroenden, förmågebedömning och identifiering av samhällsviktig verksamhet. En studie av kommuners, länsstyrelsers och centrala myndigheters arbete med risk- och sårbarhetsanalys (Critical dependencies, capacity assessment and identification of societal critical businesses. A study of how municipalities, county administrative boards and central agencies work with risk and vulnerability analyses), Swedish Civil Contingencies Agency, Karlstad.

[100] Swedish Civil Contingencies Agency (2016). *Nationell risk- och förmågebedömning 2016* (National risk and capacity assessment 2016), Swedish Civil Contingencies Agency.

[101] Swedish Civil Contingencies Agency and Swedish Water and Wastewater Association (2010). Kartläggning av SCADA-säkerhet inom svensk dricksvattenförsörjning (Mapping of SCADA security within Swedish drinking water distribution), Swedish Civil Contingencies Agency and Swedish Water and Wastewater Association, Stockholm.

[102] Swuste. P. et. al. (2016). Process safety indicators, a review of literature. Journal of Loss Prevention in the Process Industries, 40, 162-173, http://doi.org/10.1016/j.jlp.2015.12.020

[103] UN/ISDR - United Nations Secretariat of the International Strategy for Disaster Reduction (2008). Indicators of Progress: Guidance on Measuring the Reduction of Disaster Risks and the Implementation of the Hyogo Framework for Action. Geneva.

[104] UN (2014). World urbanization prospects: The 2014 revision, p. 7-10. Department of Economic and Social Affairs, Population Division, New York.

[105] Wurster. S. et.al. (2017). Certified video surveillance systems for more resilience urban societies, Urban Disaster Resilience and Security, Springer, (under review).

[106] Wurtzbacher, J. (2003). Sicherheit als gemeinschaftliches Gut. Leviathan, 31(1), 92–116. https://doi.org/10.1007/s11578-003-0005-1

ANNEXES

Annex 1 Additional EU legal acts

Annex 2 Additional legal acts in Sweden

Annex 1 Additional EU legal acts

The following list of legal acts (Table 10) provides an overview on legal acts that have not been addressed in chapter 2.1, since they do not directly imply the described obligations, but still seem relevant in the context of resilience of SCI.

Table 10: Overview further legal acts on EU level not addressed in chapter 2.1

Legal act	CI Stakeholders mainly affected	Link to the complete act
Further Directives		
Directive on electricity production from renewable energy sources 2001/77/EC (superseded)	From energy sector	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l27035
Renewable energy directive 2009/28/EC	From energy sector	http://eur-lex.europa.eu/summary/EN/uriserv:en0009
Promotion of cogeneration based on a useful heat demand in the internal energy market (2004/8/EC CHP directive)	From energy sector	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004L0008
Energy efficiency directive 2012/27/EU	From energy sector	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:315:0001:0056:en:PDF
Environmental impact assessment (Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment)	From all CI sectors	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0092
Strategic environmental assessment (Directive 2001/42/EC)	From all CI sectors	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0042
Implementation of a Scheme for Greenhouse Gas Emission Allowance Trading Directive, amending Council Directive 96/61/EC (Directive 2003/87/EC of 13 October 2003)	From energy sector	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32003L0087
Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) (EC) No 1907/2006	From all CI sectors	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02006R1907-20140410
Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products	From oil/ petroleum sector	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:en0006; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0119
Decisions and Communications		

Legal act	CI Stakeholders mainly affected	Link to the complete act
Council and Commission Decision 98/181/EC, ECSC, Euratom of 23 September 1997 on the conclusion, by the European Communities, of the Energy Charter Treaty and the Energy Charter Protocol on energy efficiency and related environmental aspects	From energy sector	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31998D0181
Commission Decision 1999/819/Euratom of 16 November 1999 concerning the accession to the 1994 Convention on Nuclear Safety by the European Atomic Energy Community (Euratom)	From atomic energy sector	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31999D0819
Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the fight against terrorism [COM(2004) 702 final – Not published in the Official Journal].	From all CI sectors	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52004DC0702
Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal C 126 of 7.6.2007].	From all CI sectors	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52006DC0786
Communication from the Commission to the European Parliament and the Council: European energy security strategy (COM(2014) 330 final of 28.5.2014).	From energy sector	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014DC0330
Communication from the Commission to the Council and the European Parliament: Tackling crime in our digital age: establishing a European Cybercrime Centre (COM(2012) 140 final of 28 March 2012).	From all CI sectors	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52012DC0140
Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a general policy on the fight against cyber crime (COM(2007) 267 final of 22.5.2007)	From all CI sectors	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52007DC0267
Communication on the EU Strategic Framework on Health and Safety at Work 2014-2020	From all CI sectors	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2014:0332:FIN

Annex 2 Additional legal acts in Sweden

The following list of legal acts (Table 11) and guidelines/ support (Table 12) as well as support/advice provided by MSB (Table 13) complement those further described in chapter 2.3.

Table 11: Overview of selected legal acts in Sweden obliging stakeholders to assess/increase resilience for the drinking water sector

Legal act	Addressees	Stakeholders mainly affected	Link to the complete act	Note
Act on Municipal and County Council Measures prior to and during Extraordinary Events in Peacetime and during Periods of Heightened Alert (2006:544)	Municipalities and counties/regions	Municipalities and counties/regions, as well as others involved	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2006544-om-kommuners-och-landstings_sfs-2006-544	
Regulation about emergency preparedness and increased alert (2006:942)	National agencies	A large number of agencies charged with regulating critical infrastructures and those charged with running some critical activities such as the Police, the Military, Coast Guard, Customs etc.	http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2006942-om-krisberedskap-och-hojd_sfs-2006-942	
Regulation about crisis preparedness and measures to be taken by responsible agencies in times increased alert (2015:1052)	National agencies	A large number of agencies charged with regulating critical infrastructures and those charged with running some critical activities such as the Police, the Military, Coast Guard, Customs etc.	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20151052-om-krisberedskap-och_sfs-2015-1052	
Regulation with instructions for MSB (2008:1002)	MSB	MSB and those affected	http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20081002-med-instruktion-for_sfs-2008-1002	
Rule about national agencies' reporting of its incidents (MSBFS 2016:2)	National agencies	A large number of agencies as listed in regulation (2015:1052)	https://www.msb.se/externdata/rs/f21ae5f7-b655-4462-a2e6-9939b952a751.pdf	*Includes advice*

Legal act	Addressees	Stakeholders mainly affected	Link to the complete act	Note
Rule about national agencies' information security (MSBFS 2016:1)	National agencies	A large number of agencies as listed in regulation (2015:1052)	https://www.msb.se/externdata/rs/b74a7b16-36a5-4de8-8f15-1297c37f1324.pdf	*Includes advice*
Rule of counties' risk and vulnerability analyses (MSBFS 2015:4)	County councils/regions	All counties and regions	https://www.msb.se/externdata/rs/15e78831-767b-4714-9fa4-3b4fd0df92a8.pdf	*Includes advice and checklist/indicators*
Rule of municipalities' risk and vulnerability analyses (MSBFS 2015:5)	Municipalities	All of them	https://www.msb.se/externdata/rs/15e78831-767b-4714-9fa4-3b4fd0df92a8.pdf	*Including definitions of terms, checklist/indicators and advice*
Rule about national agencies' risk and vulnerability analyses (MSBFS 2016:7)	National agencies	A large number of agencies as listed in regulation (2015:1052)	https://www.msb.se/externdata/rs/2ef1b968-9b11-456e-bf99-77caad87bd92.pdf	*Includes advice and checklist/indicators*
Act on protection of certain objects (2010:305)	Public agencies that run certain critical activities (need for protection against terrorism, espionage, sabotage and robbery)	The military, municipalities, counties or to organizations otherwise in charge of these activities	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/skyddslag-2010305_sfs-2010-305	
Regulation on protection of certain objects (1996:633)	Public agencies that run certain critical activities (need for protection against terrorism, espionage, sabotage and robbery)	The military, municipalities, counties or to organizations otherwise in charge of these activities (referring to law 2010:305)	http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddsforordning-1996633_sfs-1996-633	

Legal act	Addressees	Stakeholders mainly affected	Link to the complete act	Note
Rule and advice for protection of certain objects, information and material (PMFS2015:3)	Public agencies that run certain critical activities (need for protection against terrorism, espionage, sabotage and robbery)	The military, municipalities, counties or to organizations otherwise in charge of these activities (referring to law 2010:305)	http://www.sakerhetspolisen.se/download/18.1beef5fc14cb83963e7c8b/1430826384590/Sakerhetspolisens_foreskrifter_allmanna_rad_sakerhetsskydd.pdf	Includes advice
Environmental code (1998:888) *Chapter 7*	Public agencies – municipal or regional	Protecting raw water sources	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/miljobalk-1998808_sfs-1998-808	
Act on generic water services (2006: 412)	Municipalities	To assure provision of water for larger settlements	http://www.notisum.se/rnp/sls/lag/20060412.htm	
Regulation on governance of the quality of the water environment (2004: 660)	EPA and water districts	EPA and water districts	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2004660-om-forvaltning-av_sfs-2004-660	
Rule and general advice about governance plans and program for measures for surface water (HVMFS 2015:34)	Municipalities and regions	Municipalities and regions	https://www.havochvatten.se/download/18.596b74d91518c04d181819b4/1450702376173/HVMFS+2015-34-ev.pdf	Includes advice
Food Act (2006:804)	Public agencies – municipal or regional – as well as private enterprises	Municipalities e.g. as drinking water producers and suppliers	http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/livsmedelslag-2006804_sfs-2006-804	
Regulation on food (2006:813)	Public agencies – municipal or regional – as well as private enterprises	Municipalities e.g. as drinking water producers and suppliers	https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/livsmedelsforordning-2006813_sfs-2006-813	
Rule on drinking water (SLVFS 2001: 30)	Municipalities	Those in charge for drinking water production and supply	https://www.livsmedelsverket.se/om-oss/lagstiftning1/gallande-lagstiftning/slvfs-200130	Includes 30 pages with detailed advice

Legal act	Addressees	Stakeholders mainly affected	Link to the complete act	Note
Rule regarding measures to be taken in regard to sabotage and other damage to drinking water facilities (LIVSFS 2008: 13)	Municipalities	Those in charge for drinking water production and supply	https://www.livsmedelsverket.se/globalassets/om-oss/lagstiftning/dricksvatten---naturl-mineralv---kallv/livsfs-2008-13-kons.pdf	The National Food Agency has separate guidelines for SLVFS 2001:30 and LIVSFS 2008:13, encompassing a 158 pages book

Table 12: Overview of guidelines and support for implementing resilience regulations for the drinking water sector

Legal act	General advice	Other written advice, including checklists, databases, web tools	Training, conferences	Investigation and research
Act on Municipal and County Council Measures prior to and during Extraordinary Events in Peacetime and during Periods of Heightened Alert (2006:544)		Make an overall concept – about safety and security (MSB) [75] Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure [69] (MSB) Process description to follow up on municipal emergency preparedness [72] (MSB) Guidance for socially important business. Identifying socially important business and critical dependencies as well as acceptable recess time (MSB) [71] Overall orientation for emergency preparedness (MSB) *[70]* Systematic efforts to protect socially important business – Support for risk management, continuity management and to manage events (MSB) *[73]* Practicing crisis management: a handbook in planning, conducting and evaluating exercises (MSB) [74]	Web support Various conferences and seminars Maps Statistics Major exercises Advice in terms of learning from events, how to conduct a systematic safety work, public procurement	National evaluation of risks and capacities (annually, MSB) Evaluation of specific events or projects (MSB)
Rule of municipalities' risk and vulnerability analyses (MSBFS 2015:4)	Include general advice	Guide to Risk and Vulnerability Analysis (MSB) [67]	See above	See above

Legal act	General advice	Other written advice, including checklists, databases, web tools	Training, conferences	Investigation and research
Rule on drinking water (SLVFS 2001:30)	Guidance for drinking water (NFA, 2014)	Information and advice to those responsible for drinking water (National Food Agency) [65] Advice and guidance for responsible persons within drinking water production (SWA)[89] Microbiological risks in drinking water distribution (SWA) [87] Guidance – drinking water (National Food Agency) [64] Risk and vulnerability analysis for drinking water supply (National Food Agency) [60] Planning for drinking water – our most important foodstuff (several agencies and organizations) [91]	Drinking water training – disinfection, hygiene, risk analysis Training for the (SWA)	Risk analysis from raw water to tap (SWA)
Environmental Code, chapter 7 on water protection areas	General advice about water protection areas (NFS 2003: 16) Rule and general advice about governance plans and program for measures for surface water (HVMFS 2015:34)	Water protection areas – Handbook 2003:6 with general guidelines (EPA)[76] Several handbooks from SWA – risk analysis, rules, etc.		
Act on generic water services (2006: 412)	Municipalities	Brochure from the counties	Links to other sources	
Rule regarding measures to be taken in regard to sabotage and other damage to drinking water facilities (LIVSFS 2008: 13)	Guidance for drinking water (NFA, 2014)	Strategy in a water crisis with reserve water– to crisis management (National Food Agency) [61] Operational measures in a water crisis with reserve water – for emergency personnel (National Food Agency) [58] Crisis Management for drinking water (National Food Agency) [62] Exercise handbook drinking water producers (National Food Agency) [63] Web based advice in case of an accident at a water source (National Food Agency) www.livsmedelsverket.se		

Legal act	General advice	Other written advice, including checklists, databases, web tools	Training, conferences	Investigation and research
Rules and advice for protection of certain objects, information and material (PMFS 2015:3)	Include general advice	Checklist for SCADA security (National Food Agency), www.livsmedelsverket.se http://www.svensktvatten.se/vattentjanster/dricksvatten/sakerhet-och-krisberedskap/scada-sakerhet/ Advice and guidance on physical and technical protection for drinking water (SWA) [85] Safety handbook for drinking water producers (National Food Agency and SWA) [86] Guidance to improved safety in industrial information and control systems (MSB) [94] Security informed procurement (Security Services) [83] Guidance to security protection (Security Services)[82]	Training course in information security (MSB)	

Table 13: Overview of advice and support related to risk analyses in Sweden, provided by MSB

Supporting method	Type of method	Source	Description	Comment
MVA – multidimensional activity analysis	Scenario-based method for analyzing the vulnerabilities and capabilities of organizations and activities	MSB (2012) [67] : Guide to Risk and vulnerability analyses (pp. 62-63)	Starting with actors own values and perspectives – using a risk analysis matrix (probability vs. consequence) – later developing into scenarios Finally, the scenarios are evaluated	Useful as a means to discover what stakeholders find worth preserving Useful to outline and evaluate possible scenarios and what needs to be done

ROSA method	Risk and vulnerability analysis	MSB (2012)[67]: Guide to Risk and vulnerability analyses (pp 63-65)	Focused on emergency management preparedness A risk management group is a specially constructed group that works with the risk management process. It is composed of representatives from different parts of the organization. The method also stresses that other work within the area should be included, that a continuous crisis management process is created, and that the work must be an integrated part of the actor's normal activities. The purpose of the method is above all to assess the actor's ability to manage an undesirable incident, as well as to provide a stimulus for work on crisis management issues. Three values for the vulnerabilities of a scenario: very good, good and poor	Useful to assess actors' capabilities Useful as input how to assess users' needs for T1.3 Can be adapted to specific circumstances, easy to use
IBERO method	Instrument for preparedness evaluation of area responsibility	MSB (2012) [67]: Guide to Risk and vulnerability analyses (pp 65-66)	The tool is scenario-based and supports the actors with area responsibilities in their work on analyzing the ability to withstand and manage undesirable incidents, as well as review the consequences of the incidents. The tool is also IT-based and can store a large amount of information from various actors. It also supports communication between actors.	Allows for evaluation of individual organizations as well as for several actors regarding the same incident – thus relevant for analyzing shared capacity or the effects of resilience to cascading effects Visualize effects of an incident to actors and to society