

Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Final report

Annex II

2 April 2019

This report has been prepared by EY and RAND Europe for the European Commission Directorate-General for Migration and Home Affairs (DG HOME).

Evaluation Study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

European Commission

Directorate-General for Migration and Home Affairs
Directorate D: Security

Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Final report

Annex II

***Europe Direct is a service to help you find answers
to your questions about the European Union.***

Freephone number (*):

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

More information on the European Union is available on the Internet (<http://www.europa.eu>).

Luxembourg: Publications Office of the European Union, 2020

PDF ISBN 978-92-76-19513-9 doi: 10.2837/70733 DR-03-20-377-EN-N

© European Union, 2020

Reproduction is authorised provided the source is acknowledged.

Table of Contents

INTRODUCTORY NOTES	1
IMPLEMENTATION TABLES VALIDATED BY THE POCS	3
IMPLEMENTATION TABLES NOT VALIDATED BY POCS.....	244

INTRODUCTORY NOTES

The following tables provide an overview of the transposition legislation individual MS have adopted to implement Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

The tables contain information on:

- List of **national measures** transposing and implementing Directive 2008/114 into the national legal system;
- **Definitions** of the terms "critical infrastructure", "European critical infrastructure", "risk analysis", "sensitive critical infrastructure protection related information", "protection", "owners/operators of ECI", and any other relevant national definitions;
- **Scope** of national measures, including sectors and sub-sectors in scope;
- **Identification** of ECI, as per Article 3 of the Directive;
- **Designation** of ECI, as per Article 4 of the Directive;
- **Operator Security Plans**, as per Article 5 of the Directive;
- **Security Liaison Officers**, as per Article 6 of the Directive;
- **Reporting obligations**, as per Article 7 of the Directive; and
- **Appointment of European critical infrastructure protection contact points**, as per Article 7 of the Directive.

The table also contains a section on the national CIP framework, including the scope of national CIP policy, responsibilities allocated to Ministries, bodies, and offices, responsibilities allocated to operators of national CI and other distinctive features of the national CIP framework.

The tables have been compiled by the Evaluation team through desk research of the transposition legislation and relevant literature, chiefly the Report performed in 2012 by Booz & Company: "*Study to support the preparation of the review of the Council Directive 2008/114/EC, Final Report*".

Once compiled, the tables were sent to the POCs of each MS, for validation and integration of information that was missing from publicly available documents. Not all PoCs responded. Implementation tables are therefore grouped in two clusters:

- **Implementation tables validated** covering 24 Member States:
 1. Austria
 2. Belgium
 3. Bulgaria
 4. Croatia
 5. Czechia
 6. Denmark
 7. Estonia
 8. Finland
 9. France
 10. Germany
 11. Greece
 12. Hungary
 13. Italy
 14. Latvia
 15. Luxembourg
 16. Malta
 17. Netherlands
 18. Poland
 19. Portugal
 20. Romania
 21. Slovakia

22. Slovenia

23. Spain

24. Sweden

- **Implementation tables not validated** covering three Member States:

1. Cyprus

2. Lithuania

3. United Kingdom

Note on Ireland: it was not possible to fill the Implementation table for the Republic of Ireland as the applicable transposition legislation does not describe how the Directive was applied in practice.

Information provided directly by the PoCs contained in the Implementation Tables is reported in **blue**, while information contained in national legislation or relevant literature is reported in black and cited accordingly.

IMPLEMENTATION TABLES VALIDATED BY THE PoCs

Austria

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	Directive 2008/14 is implemented <ol style="list-style-type: none">1. Through particular references within several already existing legal acts (such as the Criminal Code or the Security Police Act);2. Through the APCIP Masterplan 2014 (replacing the Masterplan 2008), which is based on a government decision and frames activities and measures to enhance resilience of national and European critical infrastructures based on a voluntary, legally non-binding public private partnership (PPP) approach.	
Definitions (Art 2)		
‘critical infrastructure’	CI are those infrastructures (systems, facilities, processes, networks or parts thereof) that are essential for the maintenance of important social functions and whose disruption or destruction seriously affects the health, safety or economic and social well-being of large parts of the population or the effective functioning of state institutions.	Austrian Program for critical infrastructure protection (APCIP Masterplan 2014) § 22 Abs. 1 Z 6 Security Police Act § 74 Criminal Code
‘European critical infrastructure’	Definition according to Article 2(b) of Directive 2008/114 is commonly used	
‘risk analysis’	n/a	
‘sensitive critical infrastructure protection related information’	n/a	
‘protection’	n/a	
‘owners/operators of ECI’	n/a	
Other relevant national definitions	n/a	
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Energy Sector – Electricity and Gas	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	Common responsibility of Federal Chancellery and Federal Ministry of the Interior	
Application of the procedure for the identification of ECI (as per Annex III)	<p>ECI are identified according to national procedures based on the APCIP Masterplan 2014 (replacing the Masterplan 2008). Within this process the following main criteria are considered:</p> <ul style="list-style-type: none"> • Time factor – impact within minutes/hours; • Type of impact – impact on security police; impact on lives/ health of people; • Extent of impact – impact on a vast number of people; • Redundancy – no/few comparative companies. <p>In addition to that the question of potential cross border effects were taken into account.</p>	
<i>Step1 – Application of sectoral criteria</i>	See above	
<i>Step 2 – Application of the definition of critical infrastructure</i>	See above	
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	See above	
<i>Step 4 – Application of the cross-cutting criteria</i>	See above	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	Basis for the definition of thresholds have been bilateral consultations between responsible national authorities and operators within the PPP-approach on CIP.	
Identification of potential ECI on an ongoing basis (Art 3.1)	<p>Identification of ECI was in principle completed in 2011.</p> <p>The list of eventual ECI and national CI (ACI) is updated on an annual basis.</p>	
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	Common responsibility of Federal Chancellery and Federal Ministry of the Interior	
Informing other MS which may be significantly affected of the identity	Responsible authorities in affected Member States were contacted via the CIP PoC network. Once contacts were identified, regular information exchange has been established by the responsible authorities in each affected nation.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
and reasons for designating a potential ECI (Art. 4.1)		
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	From the AT side, either CIP PoC or their responsible heads of department were engaged in bilateral discussions. Information exchange was conducted either during meetings or by using state of the art communication tools (mainly E-Mail)	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	Common responsibility of Federal Chancellery and Federal Ministry of the Interior (via nominated CIP PoCs); via E-Mail	
Agreement for the designation of the ECI (Art. 4.3)	As soon as the draft agreement is signed by the responsible national authorities	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	Common responsibility of Federal Chancellery and Federal Ministry of the Interior (via nominated CIP PoCs); via E-Mail	
Informing the owner/operator of the designated ECI (Art. 4.5)	Common responsibility of Federal Chancellery and Federal Ministry of the Interior (via nominated CIP PoCs). Bilateral Meetings with operators	
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	Federal Agency for State Protection and Counter Terrorism (which is part of the Federal Ministry of the Interior)	
Verification that the OSP or equivalent is in place	The commitment to establish high security standards in CI is part of the APCIP Masterplan 2014. Due to the PPP approach in Austria, the development of OSPs is guaranteed through a self-commitment of the operators and co-operation agreements. The review of the OSPs takes place in the context of regular personal meetings between the authority and the security officers of the ECI and physical checks. Furthermore, the authority develops their own OSPs for ECI to secure an efficient operating of police forces, when incidents occur.	APCIP Masterplan 2014
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	Federal Agency for State Protection and Counter Terrorism	
Function of the SLO (Art. 6.1)	The SLO is the contact point for authorities when it comes to establishing a security architecture, reporting incidents and regular meetings to strengthen a PPP-relationship built on trust	APCIP Masterplan 2014

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	The verification is carried out with the help of a database with all SLOs and their reachability. At least once a year, the authority contacts the SLO and also meets with him/her personally.	APCIP Masterplan 2014
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	The Austrian CI-Database provides contacts to all European and national CI SLOs. When it comes to a certain risk or threat or other important information regarding CI-protection, reports can be sent to all SLOs in question, also filtered by geographical or sectoral data. This early warning system also is based on an encrypted mailing system.	APCIP Masterplan 2014
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	Common responsibility of Federal Chancellery and Federal Ministry of the Interior.	
Performance of threat assessments within ECI subsector within one year following the designation of ECI	A risk analysis has been carried out within the energy sector, where the most relevant operators and responsible authorities have participated. This analysis is going to be evaluated yearly. Main content are cyber threats, a major blackout and increasing interdependencies. Furthermore, a threat assessment is carried out for each national asset of CI in Austria; this assessment is part of the Authority's Security Plans.	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	Types of risks encountered in the energy sector: <ul style="list-style-type: none"> - Terroristic/extremist attack - Sabotage by inside perpetrator - Sabotage by outside perpetrator - Vandalism - Burglary - Aircraft crash - Technical breakdown - Explosions and spatially related accidents - Nuclear accident, radioactive contamination - Fire within facility - Traffic accident - Earthquake: stronger than Richter Scale 6 - Flood, water damage, high flood - Landslide, avalanche, rock fall - Storm, pressure of snow or ice - Fire outside the facility - Geomagnetic disturbance - Cyber risks in general - Risks for ICT systems of energy systems - Increasing number of access points / Increasing complexity (Smart Meter, Smart Home, E-Cars, ...) 	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	PoCs are appointed by the Heads of Department responsible for Critical Infrastructure Protection within the Federal Chancellery and the Federal Ministry of the Interior	
MS body(-ies) serving as ECIP contact point	Federal Chancellery and Federal Ministry of the Interior are serving as EPCIP PoC	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures		
Scope of national CIP policy		
Sectors of critical importance	Energy, transport, ICT, finance, healthcare, water supply, food supply, chemical industry, constitutional institutions, rescue and operational services, research, social and distribution systems.	§ 22 Abs. 1 Z 6 Security Police Act § 74 Criminal Code
Number of national CI	Approx. 400	
Number of national CI operators	As an operator-based approach is followed, the number of operators corresponds to the number of national CI	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	Common responsibility of Federal Chancellery and Federal Ministry of the Interior	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	Have been identified through bilateral consultations between responsible national authorities and operators within the PPP-approach on CIP.	
Coordination of ministries, bodies and offices concerned	Common responsibility of Federal Chancellery and Federal Ministry of the Interior; regular consultation meetings between ministries and other bodies concerned take place (Advisory Board APCIP)	
Communication owners/operators with	Responsible Authority: Federal Agency for State Protection and Counter Terrorism. Communication takes place with regular meetings on a personal level	§ 22 Abs. 1 Z 6 Security Police Act

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	(building trust) and also via an early warning system (as described above in the chapter of the SLOs).	
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	Responsible Authority: Federal Agency for State Protection and Counter Terrorism. Background Checks are carried out by this agency and are possible for employees of CI who work in sensitive areas. CI inspections are also run by the Agency while developing Security Plans to guaranty efficient intervention of police forces.	§ 55b Security Police Act § 22 Abs. 1 Z 6 Security Police Act
Other relevant aspects of national authorities involved in CIP protection	n/a	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Operators have to name a security officer to the authority, but on a voluntary basis within the PPP-approach and regulated in co-operation agreements.	APCIP Masterplan 2014
- Preparation of a security plan	Operators have to prepare a security plan and discuss it with the authority, but on a voluntary basis within the PPP-approach and regulated in co-operation agreements.	APCIP-Masterplan 2014
- Review of the plan (timing)	The security plan is reviewed in a personal meeting once year, but on a voluntary basis within the PPP-approach.	APCIP Masterplan 2014
- Reporting incidents	Operators have to report severe incidents, but on a voluntary basis within the PPP-approach and regulated in co-operation agreements.	APCIP Masterplan 2014
- Exchange of information	Exchange of information takes place regularly, but on a voluntary basis within the PPP-approach and regulated in co-operation agreements.	APCIP Masterplan 2014
Other distinctive features of the national CIP framework		
- Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures	Main principles of APCIP are: <ul style="list-style-type: none"> • Operator based approach • Subsidiarity and voluntary commitment of companies • Complementarity • Confidentiality • Co-operation 	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
<ul style="list-style-type: none"> Channels used for information exchange 	<ul style="list-style-type: none"> Proportionality All-hazards-approach 	

Belgium

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	"Loi relative à la sécurité et la protection des infrastructures critiques"- 1er JUILLET 2011.	Moniteur Belge ; Number: 2ème édition ; Publication date: 2011-07-15
Definitions (Art 2)		
'critical infrastructure'	<p>"Critical infrastructure" means an installation, system or part thereof, of federal interest, which is essential for maintaining the vital functions of society, health, safety, security and well-being; economic or social life of the citizens, whose interruption of operation or destruction would have a significant impact due to the failure of these functions.</p> <p>"National critical infrastructure": Critical infrastructure located on Belgian territory, whose interruption of operation or destruction would have a significant impact in the country.</p>	1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 3 (modified by "Loi 2018-07-15/08, art. 41"); Article 13
'European critical infrastructure'	"European Critical Infrastructure" : means the national critical infrastructure whose interruption of operation or destruction would have a significant impact on at least two Member States of the European Union or a critical infrastructure that is not located on the Belgian territory but in another Member State of the European Union, whose interruption of operation or destruction would have a significant impact on at least two Member States of the European Union, including Belgium.	
'risk analysis'	"risk analysis" : identification of the main scenarios of potential threats of intentional acts intended to interrupt the operation of the critical infrastructure or to destroy it	
'sensitive critical infrastructure protection related information'	n/a	
'protection'	n/a	
'owners/operators of ECI'	"Operator" : any natural or legal person responsible for investments in or for the day-to-day management of a critical national or European infrastructure;	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Other relevant national definitions	<p>"DGCC": General Directorate of the Crisis Centre of the Federal Public Service of the Interior (<i>Direction générale Centre de Crise du Service public fédéral Intérieur</i>), in charge of the special protection of goods and services; persons and the national coordination in matters of public order;</p> <p>"OCAM": Coordinating body for the threat analysis (<i>Organe de coordination pour l'analyse de la menace</i>) instituted by the law of 10 July 2006 relating to the analysis of the threat;</p> <p>"Sectoral authority":</p> <ul style="list-style-type: none"> a) For the transport sector: the Minister responsible for Transport or, by delegation, the head of the personnel of his administration; b) For the energy sector: the Minister in charge of Energy or, by delegation, a senior member of the staff of his administration; c) For the finance sector: the Minister having Finance in his or her attributions or, by delegation, a senior member of the personnel of his administration; d) For the electronic communications sector: the Minister having Electronic Communications in his or her attributions or, by delegation, an executive member of the staff of his administration or a member of the Belgian Institute of Postal Services and Telecommunications. <p>"Other points of federal interest": Places that are not designated as critical infrastructure but which are of particular interest for the public order, for the special protection of persons and property, for the management of situations of emergency or for military interests;</p> <p>"Points of local interest": Places that are neither critical infrastructures nor other points of federal interest, but which are of particular interest for the execution of local administrative police missions and which could require the taking of protective measures by the bourgmestre;</p> <p>"Electronic communications": electronic communications covered by the law of 13 June 2005 on electronic communications;</p>	
Scope (Art 3.3)		
<p>Sectors and sub-sectors in scope:</p> <ul style="list-style-type: none"> - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports) 	<ul style="list-style-type: none"> - Transport sector - Energy sector (excluding nuclear) <p>The Energy sector comprises the following sub-sectors:</p> <ul style="list-style-type: none"> a) Electricity, consisting of infrastructures and installations for the production and transmission of electricity, for the supply of electricity; b) Petroleum, consisting of petroleum production, refining, treatment, storage and transport by oil pipelines; 	<p><i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 3</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>c) Gas, consisting of gas production, refining, treatment, storage, transportation by pipelines and liquefied natural gas terminals.</p> <p>The Transportation sector comprises the following sub-sectors:</p> <ol style="list-style-type: none"> 1) Road transport; 2) Rail transport; 3) Air transport; (<i>for which only specific provisions of the legislation apply</i>) 4) Inland navigation; 5) Deep sea and short sea shipping and ports. 	
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The sectoral authority (see list of definitions) identifies, for the sector under its jurisdiction, the critical national and European infrastructures	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 5</i>
Application of the procedure for the identification of ECI (as per Annex III)	<p>The sectoral authority conducts this identification after consulting the regions for potential critical infrastructure within their remit and, if deemed useful, representatives from the sector and potential critical infrastructure operators.</p> <p>The identification of the potential European critical infrastructures which cross all the stages of this procedure is communicated only to the Member States likely to be affected significantly by these infrastructures.</p>	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 5</i>
<i>Step1 – Application of sectoral criteria</i>	The sectoral authority establishes sectoral criteria to be met by the ECI in view of the particular characteristics of the sector concerned, in consultation with the DGCC and the involved regions. The sectoral authority shall apply to the list of identified national critical infrastructures the sectoral criteria. If the infrastructure meets these criteria, it shall be subject to the next step in the procedure.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 3 and Annex (section B, par I)</i>
<i>Step 2 – Application of the definition of critical infrastructure</i>	The sectoral authority applies the criteria in step 1, step 3 and step 4 to a list of infrastructures, previously identified during the procedure of identification of national critical infrastructure in the Annex, section A of the Law.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Annex (section B and section A)</i>
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	The sectoral authority applies the transboundary element of the definition of the critical European infrastructure referred to in Article 3 of the Law. If the infrastructure meets this definition, it is submitted to the next stage of the procedure.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition;</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		15/07/2011; Annex (section B, par. II)
<i>Step 4 – Application of the cross-cutting criteria</i>	<p>The sectoral authority applies the cross-cutting criteria referred to in Article 6 of the Law. In particular, the cross-cutting criteria to be met by the ECI are:</p> <ol style="list-style-type: none"> 1. The potential number of victims, in particular the number of dead or wounded, or 2. The potential economic impact, in particular the extent of the economic losses. and/or degradation of products or services, including the impact on the environment, or 3. The potential impact on the population, including the impact on public confidence, physical suffering and disruption of daily living, including the disappearance of essential services. <p>The cross-cutting criteria take into account: the severity of the impact and the existence of alternatives, as well as the duration of the shutdown / recovery.</p>	1er JUILLET 2011. — <i>Loi relative à la sécurité et la protection des infrastructures critiques.</i> Moniteur Belge; 2ème édition; 15/07/2011; Article 6 and Annex, (section B, par III)
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	<p>The sectoral authority establishes the impact levels or thresholds applicable to the cross-cutting criteria to be met by the European critical infrastructures, in consultation with the DGCC and, where appropriate, after consulting the regions concerned.</p> <p>Incidence levels or thresholds for cross-cutting criteria are based on the severity of the impact of the interruption of operation or destruction of a given infrastructure. The sectoral authority shall establish, on a case-by-case basis, the impact levels or thresholds applicable to the intersectoral criteria to be met by the European Critical Infrastructure, in consultation with the DGCC, with the Member States concerned and, where appropriate, after consultation of the regions concerned.</p>	1er JUILLET 2011. — <i>Loi relative à la sécurité et la protection des infrastructures critiques.</i> Moniteur Belge; 2ème édition; 15/07/2011; Article 6 § 5
Identification of potential ECI on an ongoing basis (Art 3.1)	<p>The sectoral authority communicates the list of potential European critical infrastructures it has identified to the DGCC and, where appropriate, to the regions concerned</p> <p>Each sectoral authority shall proceed with the renewal of the identification process, for critical infrastructure within its sector, at least once every five years.</p>	1er JUILLET 2011. — <i>Loi relative à la sécurité et la protection des infrastructures critiques.</i> Moniteur Belge; 2ème édition; 15/07/2011; Article 7 (modified by "Loi 2018-07-15/08, art. 44");
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	The EPCIP contact point (DGCC - <i>Direction générale Centre de Crise du Service public fédéral Intérieur</i>) is responsible, in collaboration with the sectoral authority and, where appropriate, with the regions concerned, for bilateral or multilateral discussions with the Member States of the European Union concerned, both in	1er JUILLET 2011. — <i>Loi relative à la sécurité et la protection des infrastructures critiques.</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>terms of infrastructure of potential ECI identified on Belgian territory as those identified by the other Member States on their territory.</p> <p>When an agreement has been reached on the identification of European critical infrastructures in Belgium, the sectoral authority designates these infrastructures after consultation with the DGCC and, where appropriate, after consulting the regions concerned</p>	<i>Moniteur Belge; 2ème édition; 15/07/2011; Article 7</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	DGCC is responsible for informing the other MS.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 7 § 2</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	The DGCC is responsible, in collaboration with the sectoral authority and, where appropriate, with the regions involved, for bilateral or multilateral discussions with the MS concerned, regarding both potential European critical infrastructures identified in Belgium and those identified by other Member States on their territory.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 7 § 2</i>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	DGCC informs the EC about the wish to engage in bilateral / multilateral discussions. This is done through meetings / exchange of letters / emails /etc.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011</i>
Agreement for the designation of the ECI (Art. 4.3)	The sectoral authority designates national critical infrastructures, after consulting the DGCC and, where appropriate, after consulting the regions concerned	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 7</i>
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	-	
Informing the owner/operator of the designated ECI (Art. 4.5)	The sectoral authority shall notify the operator of the reasoned decision to designate its infrastructure as a critical infrastructure and shall send a copy of this decision, indicating the date of notification to the DGCC.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 8</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	Without prejudice to the powers of judicial police officers, an inspection service by sector or, where appropriate, by sub-sector, is set up to monitor compliance with the provisions of this Act and its decrees on the part of the operators of that sector or sub-sector. The King designates, for a given sector or, where appropriate, by sub-sector, the inspection service competent to carry out the inspection.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 24</i>
Verification that the OSP or equivalent is in place	The operator/owner of the ECI is responsible for organising and updating of the OSP according to the lessons learned from exercises or any modification of the risk analysis.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 13; § 6 and Article 24</i>
Verification that the OSP or equivalent is appropriately and regularly reviewed	The designated inspection service can: <ol style="list-style-type: none"> 1. Enter without prior warning, on presentation of their IDs, in the premises of the operator of the critical infrastructure subject to their control 2. Obtain a copy of the OSP and any act, document or other source of information necessary for the exercise of their mission; 3. Carry out any examination, control and hearing and to request any information they deem necessary for the performance of their duties. 	
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The critical infrastructure operator shall designate a SLO and communicate the contact data to the Sector Authority within six months of notification of the designation as Critical Infrastructure, as well as after each update of these data.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 12</i>
Function of the SLO (Art. 6.1)	The SLO acts as a point of contact vis-à-vis the sectoral authority, the DGCC, the bourgmestre and the police services for any question related to the security and protection of the infrastructure	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 12</i>
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	Where a SLO already exists under national or international provisions applicable in a sector or sub-sector, the operator of a critical infrastructure shall communicate the contact details to the sectoral authority.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 12</i>
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	The DGCC, the police services and the OCAM exchange information useful for taking external measures to protect critical infrastructures. The SLO has to be available at any time.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 12§ 3;</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	The crisis enter is reachable 24/7 for stakeholders in the exchange of information or measures regarding the protection critical infrastructures.	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	DGCC (Direction générale Centre de Crise du Service public fédéral Intérieur)	1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 2
Performance of threat assessments within ECI subsector within one year following the designation of ECI	Within 9 months of notification of the designation of an infrastructure as a critical infrastructure, the DGCC receives a threat analysis from OCAM (<i>Organe de coordination pour l'analyse de la menace</i>) for the infrastructure and for the sub-sector to which it belongs.	1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 15
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	Every 2 years a report is being send from the Belgian CIP POC, to the European Commission, per subsector. The last report has been submitted in January 2017, so the next will be in January 2019.	1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 10
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The DGCC is designated, by the law of 2011, as the national contact point for the protection of European critical infrastructures, for all sectors and sub-sectors. Sectors, for Belgium in its relations with the European Commission and the Member States.	1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 2
MS body(-ies) serving as ECIP contact point	DGCC	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	"Loi relative à la sécurité et la protection des infrastructures critiques"- 1er JUILLET 2011	Moniteur Belge ; Number: 2ème édition ; Publication date: 2011-07-15

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	The Belgian national approach to CIP is spelled out in the national transposition law for Directive 114/2008. The overarching objective is to prevent each event that causes damage to the infrastructure or a part of it.	
Scope of national CIP policy		
Sectors of critical importance	<ul style="list-style-type: none"> a) Transport sector: b) Energy sector c) Finance sector d) Electronic communications sector 	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 3</i>
Number of national CI	n/a	
Number of national CI operators	n/a	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	Sectoral authorities are responsible for the protection of national CI	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011;</i>
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	The process regarding the identification and designation of national CI is the same adopted for the ECI. The sectoral authority establishes sectoral and cross-cutting criteria in collaboration with the DGCC and, where appropriate, after consulting the regions concerned. The list of potential CI has to be communicated to the DGCC and regions concerned.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011;</i>
Coordination of ministries, bodies and offices concerned	Sectoral authorities (see definitions above), together with OCAM	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011;</i>
Communication with owners/operators	The sectoral authority notifies the operator concerning the designation and shall send a copy of this decision, indicating the date of notification to the DGCC.	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011;</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	The DGCC shall inform the mayor of the municipality in whose territory the critical infrastructure of this designation is located	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011;</i>
Other relevant aspects of national authorities involved in CIP protection	n/a	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Appointment of a SLO as illustrated above	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011;</i>
- Preparation of a security plan	<p>The operator/owner of a CI has to develop a OSP that comprise at least:</p> <ul style="list-style-type: none"> - Permanent internal security measures, to be applied in all circumstances; - Gradual internal security measures to be applied according to the threat. <p>The procedure for drawing up the OSP shall include at least the following steps:</p> <p>a) the inventory and location of the points of the infrastructure which, if affected, could cause the interruption of its operation or its destruction;</p> <p>b) a risk analysis, consisting of an identification of the main scenarios of potential threats of acts intended to interrupt the operation of the critical infrastructure or to destroy it;</p> <p>c) an analysis of the vulnerabilities of the critical infrastructure and the potential impacts of the interruption of its operation or its destruction according to the various scenarios selected;</p> <p>d) for each scenario of the risk analysis, the identification, selection and prioritisation of internal security measures</p>	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011;</i>
- Review of the plan (timing)	The plan has to be drawn up within one year after the notification of the designation and the operator/owner of the CI should applied the internal security measures within 24 months	<i>1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 13</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
- Reporting incidents	In accordance with the modalities determined by the Minister of the Interior, the SICAD warns the DGCC of any event of which it is aware and which is likely to threaten the security of the critical infrastructure.	1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 14 § 2
- Exchange of information	When an event occurs likely to threaten the safety of the critical infrastructure, the operator is obliged to immediately notify SICAD (<i>service d'information et de communication de l'arrondissement</i>), via the emergency numbers 101 or 112, the service designated by the sectoral authority and the DGCC	1er JUILLET 2011. — Loi relative à la sécurité et la protection des infrastructures critiques. Moniteur Belge; 2ème édition; 15/07/2011; Article 14
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 		

Bulgaria

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<ol style="list-style-type: none"> 1. Disaster Protection Act 2. ПОСТАНОВЛЕНИЕ № 38 ОТ 18 ФЕВРУАРИ 2013 Г. за приемане на Наредба за реда за установяването и означаването на европейски критични инфраструктури в Република България и мерките за тяхната защита (DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection) 	
Definitions (Art 2)		
'critical infrastructure'	(new –SG 80/11, in force from 14.10.2011) "Critical infrastructure" shall be a system or parts thereof, which are essential for the maintenance of vital public functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would cause significant negative	Disaster Protection Act

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	consequences in the Republic of Bulgaria as a result of the failure to retain those functions.	
'European critical infrastructure'	(new –SG 80/11, in force from 14.10.2011) "European critical infrastructure" shall be the critical infrastructure, located on the territory of the Republic of Bulgaria the disruption or destruction of which cause significant negative consequences in at least two European Union Member States. The importance of the said consequences shall be assessed in terms of cross-cutting criteria - numbers of sites and injuries, economic and social consequences, taking into consideration effects resulting from cross-sector dependencies on other types of infrastructure.	
'risk analysis'	(new –SG 80/11, in force from 14.10.2011) "Risk analysis and assessment" shall mean the determination of the nature and extent of the risk as a function of the threat, vulnerability and probability.	
'sensitive critical infrastructure protection related information'	(new –SG 80/11, in force from 14.10.2011) "Information related to critical infrastructure protection" shall mean any fact relating to a critical infrastructure, which if disclosed and made public could be used to plan and/or act aimed at causing disruption or destruction of critical infrastructure sites, elements or installations.	
'protection'	(new –SG 80/11, in force from 14.10.2011) "Protection" shall be the set of activities aimed at ensuring the proper functioning, continuity and integrity of critical infrastructures in order to deter, reduce, mitigate and neutralise a threat, a risk or the vulnerability thereof.	
'owners/operators of ECI'	(new –SG 80/11, in force from 14.10.2011) "Owners/operators of European critical infrastructures" are natural persons, legal entities or organisations in charge of the investing, or for the proper functioning, the continuity and integrity of, a particular system or part thereof, designated as an ECI.	
Other relevant national definitions	Mentioned at the Additional provisions section of the Disaster Protection Act.	
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	I. Energy a) Electricity; b) Petroleum; c) Gas II. Transport a) Road transport b) Rail transport	<i>DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	c) Air transport d) Inland waterway transport e) Sea transport III. Information and Communication Infrastructure	<i>Bulgaria and the Measures for their Protection, Annex I</i>
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	Competent Ministries	<i>Disaster Protection Act, art.18 a)</i>
Application of the procedure for the identification of ECI (as per Annex III)	The identification of potential ECI shall be done following a particular procedure, composed by four steps	<i>DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 4</i>
<i>Step1 – Application of sectoral criteria</i>	Step 1 - initial selection of critical infrastructures in the sector concerned in accordance with sectoral criteria;	
<i>Step 2 – Application of the definition of critical infrastructure</i>	Step 2 - from the potential ECI identified in step 1, only the identified critical infrastructures shall be selected in accordance with the Disaster Protection Act;	
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	Step 3 - Selection of potential ECI under item 2 according to the definition of ECI contained in the Disaster Protection Act is made and the cross-sectoral criteria are applied.	
<i>Step 4 – Application of the cross-cutting criteria</i>	Step 4 - The cross-cutting criteria are: 1. potential number of perished or injured persons; 2. economic impacts - assessing the significance of economic losses and / or impaired quality of products or services, including possible environmental impacts; 3. public consequences - assess the implications for public confidence, physical suffering and disruption of everyday life, including the loss of basic services.	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	The thresholds for cross-sectoral criteria, determined on a case-by-case basis by the competent minister in agreement with the European Union (EU) Member States concerned, are based on the degree of disturbance or destruction of the infrastructure.	<i>DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 3(3)</i>
Identification of potential ECI on an ongoing basis (Art 3.1)	N.A.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	Competent Ministries	
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	The potential ECI is referred to as an ECI after reaching agreement with the EU Member States that may be significantly affected	<i>DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 5</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	The national Point of Contact together with the competent Ministry engage in discussion with other MS through organisation of bilateral meetings and visits. The exchange of information is via email.	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	The national Point of Contact (Minister of Interior)	<i>DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 3(3) – art. 8 (2)</i>
Agreement for the designation of the ECI (Art. 4.3)	There is an agreement between the competent authority and the other MS which could be potentially affected by the ECI. Moreover, they identify the threshold values for cross-cutting criteria	<i>DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 3(3)</i>
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The National Contact Point (Minister of Interior) informs the EC annually regarding: 1. The number of designated ECI per sector and the number of MS dependent on each designated ECI; 2. The number of infrastructures by sectors for which the thresholds of the cross-cutting criteria have been discussed.	<i>DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		Bulgaria and the Measures for their Protection
Informing the owner/operator of the designated ECI (Art. 4.5)	The respective Ministry notifies the owner/operator of the infrastructure for its designation as ECI. Information on the designation of an infrastructure as an ECI has the appropriate classification level according to the Protection of Classified Information Act (CIPA) and EU law.	DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 5
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The competent Ministry	ПОСТАНОВЛЕНИЕ № 18 ОТ 1 ФЕВРУАРИ 2011 Г. ЗА УСТАНОВЯВАНЕТО И ОЗНАЧАВАНЕТО НА ЕВРОПЕЙСКИ КРИТИЧНИ ИНФРАСТРУКТУРИ В РЕПУБЛИКА БЪЛГАРИЯ И МЕРКИ ЗА ТЯХНАТА ЗАЩИТА;
Verification that the OSP or equivalent is in place	The agreed OSP under shall be approved by the competent minister	
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The competent Ministry	
Function of the SLO (Art. 6.1)	The SLO shall immediately inform the competent Minister identifying hazards and risks for the relevant ECI.	DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 7
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	The competent Ministry ensures the control, which includes verification of existing of SLO.	DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 11 (1) p.2.

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	The information transmitted between the SLO, the owner /operator of the designated ECI and the relevant authority, has a level of classification under the CIPA and EU law.	DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 7 (3)
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	The competent Ministry	
Performance of threat assessments within ECI subsector within one year following the designation of ECI	Within one year after the designation of the ECI, relevant Ministry assesses the risks of the sub-sectors with ECI and exercises constant control.	DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 9
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The competent Ministry, every two years, through the contact point for the Republic of Bulgaria on the protection of the ECI, presents to the EC a report on the types of vulnerabilities, hazards and risks for the ECI sectors.	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The Minister of the Interior or an employee appointed by him/her shall be the contact point for the Republic of Bulgaria for the protection of the ECI. Moreover, the Minister of Interior or an employee appointed by him/her shall coordinate the issues of protection of the ECI in the Republic of Bulgaria with the other EU Member States and with the European Commission.	DECREE No 38 OF 18 FEBRUARY 2013 for the adoption of the Regulation on the Procedure for the Establishment and Designation of European Critical Infrastructures in the Republic of Bulgaria and the Measures for their Protection, Art. 8
MS body(-ies) serving as ECIP contact point	The Minister of the Interior	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	НАРЕДБА ЗА РЕДА, НАЧИНА И КОМПЕТЕНТНИТЕ ОРГАНИ ЗА УСТАНОВЯВАНЕ НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ И ОБЕКТИТЕ ИМ И ОЦЕНКА НА РИСКА ЗА ТЯХ (https://www.lex.bg/laws/ldoc/2135816878)	Обн. ДВ. бр.81 от 23 Октомври 2012г, изм. и доп. ДВ. бр.19 от 26 Февруари 2013г, изм. ДВ. бр.27 от 5 Април 2016г

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Scope of national CIP policy		
Sectors of critical importance	<p>Energy:</p> <ol style="list-style-type: none"> 1. Electricity 2. Petroleum 3. Gas 4. Heat energy <p>Transport:</p> <ol style="list-style-type: none"> 1. Road transport and road infrastructure 2. Rail and railway infrastructure 3. Air transport and airports 4. Water transport and ports <p>Information and Communication Technologies:</p> <ol style="list-style-type: none"> 1. Electronic communications networks 2. Information and Communication Infrastructure <p>IV. Post and courier services</p> <p>V. Environment</p> <ol style="list-style-type: none"> 1. Environment 2. Water, water supply and sewerage <p>VI. Agriculture and Food</p> <ol style="list-style-type: none"> 1. Agriculture 2. Food 3. Forests and hunting farms <p>VII. Healthcare</p> <ol style="list-style-type: none"> 1. Medical and hospital care 2. Drugs <p>VIII. Finance</p> <p>IX. Economy</p> <p>X. Sports facilities and facilities</p> <p>XI. Education, science and technology</p> <p>XII. Natural Resources</p> <p>XIII. Tourism</p> <p>XIV. Regional Development and Urban Development</p> <p>XV. Defence</p> <ol style="list-style-type: none"> 1. Defence industry 2. Military infrastructure and military formations <p>XVI. Justice, public order and security</p> <p>XVII. Government and social governance</p> <p>XVIII. Disaster protection</p> <p>XIX. Cultural Heritage</p> <ol style="list-style-type: none"> 1. Real Cultural Values 	<p>НАРЕДБА ЗА РЕДА, НАЧИНА И КОМПЕТЕНТНИТЕ ОРГАНИ ЗА УСТАНОВЯВАНЕ НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ И ОБЕКТИТЕ ИМ И ОЦЕНКА НА РИСКА ЗА ТЯХ (Appendix 1)</p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	2. Movable cultural values	
Number of national CI	Classified information	
Number of national CI operators	Classified information	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	The identification of critical infrastructures and their sites and their risk assessment are carried out with a view to reducing the risk of disasters and protecting the population.	НАРЕДБА ЗА РЕДА, НАЧИНА И КОМПЕТЕНТНИТЕ ОРГАНИ ЗА УСТАНОВЯВАНЕ НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ И ОБЕКТИТЕ ИМ И ОЦЕНКА НА РИСКА ЗА ТЯХ (Art.1)
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	The Minister of the Interior shall instruct the development of a risk assessment methodology for the established critical infrastructures and their sites. The working groups (composed by competent Ministries and other relevant bodies) shall develop a methodology for risk assessment of established critical infrastructures and their sites in the respective sector, The methodology shall be sent to the owners / operators of the established critical infrastructures.	НАРЕДБА ЗА РЕДА, НАЧИНА И КОМПЕТЕНТНИТЕ ОРГАНИ ЗА УСТАНОВЯВАНЕ НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ И ОБЕКТИТЕ ИМ И ОЦЕНКА НА РИСКА ЗА ТЯХ (Art.4)
Coordination of ministries, bodies and offices concerned	<p>The coordination of the activities for establishing critical infrastructure and their sites shall be carried out by the Minister of Interior.</p> <p>The issue of critical infrastructure Defence is closely monitored by the Bulgarian Ministry of Defence. Special attention is given to the new phenomenon – cyber security. The example with cyber-attacks on Estonia (2007) and Georgia (2008) increased the focus on the fact Bulgaria is facing a relatively new threat for which it has to be prepared</p>	<p>НАРЕДБА ЗА РЕДА, НАЧИНА И КОМПЕТЕНТНИТЕ ОРГАНИ ЗА УСТАНОВЯВАНЕ НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ И ОБЕКТИТЕ ИМ И ОЦЕНКА НА РИСКА ЗА ТЯХ (Art.4)</p> <p>https://www.mod.bg/bg/</p>
Communication with owners/operators	Within one month after the validation of the list of critical infrastructures and their sites, the competent authorities inform the owners/operators of critical infrastructure, as well as the respective district governors and mayors of municipalities for their establishment	НАРЕДБА ЗА РЕДА, НАЧИНА И КОМПЕТЕНТНИТЕ ОРГАНИ ЗА УСТАНОВЯВАНЕ НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ И ОБЕКТИТЕ ИМ И ОЦЕНКА НА РИСКА ЗА ТЯХ (Art.10)
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	<p>The information on critical infrastructure and their OSP is collected by:</p> <ol style="list-style-type: none"> 1. On-site inspections; 2. Gathering data from owners/managers/operators of NCI 3. Gathering data from CI on the basis of the Disaster Protection Act, the Municipal Disaster Protection Plans, the categorisation of settlements according 	НАРЕДБА ЗА РЕДА, НАЧИНА И КОМПЕТЕНТНИТЕ ОРГАНИ ЗА УСТАНОВЯВАНЕ НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ И ОБЕКТИТЕ

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>to the number of the potentially affected population according to the Disaster Protection Act, the annual reports on the activities for disaster protection.</p> <p>In carrying out inspections, the control bodies shall be entitled:</p> <ol style="list-style-type: none"> 1. access to critical infrastructure sites in accordance with established procedures; 2. require information relating to critical infrastructures and their sites; 3. involve experts. <p>When conducting inspections, the control authorities shall be obliged to observe the state, business and trade secrets, as well as not to disclose data from the inspection</p>	ИМ И ОЦЕНКА НА РИСКА ЗА ТЯХ (Art.6; Art.16)
Other relevant aspects of national authorities involved in CIP protection	<p>The Minister of the Interior shall establish and maintain a database on the critical infrastructures and their sites.</p> <p>The information, concerning the maintenance and updating of the database shall be submitted to the Minister of Interior by the authorities responsible of the identification of the NCI</p>	НАРЕДБА ЗА РЕДА, НАЧИНА И КОМПЕТЕНТНИТЕ ОРГАНИ ЗА УСТАНОВЯВАНЕ НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ И ОБЕКТИТЕ ИМ И ОЦЕНКА НА РИСКА ЗА ТЯХ (Art.6; Art.14)
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Yes	
- Preparation of a security plan	Yes	
- Review of the plan (timing)	Yes	
- Reporting incidents	Yes	
- Exchange of information	Yes	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>'Cybersecurity:</p> <p>Bulgaria adopted its national Cyber Security Strategy, National Cyber Security Strategy Cyber Resilient Bulgaria 2020, in July 2016</p> <p>The strategy sets out 9 objectives:</p> <p>1 - Establish and develop the national system for cyber security and resilience</p>	<p>Национална стратегия за киберсигурност</p> <p>„Киберустойчива България 2020“; 2016</p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	2 - Ensure Network and Information Security as the foundation of cyber resilience 3 - Support protection and sustainability of digitally dependent critical infrastructures 4 - Improve the interaction and information sharing between state, business and society 5 - Develop and improve the regulatory framework 6 - Step up the fight against cyber crime 7 - Lead cyber defence and protection of national security 8 - Raise awareness, knowledge and competencies and develop a stimulating environment for research and innovation in the field of cyber security 9 - International interaction - cyber diplomacy and Interoperability	

Croatia

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system		<i>Critical Infrastructure Act (CIA)</i>
Definitions (Art 2)		
'critical infrastructure'	'National Critical Infrastructures' are Systems, Networks and Objects of National Importance whose interruption in performance or interruption in the delivery of goods or services may have serious consequences on national security, the health and lives of people, property and the environment, security and economic stability and the continuous functioning of the authorities	CIA (Article 3)
'European critical infrastructure'	'European Critical Infrastructure' shall mean a critical infrastructure which is of interest to at least two Member States, or to one Member State while being located on the territory of another Member State.	CIA (Article 3)
'risk analysis'	Risk Analysis shall mean consideration of potential threat scenarios in order to evaluate the vulnerability and the potential impact of disruption or destruction of critical infrastructure.	
'sensitive critical infrastructure protection related information'	Sensitive data shall mean critical infrastructure information which pursuant to a specific regulation is marked as classified information.	
'protection'	Critical Infrastructure Protection shall mean activities aimed at ensuring the functionality, continuity and provision of critical infrastructure goods/services and preventing threats to critical infrastructure.	
'owners/operators of ECI'	The owner / manager security plan shall mean a plan which ensures the confidentiality, all-inclusiveness and availability of organisational, staff, material, information and communication and other solutions, as well as permanent and graduated security measures necessary for continual functioning of critical infrastructure.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Other relevant national definitions	<p>A contact point shall mean a central state administration body which, on behalf of the state, conducts communication with competent bodies of the European Union and other States for the purpose of exchanging information on critical infrastructure and the implementation of established activities in their protection and ensuring their continuity.</p> <p>Sectoral criteria (benchmarks) shall mean a set of specific criteria (benchmarks) against which the risk to systems and networks of critical infrastructures in a specific sector is assessed. The Critical Infrastructure Security Coordinator shall mean a person dealing with issues regarding critical infrastructure protection between the owner / operator and central state administration bodies competent for specific critical infrastructure sector.</p>	
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	The ECI sectors are defined in accordance with the EU Directive	CIA (Article 15)
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	ECI is determined by the Government in accordance with the proposal of the central state administration body competent for the particular CI sector (Ministry of the Sea, Transport and Infrastructure and Ministry of Environment and Energy)	CIA (Article 15)
Application of the procedure for the identification of ECI (as per Annex III)	In determining the ECI in the Republic of Croatia, the provisions of this Law shall apply to the determination of national critical infrastructure, and in particular the sectoral criteria and cross-cutting criteria of this Law, with the participation of the competent representatives from the Member States concerned.	CIA (Article 15)
<i>Step1 – Application of sectoral criteria</i>	Sectoral criteria are defined by the central state administration bodies competent for the particular sector in co-operation with regulatory agencies and professional associations for each sector.	CIA (Article 9)
<i>Step 2 – Application of the definition of critical infrastructure</i>	This area is not explicitly defined by CIA or by any other act.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	It is not specified in the law how the transboundary element is applied in practice.	
<i>Step 4 – Application of the cross-cutting criteria</i>	Cross-cutting criteria are applied in the risk analysis of all critical infrastructures in the following order and include <ul style="list-style-type: none"> Human losses (estimated number of deaths or injuries due to the breakdown of some critical infrastructure), Economic losses (estimated due to the importance of economic loss and / or defamation of the quality of products or services, including possible environmental impacts), Impact on the public (which is assessed with regard to the impact on public confidence, physical suffering and the reversal of everyday life, including the loss of basic and public services) 	CIA (Article 9)
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	Criteria thresholds are the part (annex) of the Rules on the CIP risk analysis methodology (numerical and descriptive indicators of the cross-cutting criteria for critical infrastructure identification and risk analysis) and classified.	CIA (Article 8, 9, 11, 15)
Identification of potential ECI on an ongoing basis (Art 3.1)	The Government of the Republic of Croatia, in accordance with the proposal of the competent state administration bodies shall adopt an annual report on the number of ECIP per sector and according to the number of interested MS.	CIA (Article 17)
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	In the territory of the Republic of Croatia the European Critical Infrastructure will be designated by the Government of the Republic of Croatia in accordance with the competent state administration bodies proposals. These activities are coordinated by state administration body responsible for protection and rescue (National Protection and Rescue Directorate – NPRD).	CIA (Article 17)
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	The Government of the Republic of Croatia informs the interested MS in co-operation with the responsible state administration body and NPRD.	CIA (Article 15, 17)
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	This area is not explicitly specified by law (CIA). If the CI of importance for the Republic of Croatia is situated on the territory of another Member State, the Croatian Government proposes to the competent authority of that State the determination of ECI.	CIA (Article 15)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	Specific channels for negotiations are not mentioned. In accordance with the law, information exchange is carried out through CIP contact point (NPRD).	CIA (Article 18)
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	It is not specified who is the body responsible for communicating to European Commission about the wish to engage bilateral agreement with other MS or the channels to be used. In the law, it is specified only that if the Member State, on whose territory the critical infrastructure is located, does not accept the proposal of the Republic of Croatia, the Government of the Republic of Croatia shall inform the European Commission thereof and request its involvement.	CIA (Article 15)
Agreement for the designation of the ECI (Art. 4.3)	In the law, it is not specified when the agreement is considered achieved.	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The Government of the Republic of Croatia shall adopt an annual report on the number of critical European infrastructures per sector and the number of interested countries dependent on each critical infrastructure, at the proposal of National Protection and Rescue Directorate (NPRD) that includes the reports of responsible central government bodies in whose sectors ECI are identified.	CIA (Article 17)
Informing the owner/operator of the designated ECI (Art. 4.5)	The competent central state administration bodies, upon designation of an ECI, shall inform the owners / managers of critical infrastructures within its scope of competence and the relevant regulatory agency. Channels used are not specified.	CIA (Article 15)
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The competent central state administration bodies shall (in co-operation with the competent regulatory agencies) determine whether the OSP has been drafted respecting sectorial criteria and cross-cutting criteria. The OSP are reviewed within one year from the appointment of the critical infrastructure, and then regularly once a year.	CIA (Article 10, 12 and 13)
Verification that the OSP or equivalent is in place	Verification is carried out through inspection by inspectors of the responsible central state administration body.	CIA (Article 20)
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The competent state administration bodies shall determine whether the SLO is in place.	CIA (Article 14 and 20)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Function of the SLO (Art. 6.1)	SLO is responsible for communication in security matters between the owner / manager and the competent state administration body. <i>Note: In accordance with the law (CIA, Art. 14), the central state administration bodies responsible for the CIP/ECIP sectors must appoint SLO whose task is to communicate with NPRD.</i>	CIA (Article 14)
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	It is not specified how the verification of the existence of SLO takes place, <i>but is checked through the inspection.</i>	CIA (Article 20)
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	<i>The specific communication mechanism is not specified.</i>	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	The Government of the Republic of Croatia (based on the NPRD report)	CIA (Article 17)
Performance of threat assessments within ECI subsector within one year following the designation of ECI	<i>The National Protection and Rescue Directorate (NPRD), within the scope of which protection and rescue work, in co-operation with the relevant central government bodies whose scope of activity includes critical infrastructure, regularly monitors, assesses the threats and proposes operational and other measures to assess the criteria and the need for a measure proposal to manage and protect critical infrastructures. Specifics of the threat assessment are not provided.</i> <i>The threat assessment is a part of the risk analysis.</i>	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The Government of the Republic of Croatia shall submit to the European Commission every two years a summary of general information on the types of threats, threats and weaknesses identified in each ECI sector in the Republic of Croatia.	CIA (Article 17)
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	<i>The procedure for the appointment of the contact point is not strictly defined by CIA.</i>	CIA (Article 18)
MS body(-ies) serving as ECIP contact point	The contact point for exchanging information and coordinating activities related to European Critical Infrastructures with other Member States and the bodies of the European Union is National Protection and Rescue Directorate (NPRD).	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	Same as above (transposition law)	
Scope of national CIP policy		
Sectors of critical importance	<p>National Critical Infrastructure Sectors may be in particular:</p> <ul style="list-style-type: none"> - Energy (production, including accumulation and dams, transmission, storage, energy and energy transport, distribution systems), - Communication and information technology (electronic communications, data transmission, information systems, audio and audio-visual media services), - Transport (road, rail, air, sea and inland waterways), - Health (health care, production, traffic and drug control), - Water management (regulatory and protective water structures and communal waterworks), - Food (production and supply of food and food safety system, commodity supply), - Finance (banking, stock exchanges, investments, insurance and payment systems), - Production, storage and transport of dangerous substances (chemical, biological, radiological and nuclear materials), - Public services (public order and security, protection and rescue, emergency medical assistance), - National monuments and values <p>Apart from the sectors referred to above, the Government of the Republic of Croatia may determine the critical infrastructure from other sectors.</p>	<u>CIA (Article 4)</u>
Number of national CI		
Number of national CI operators	According the law, the list of NCI is classified.	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	<p>Definitions of objectives and scope</p> <p>The Republic of Croatia has implemented Council Directive 2008/114/EC into national law by drafting and adopting the Critical Infrastructure Act, which provides for a process of regulation for national and European CI.</p>	CIA

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>Under this act, National CI is defined as “the systems, networks and objects of national importance whose disruption in operation or interruption in the delivery of the goods can have serious consequences for national security, health and lives of people, property or environment, security and economic stability and continuous functioning of the government.” Currently, the normative framework for CI protection in the Republic of Croatia is comprised of a critical infrastructure security and resilience system and the Critical Infrastructure Act. This framework has led to two important documents, pursuant to the Critical Infrastructure Act. The first document issued under the Critical Infrastructure Act is the Decision on designation the sectors from which the central state administrative bodies identify national critical infrastructure and lists of the order of the sectors of critical infrastructures (Decision on Designation). In the Decision on Designation, a total of eleven sectors have been determined from which ministries (the central administrative bodies) can identify the national CI.</p> <p>The second document, entitled “Rules on the methodology for drafting business risk analysis of critical infrastructure”, determines the guidelines, criteria and measurements for CI identification and risk analysis management. According to the CIA (Article 7) the central state administration bodies, together with the regulatory agencies, are responsible for identifying NCIP and for their protection, within the framework of their activities.</p>	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	The National Protection and Rescue Directorate (NPRD), in co-operation with the sectoral competent central government bodies and regulatory agencies, regularly monitors and assesses the threats and proposes operational and other measures for evaluation of criticality and measures to be taken for CIP protection.	CIA (Article 6)
Coordination of ministries, bodies and offices concerned	<p>Coordination of Ministries:</p> <p>This regulatory framework has determined the processes for identifying and defining national CI within the Decision on Designation’s eleven sectors. In these sectors there are nine competent ministries, along with a state administrative body responsible for protection and rescue, the National Protection and Rescue Directorate (NPRD), which functions at a lower governmental level than the ministries. The NPRD is the coordinator of the CIP system and is the national ECIP contact point for co-operation with other countries and the European Commission.</p>	
Communication with owners/operators	As described in the table above.	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	Inspection supervision of the implementation of this Act by the owner / operator of critical infrastructures shall be carried out by competent central government authority in accordance with its responsibilities	CIA (Article 20)
Other relevant aspects of national authorities involved in CIP protection		
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	As described in the table above.	
- Preparation of a security plan	As described in the table above.	
- Review of the plan (timing)	The security plans shall be reviewed within one year of CI designation, and regularly once a year.	CIA (Article 13)
- Reporting incidents	This area is not regulated by CIA.	
- Exchange of information	As described in the table above.	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Cybersecurity</p> <p>Croatia adopted:</p> <ul style="list-style-type: none"> - The National Cybersecurity Strategy and the Action Plan - in October 2015. - Act on Key Service Providers and Digital Service Providers' Cyber Security - in July 2018.- Croatia has thus implemented the Directive 2016/1148 (NIS Directive) into the national legislation and ensured the implementation of Commission Implementing Regulation 2018/151 for the implementation of the Directive 2016/1148. <p>This Act regulates the procedures and measures for achieving a high level of key service providers and digital service providers cyber security, competencies and powers of the relevant sectoral bodies, unique national contact points, incident prevention and protection bodies (the competent CSIRT) and technical bodies for conformity assessment, supervision of key</p>	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>service operators and digital service providers in the implementation of this Law.</p> <p>The purpose of the Law is to ensure the implementation of measures to achieve a high level of cyber security in delivering services that are of particular importance for the conduct of key social and economic activities, including the functioning of the digital market.</p> <p>The Main bodies that were responsible for the cybersecurity are:</p> <ul style="list-style-type: none"> • The Information Systems Security Bureau (ZSIS) - CSIRT • Croatian Academic and Research Network (CarNet) – National CSIRT/NCERT • The office of the National Security Council • Ministry of the Interior 	

Czechia

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<p>The Crisis Act specifies domain and jurisdiction of state authorities and of authorities of territorial self-governing units and rights and obligations of legal and natural entities during preparedness for crisis situations, which are not related to provision of defence of Czechia against an external attack and during their solution and protection of critical infrastructure and responsibility for the breach of these obligations.</p> <p>The Crisis Act processes relevant regulations of the European Union and modifies specification and protection of European critical infrastructure.</p> <p>Governmental order No. 432/2010 Coll. specifies cross-cutting and sectoral criteria for the identification of a critical infrastructure element.</p> <p>Governmental order No. 462/2000 Coll. contains specification and structure of crisis preparedness plan of CI subjects.</p> <p>Methodology serves to ensure a uniform approach in processing the plans of crisis preparedness and plans of crisis preparedness of subject of critical infrastructure.</p>	<p>Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts (the Crisis Act)</p> <p>Governmental order No. 432/2010 Coll. on the criteria for the identification of critical infrastructure element</p> <p>Governmental order No. 462/2000 Coll. on the implementation of section 27 paragraph 8 and section 28 paragraph 5 of Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts</p> <p>Methodology for processing the plans of crisis preparedness according to Section 17 and 18 of Governmental order No. 462/2000 Coll. for the execution of Section 27 paragraph 8 and Section 28 paragraph 5 of Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts</p>
Definitions (Art 2)		
'critical infrastructure'	Critical infrastructure shall denote the element of critical infrastructure or the system of elements of critical infrastructure, disruption of which would have a significant impact on the State security, on ensuring the basic living needs of the population, on health of people and State economy.	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts (the Crisis Act)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
'European critical infrastructure'	European Critical Infrastructure shall denote the critical infrastructure within the territory of Czechia, disruption of which would have a significant impact on other member state of the European Union.	Article 2 (Term Specification)
'risk analysis'	N/A	
'sensitive critical infrastructure protection related information'	N/A	
'protection'	Critical infrastructure protection shall denote the set of measures aimed at reducing disruption risk of function of the critical infrastructure element.	
'owners/operators of ECI'	Subject of critical infrastructure shall denote the operator of the critical infrastructure element; in case the operator is the operator of European critical infrastructure, the element is considered to be the subject of European critical infrastructure	
Other relevant national definitions	<p>"Element of critical infrastructure" shall denote primarily building, establishment, vehicle or public infrastructure³⁶), determined in accordance with the cross-cutting and sectoral criteria; in case the element of critical infrastructure is a part of European critical infrastructure it is considered to be an element of European critical infrastructure.</p> <p>"Cross-Cutting criteria" shall denote the set of criteria for assessing seriousness of impact of disruption of critical infrastructure element functioning with limiting value of loss of lives, health impact, extremely severe economic impact or impact on public as a result of extensive restriction of provision of essential services or other serious intervention into everyday life.</p> <p>"Sectoral criteria" shall denote the technical or operational criteria determining the critical infrastructure element in the sector of energy, water management, food industry and agriculture, health service, transport, communication and information systems, financial market and currency, emergency services and public administration.</p> <p>"Crisis situation" shall denote an emergency event according to the Integrated Rescue System Act, disruption of critical infrastructure or another threat when the state of danger, the emergency state or the state of State menace is declared.</p> <p>"Crisis measures" shall denote an organisational or technical measure intended to deal with crisis situation and elimination of its consequences, including the measures interfering with personal rights and obligations</p>	
Scope (Art 3.3)		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<p>Sectors and sub-sectors in scope:</p> <ul style="list-style-type: none"> - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports) 	<p>Energy</p> <ul style="list-style-type: none"> • Electricity (Electricity production facility, Transmission system, Distribution system) • Gas (Transmission system, Distribution system, Gas storage) • Oil and oil (petroleum) products (Transmission system, Distribution system, Oil and fuel storage, Fuel production) • Central thermal energy supply system (Thermal production facility, Thermal energy distribution) <p>Transport</p> <ul style="list-style-type: none"> • Road transport • Rail transport • Air transport • Inland water transport 	<p>Governmental order No. 432/2010 Coll. on the criteria for the identification of critical infrastructure element (Annex 1)</p>
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	<p>1) Government decides on the basis of the list submitted by the Ministry of Interior on the elements of critical infrastructure and the elements of European critical infrastructure which are operated by the organisational unit of the state</p> <p>2) Ministries and other central administrative authorities identify by general measure the element of critical infrastructure and the element of European critical infrastructure, unless they are not the elements specified by section 4 paragraph 1 letter e) and inform the Ministry of Interior about this identification without undue delay, including figures about the number of member states that are dependent on such determined elements of European critical infrastructure</p>	<p>Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 4, paragraph 1 letter e), section 9, paragraph 3 letter c)</p>
Application of the procedure for the identification of ECI (as per Annex III)	The procedure is indicated below:	
<i>Step1 – Application of sectoral criteria</i>	Entities tasked with implementing this step are responsible authorities of individual CI sectors (respective Ministries and other central administrative authorities, into whose sphere the CI sectors fall) and subjects of CI (individual owners or operators of the CI). The selection is carried out on the basis of fulfilment of sector criteria.	<p>Governmental order No. 432/2010 Coll. on the criteria for the identification of critical infrastructure element</p>
<i>Step 2 – Application of the definition of critical infrastructure</i>	This step is directly intertwined with the previous one. The core of this step is that the potential CI has to comply with the CI definition which is given by legislation (Directive). This step is carried out by the same entities as in the previous step.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	The ECI definition is applied to CI defined by the sector criteria and complying with the CI definition. The CI's which satisfy the transboundary element definition of ECI, will follow the next step of the procedure. The CI's which do not satisfy the transboundary element of the definition of ECI can be designated as national CI's of Czechia. This step is carried out by the same entities as in the previous two steps.	
<i>Step 4 – Application of the cross-cutting criteria</i>	Each MS shall apply the cross-cutting criteria to the remaining potential ECI. This step is managed by the Ministry of Interior – Directorate General of the Fire Rescue Service of the Czechia. The CI that have passed through all the steps of this procedure are considered to be potential ECI. These potential ECI will be announced by the Ministry of Interior – DG FRS CR to a respective EU authority and to those Member States which they may have an impact on. The subsequent steps of this procedure are carried out on the EU level	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	<p>Cross-cutting criteria for the identification of a critical infrastructure element are defined in the Governmental order No. 432/2010 Coll.</p> <p>An impact criterion for the identification of a critical infrastructure element is the aspect of:</p> <ul style="list-style-type: none"> a) More than 250 casualties or more than 2500 people who needed hospitalisation for longer than 24 hours, b) Economic impact with threshold value of economic loss greater than 0,5% GDP, or c) Impact on society with threshold value of a large limitation of necessary service provision or another serious intervention into the daily life of more than 125000 people. 	
Identification of potential ECI on an ongoing basis (Art 3.1)	<p>It is not indicated in the transposition document but ministries and other central administrative authorities:</p> <ul style="list-style-type: none"> 1) annually provide the Ministry of Interior with information on protection of European critical infrastructure including the data on vulnerability types, threats and identified risks 2) every two years provide information for the Ministry of Interior on exercised controls of the entities of European critical infrastructure including information on serious findings and ordered measures <p>Frequency of revision of identified elements of critical infrastructure or element of European critical infrastructure is not indicated in transposition documents but the list of the identified elements of critical infrastructure which are operated by the organisational unit of the state are reviewed usually every year</p>	<p>Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts</p> <p>Section 9 paragraph 3 letters f) and g)</p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	<p>1) Government decides on the basis of the list submitted by the Ministry of Interior on the elements of critical infrastructure and the elements of European critical infrastructure which are operated by the organisational unit of the state</p> <p>2) Ministries and other central administrative authorities identify by general measure the element of critical infrastructure and the element of European critical infrastructure, unless they are not the elements specified by section 4 paragraph 1 letter e) and inform the Ministry of Interior about this identification without undue delay, including figures about the number of member states that are dependent on such determined elements of European critical infrastructure.</p>	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 4, paragraph 1 letter e), section 9, paragraph 3 letter c)
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	<p>The Ministry of Interior fulfils the tasks in the area of critical infrastructure resulting from the membership of the Czechia in the European Union and provides international exchange of information in this area.</p> <p>The Ministry of Industry and Trade and the Ministry of Transport provide information about designating and potential ECI to the Ministry of Interior.</p>	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 10 paragraph 1 letter g)
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	Not indicated in transposition documents.	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	The Ministry of Interior fulfils the tasks in the area of critical infrastructure resulting from the membership of Czechia in the European Union, provides international exchange of information in this area, serves as the contact point of Czechia in the frame of European critical infrastructure and submits the European Commission reports on tasks of implementation arising from the EU legislation in this area.	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 10 paragraph 1 letter g)
Agreement for the designation of the ECI (Art. 4.3)	Not indicated in transposition documents.	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The Ministry of Interior annually informs the EC about the number of ECI per sector and on the number of MS of the European Union that are affected by ECI in Czechia.	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 10 paragraph 1 letter h)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Informing the owner/operator of the designated ECI (Art. 4.5)	Not indicated in transposition documents.	
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	Subject of critical infrastructure is responsible for protection of the critical infrastructure element. For this purpose, he/she is obliged a) to process the plan of crisis preparedness of the subject of critical infrastructure within one year since the decision of the Government or since the day of coming into force of the measure of general nature, which designated the element of critical infrastructure; b) to allow the competent Ministry or other central administrative authority the execution of control of the crisis preparedness plan of the critical infrastructure subject and protection of the element of critical infrastructure including the entry permission on grounds and into premises where the element is located; c) to inform without undue delay the competent Ministry or other central administrative authority about organisational, production or other change, in case it is obvious that this change may affect determination of the element of critical infrastructure, in particular information about permanent shutdown, termination of business or restructuring.	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 29a Governmental order No. 462/2000 Coll. on the implementation of section 27 paragraph 8 and section 28 paragraph 5 of Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 19 paragraph 2
Verification that the OSP or equivalent is in place	The sectoral competent Ministry or other central administrative authorities have to control if the OSP is in place. To this end, inspections and spot checks are carried out. The OSP are reviewed every four years after their verification or immediately in case of significant change.	
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	1) The subject of critical infrastructure determines the security liaison officer and informs the competent Ministry or other central administrative authority about this designation. The subject of critical infrastructure shall execute this without undue delay. 2) Until the time of determination of the Security Liaison Officer, his/her tasks are fulfilled by the subject of critical infrastructure. 3) The Security Liaison Officer can only be the person meeting all requirements of professional competence. Professionally competent is the person who has obtained university or college education, a graduate of the accredited study programme providing comprehensive knowledge of safety and security of Czechia, of protection of population or crisis management or has at least three-year experience in this field.	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 29c paragraph 1, 2 and 4
Function of the SLO (Art. 6.1)	The Security Liaison Officer cooperates in fulfilling the tasks instead of the subject of critical infrastructure.	Act No. 240/2000 Coll. on Crisis Management and on

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		the amendments of certain Acts Section 29c paragraph 3
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	Not indicated in transposition documents.	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	Not indicated in transposition documents.	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	<p>The body responsible for fulfilling reporting obligations with the entities of European Union is the Ministry of Interior, as is specified below.</p> <p>Furthermore, the competent ministries and other central administrative authorities for protection of CI annually provide to the Ministry of Interior the information on protection of ECI, including the data on vulnerability types, threats and identified risks and every two years provide the information for the Ministry of Interior concerning the controls performed on operators of ECI, including information on serious findings and correction measures.</p>	<p>Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 10 paragraph 1 letters h) and i)</p> <p>Section 9 paragraph 3 letters f) and g)</p>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	<p>Ministries and other central administrative authorities annually provide the Ministry of Interior with information on protection of ECI, including the data on vulnerability types, threats and identified risks.</p> <p>The main content of the threat assessment is not specified.</p>	<p>Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 9 paragraph 3 letters f)</p>
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	<p>The Ministry of the Interior every two years submits to the EC a summary report of general data about types of vulnerabilities, threats and risks discovered in various sectors of ECI.</p> <p>The specific content of the summary is not specified.</p>	<p>Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 10 paragraph 1 letter i)</p>
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	<p>The Ministry of Interior is a contact point for the ECI matters and performs tasks in the CIP sector relating to Czechia's membership in EU (proposes crosscutting criteria; processes a list that is a base for CI</p>	<p>Act No. 240/2000 Coll. on Crisis Management and on</p>
MS body(-ies) serving as ECIP contact point		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	elements and ECI elements determination; communicates and informs the EC about ECI; etc.).	the amendments of certain Acts Section 10 paragraph 1 letter g)

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<p>National CIP measures and definitions already existed before 2008 and were included in non-legislative acts. They were successively implemented within the Crisis Act. In 2010, in response to the European Council Directive the National Programme for Critical Infrastructure Protection and the Comprehensive strategy of Czechia for Critical Infrastructure were adopted. These documents defined the rights and duties of those authorities involved in preparing for emergencies, their management, and the protection of critical infrastructures.</p> <p>The Concept of Population Protection till 2020 with the outlook to 2030 (2013) and the Security strategy of the Czech Republic (2015) followed as consecutive documents in this field.</p>	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts, National Programme for Critical Infrastructure Protection (2010), Comprehensive strategy of the Czech Republic for Critical Infrastructure (2010), The Concept of Population Protection till 2020 with the outlook to 2030 (2013) and Security strategy of Czechia (2015)
Scope of national CIP policy		
Sectors of critical importance	<ol style="list-style-type: none"> 1. Energy 2. Water resource management 3. Food industry and agriculture 4. Health sector 5. Transport 6. Communication and information systems 7. Financial market and currency 8. Emergency services 9. Public administration 	Governmental order No. 432/2010 Coll. on the criteria for the identification of critical infrastructure element (Annex 1)
Number of national CI	Approximately 1900	
Number of national CI operators	Approximately 150	
Responsibilities allocated to Ministries, bodies, and offices		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Definition of scope and objectives of the national CIP strategy	<p>Particular importance is attached to the protection of CI within the Security Strategy of Czechia. Czechia monitors foreign investment into individual sectors of CI and into strategic companies in order to avert the threat of misuse of such investment as a channel through which a foreign power might promote its economic and political interests at the expense of Czechia. In order to protect CI and strategic companies, especially in the energy sector — in the subsectors of electricity, natural gas, crude oil and oil products, and heat energy — and the information and communications technology sector, Czechia views it as necessary:</p> <ul style="list-style-type: none"> • To increase the protection and resilience of national CI and ECI, • To cooperate with the owners/operators CI, • To retain control over CI where it is still owned by the state, and to avoid diminishing the state's influence and control over strategic companies operating in individual areas of critical infrastructure. <p>Since 2011 the issue of critical infrastructure protection has been a part of the system of crisis management. It has been incorporated into the legal system implementing the Council Directive 2008/114/EC from December 8th, 2008 on Identification and Designation of the European Critical Infrastructures and the Need to Improve their Protection. The critical infrastructure, especially its protection, represents the possible future potential for further development of the crisis management system. The Amendment of the Crisis Act from 2010 incorporated the system of critical infrastructure into crises management, set the method determining the elements of critical infrastructure and the rights and obligations of the entities of critical infrastructure. The absence of legislation on the issue of exact methods and procedures of critical infrastructure protection elements in all the sectors defined by the law can be considered as a gap.</p> <p><u>Due to this gap the Concept of Population Protection set the following objectives:</u></p> <p>Precise the system of critical infrastructure protection (e.g. revise or supplement the designated sectors of the critical infrastructure) and define by the statutory legislative instruments or technical standards the specific requirements for realisation of various types of protection (physical, personal, information, cyber etc.) of the</p>	<p>Security Strategy of Czechia (2015)</p> <p>The Concept of Population Protection till 2020 with the outlook to 2030 (2013)</p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	critical infrastructure. Involve the critical infrastructure entities in the process of the legislative and methodological documents.	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	Described in the table above The sectorally competent annually provide the Ministry of Interior with information on protection of European critical infrastructure including the data on vulnerability types, threats and identified risks,	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts Section 9 paragraph 3 letter f)
Coordination of ministries, bodies and offices concerned	Described in the tables above The coordination role fulfils the Ministry of Interior. The sectorally competent ministries, other central administrative authorities and subjects of critical infrastructure fulfil the tasks in the area of critical infrastructure resulting from the Crisis Act.	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts
Communication with owners/operators	The Crisis Act establishes that the subjects of critical infrastructure (operators) must inform without undue delay the sectorally competent Ministry or other central administrative authority about any developments that could affect the status of the CI, in particular information about permanent shutdown, termination of business or restructuring.	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	Sectorally competent Ministries, under the coordination of the Ministry of Interior.	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts
Other relevant aspects of national authorities involved in CIP protection	N/A	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	It is described in the table above	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts
- Preparation of a security plan	It is described in the table above	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts
- Review of the plan (timing)	It is described in the table above	Act No. 240/2000 Coll. on Crisis Management and on

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
		the amendments of certain Acts
- Reporting incidents	N/A	
- Exchange of information	It is described in the table above	Act No. 240/2000 Coll. on Crisis Management and on the amendments of certain Acts
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Measures for business security One of the main objectives defined within Concept of Population Protection is to precise the system of critical infrastructure protection (e.g. revise or supplement the designated sectors of the critical infrastructure) and define by the statutory legislative instruments or technical standards the specific requirements for realisation of various types of protection (physical, personal, information, cyber etc.) of the critical infrastructure. Involve the critical infrastructure entities in the process of the legislative and methodological documents.</p> <p>Cybersecurity measures The Strategy represents a comprehensive set of measures aiming to achieve the highest possible level of cyber security in Czechia. To this aim, it defines the vision Czechia would like to follow in this field. Furthermore, the Strategy stipulates the basic principles which will be kept and defines the particular challenges and problems both Czechia and the international environment have to counter. The main goals, which shall be achieved in the upcoming five years, are the key part of the Strategy. They are divided into the following priority areas:</p> <ul style="list-style-type: none"> • Ensuring efficiency and strengthening of all structures, processes and co-operation in the field of cyber security • Active international co-operation • Protection of the national Critical Information Infrastructure and IT systems • Co-operation with private sector • Support to the development of Police capabilities to investigate and prosecute information crime. 	<p>The Concept of Population Protection till 2020 with the outlook to 2030 (2013)</p> <p>National Cyber Security Strategy of Czechia for the period from 2015 to 2020</p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> Cybersecurity legislation (development of legislative framework). Participation in creation and implementation of European and international regulations. 	

Denmark

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<ul style="list-style-type: none"> - <i>Bekendtgørelse om kritisk europæisk infrastruktur på vejområdet</i> - <i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse</i> - <i>Bekendtgørelse om europæisk kritisk infrastruktur på jernbaneområdet</i> - <i>Bekendtgørelse om europæisk kritisk infrastruktur på havneområdet</i> <p>Denmark decided to adopt the Directive through four different Executive Orders, one for each sector involved. While the Orders concerning the transport sector, which implemented the Directive with a formal transposition, regarding the energy sector the transposition was more detailed.</p>	<p><i>BEK nr 11 af 07/01/2011 – Gældende - Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse (EPCIP-direktivet)</i></p> <p><i>BEK nr 7 af 06/01/2011 - Gældende - Bekendtgørelse om kritisk europæisk infrastruktur på vejområdet (EPCIP-direktivet)</i></p> <p><i>BEK nr 1726 af 22/12/2010 - Gældende - Bekendtgørelse om europæisk kritisk infrastruktur på havneområdet (EPCIP-direktivet)</i></p> <p><i>BEK nr 1461 af 14/12/2010 - Gældende - Bekendtgørelse om europæisk kritisk infrastruktur på jernbaneområdet (EPCIP-direktivet)</i></p>
Definitions (Art 2)		
'critical infrastructure'	A Critical infrastructure is an asset, systems or parts thereof located in the Member States which are essential for the maintenance of vital social functions and human health, safety and economic or social welfare and whose interruption or destruction will significantly affect a Member State	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, Section 2</i>
'European critical infrastructure'	A European Critical Infrastructure is a Critical Infrastructure located in the Member States, whose interruption or destruction will have significant consequences for two or more Member States. The significance of the consequences is assessed on the basis of the cross-cutting criteria. This also includes consequences due to cross-sectoral dependence of other types of infrastructure.	
'risk analysis'	Risk analysis: consideration of relevant threat scenarios to assess vulnerability and the potential consequences of critical interruption or destruction.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
'sensitive critical infrastructure protection related information'	Sensitive information on critical infrastructure protection: Critical Infrastructure data, which, if published, may be used to plan and act in order to cause interruption or destruction of critical infrastructure.	
'protection'	Protection: All activities aimed at ensuring the functionality, continuity and integrity of critical infrastructure in order to deter, mitigate and neutralise a threat, risk or vulnerability.	
'owners/operators of ECI'	European Critical Infrastructure Owners: Companies, etc., which are responsible for investments in a specific infrastructure or part thereof European Critical Infrastructure Operators: Companies, etc., which are responsible for the day-to-day operation of a specific infrastructure or part thereof	
Other relevant national definitions		
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Energy: 1) Electricity sector; 2) Natural gas sector; 3) Oil sector Transport 4) Road transport; 5) Rail transport; 6) Ports	<i>BEK nr 11 af 07/01/2011 – Gældende - Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse (EPCIP-direktivet)</i> <i>BEK nr 7 af 06/01/2011 - Gældende - Bekendtgørelse om kritisk europæisk infrastruktur på vejområdet (EPCIP-direktivet)</i> <i>BEK nr 1726 af 22/12/2010 - Gældende - Bekendtgørelse om europæisk kritisk infrastruktur på havneområdet (EPCIP-direktivet)</i> <i>BEK nr 1461 af 14/12/2010 - Gældende - Bekendtgørelse om europæisk kritisk infrastruktur på</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		<i>jernbaneområdet</i> (EPCIP-direktivet)
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The Danish Energy Agency (energy sector) The Danish Transport, Building and Housing Authority (transport sector)	
Application of the procedure for the identification of ECI (as per Annex III)	For the identification of European Critical Infrastructure, the procedure is composed by four consecutive steps. This procedure begins with a broad survey of potential European Critical Infrastructure. On this basis, potential European Critical Infrastructure, which meets the one-step steps in the procedure, must review the next step in the procedure.	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, Section 4</i>
<i>Step1 – Application of sectoral criteria</i>	Step 1 - Sector-based criteria are used to make an initial selection of potential European Critical Infrastructure in the energy sectors concerned.	
<i>Step 2 – Application of the definition of critical infrastructure</i>	Step 2- The Energy Agency uses the definition of critical infrastructure, on the potential European Critical Infrastructure identified in Step 1. The significance of the consequences is determined either by using national methods for identifying critical infrastructure or by reference to the cross-criteria at an appropriate national level. For infrastructure providing important services, consideration should be given to alternatives to this and for the expected duration of a potential interruption or restoration.	
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	The Danish Energy Agency uses the definition of European Critical Infrastructure on the potential European Critical Infrastructure identified through the first two steps of the procedure. For infrastructure providing important services, consideration should be given to alternatives to this and for the expected duration of a potential interruption or restoration.	
<i>Step 4 – Application of the cross-cutting criteria</i>	The Danish Energy Agency uses the cross-criteria criteria for the potential European Critical Infrastructure, which has met the first three steps of the procedure. The cross-criteria take account of the serious consequences expected to be, and - for infrastructure providing essential services, whether there are alternatives to this and for the expected duration of potential interruption or restoration. Potential European Critical Infrastructure, which does not meet the cross-criteria, is not considered European Critical Infrastructure. The cross-cutting criteria include the following:	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>1) Criterion of victims (an assessment of the potential number of killed or injured).</p> <p>2) Criterion of economic impact (an assessment of the size of the economic loss or deterioration of goods or services, including potential environmental impacts).</p> <p>3) The criterion of general impact (an assessment of the consequences with regard to the confidence of the population, physical disorders and disturbance of everyday life, including outcomes of essential services).</p>	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	Energy sector: The threshold values for the cross-cutting criteria must be based on the severity of the interruption or destruction of a particular infrastructure	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, Section 6</i>
Identification of potential ECI on an ongoing basis (Art 3.1)	The Danish Energy Agency (energy sector) and the Danish Transport, Building and Housing Authority (transport sector) review this identification and designation once a year	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, section 8</i>
Designation of the ECI (Art. 4)		
<i>MS body(-ies) responsible for the designation of ECI (discussions and agreement)</i>	<p><i>The Danish Energy Authority (energy sector)</i></p> <p>The Danish Transport, Building and Housing Authority (transport sector)</p>	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, section 7</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	Prior to any nomination, the Danish Energy Agency has discussions with the other Member States, which may be significantly affected by the potential European Critical Infrastructure. If appointment is to be made, the Danish Energy Agency agrees with relevant Member States.	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, section 7</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	The Danish Energy Agency shall provide contact with relevant other Member States, to other authorities and to the Commission on the designation of European Critical Infrastructure in Energy, located in and outside of Denmark.	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, section 7</i>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Agreement for the designation of the ECI (Art. 4.3)	See section above "Informing other MS"	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	Not specified in the Executive Order	
Informing the owner/operator of the designated ECI (Art. 4.5)	<p>Prior to any designation, the Danish Energy Agency shall hear operators of the infrastructures designated as European Critical Infrastructure.</p> <p>The Danish Energy Agency informs the operator and the owner of a concrete infrastructure about its designation as European Critical Infrastructure.</p>	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, section 7</i>
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	<p>The operator must establish a safety plan for the infrastructure. The operator shall submit the safety plan to the Danish Energy Agency for approval within 12 months after the operator has been notified that the infrastructure has been designated as European Critical Infrastructure. The Danish Energy Agency may draw up guidelines on the emergency preparation. Guidelines and instructions must be available to operators, who will be informed accordingly.</p>	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, section 9</i>
Verification that the OSP or equivalent is in place		
Verification that the OSP or equivalent is appropriately and regularly reviewed	<p>The operator shall ensure that the safety plan is regularly reviewed to the extent necessary for the development, including significant changes to the company, infrastructure and its risks, vulnerabilities and safety conditions. The operator shall submit at least the safety plan for approval every three years</p>	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, section 12</i>
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	<p>The operator of an infrastructure designated as European Critical Infrastructure shall designate the following contacts:</p> <ol style="list-style-type: none"> 1) A security officer for this infrastructure, 2) A contact point in emergency situations (operational contact). <p>The security officer must be safety approved at an appropriate level, determined by the Danish Energy Authority</p>	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, section 14</i>
Function of the SLO (Art. 6.1)	<p>The security officer acts as a contact point for security issues between the operator and the Danish Energy Agency and other relevant authorities. The contact point in emergency situations (operational contact) shall at any time serve as a link to the operator and shall be able to receive information</p>	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	from the Danish Energy Authority and other authorities in accordance with the OSP and shall ensure that the operator takes the necessary measures, including the dissemination of information internally in the company.	<i>vurdering af behovet for bedre beskyttelse, section 14</i>
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	Not specified in the Executive Order	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	The Danish Energy Agency shall establish an appropriate communication mechanism between the Danish Energy Agency, the security officer and the contact point listed in section above, in order to exchange relevant information on the identified risks and threats associated with the European Critical Infrastructure concerned.	<i>Bekendtgørelse om identifikation og udpegning af europæisk kritisk infrastruktur på energiområdet og vurdering af behovet for bedre beskyttelse, section 14</i>
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	Not specified in the Executive Order	
Performance of threat assessments within ECI subsector within one year following the designation of ECI	Not specified in the Executive Order	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	Not specified in the Executive Order	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	Not specified in the Executive Order	
MS body(-ies) serving as ECIP contact point	Not specified in the Executive Order	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures		
Scope of national CIP policy		
Sectors of critical importance	<ul style="list-style-type: none"> Not applicable 	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Number of national CI	n.a.	
Number of national CI operators	n.a.	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	Sector-specific	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	Sector-specific	
Coordination of ministries, bodies and offices concerned	Not applicable	
Communication with owners/operators	Sector-specific	
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	Sector-specific	
Other relevant aspects of national authorities involved in CIP protection	The Danish Emergency Management Agency develops optional methodology for CI identification for sector-specific use.	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Yes. Subject to sector-specific guidelines and legislation.	
- Preparation of a security plan	Yes. Subject to sector-specific guidelines and legislation.	
- Review of the plan (timing)	Yes. Subject to sector-specific guidelines and legislation.	
- Reporting incidents	Yes. Subject to sector-specific guidelines and legislation.	
- Exchange of information		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Cybersecurity: The primary objective of the cyber defence is to enhancing the protection of critical infrastructure. Through the delivery of preventive advice and assistance, a stronger cyber defence contribute to ensuring coherence and increased robustness across sectors. The relevant measures were adopted with the Danish National Cyber Security Strategy in May 2018.</p> <p>In Denmark the approach is sectoral. This means that it is always the specific sector that is responsible for ensuring appropriate preparation so that the critical functions can be maintained.</p>	<p><i>National Cyber Security Strategy (May 2018)</i></p>

Estonia

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<p>1. <i>Hädaolukorra seadus – Emergency Act</i> https://www.riigiteataja.ee/en/eli/513062017001/consolide</p> <p>2. <i>Elutähtsa teenuse toimepidevuse riskianalüüsi ja plaani, nende koostamise ning plaani kasutuselevõtmise nõuded ja kord - Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan</i> https://www.riigiteataja.ee/en/eli/525092017001/consolide</p>	
Definitions (Art 2)		
'critical infrastructure'	<p>A critical infrastructure definition is equivalent to the vital service definition.</p> <p>A vital service is a service that has an overwhelming impact on the functioning of society and the interruption of which is an immediate threat to the life or health of people or to the operation of another vital service or service of general interest. A vital service is regarded in its entirety together with a building, piece of equipment, staff, reserves and other similar facilities indispensable to the operation of the vital service.</p>	<i>Emergency Act (Article 2 p 4)</i>
'European critical infrastructure'	Not defined.	
'risk analysis'	A continuity risk assessment of a vital service describes the risks causing an interruption of the service, the probability of the risks, the consequences of an interruption and other significant circumstances.	Emergency Act (Article 39 p 2)
'sensitive critical infrastructure protection related information'	Not defined. Sensitive information is protected through Public Information Act. A holder of information is required to classify the following as information intended for internal use: <ul style="list-style-type: none"> a) The risk assessment of vitally services and information concerning the operational continuity plan; b) Information whose disclosure may violate a business secret. 	Public Information Act -. (Article 35 p 17 and 18 ¹).
'protection'	<p>Not defined. It is set down through other definitions.</p> <p>The continuity of a vital service is the capability of the provider of the vital service to ensure continuous operation and to restore continuous operation after an interruption of the vital service.</p>	Emergency Act (Article 2 p 5)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	The purpose of the critical information infrastructure protection (CIIP) is to maintain a trouble-free functioning of the country's essential information and communication systems	
'owners/operators of ECI'	<p>A provider of a vital service is a legal person whose competence includes the fulfilment of a public administration duty defined as a vital service or a person operating as an undertaking providing a vital service in the case specified in law.</p> <p>The service provider's criteria are set out in the sectoral laws.</p>	Emergency Law (Article 38 p 1 and 2).
Other relevant national definitions	<p>An emergency is an event or a chain of events or an interruption of a vital service which endangers the life or health of many people, causes major proprietary damage, major environmental damage or severe and extensive interferences with the continuity of vital services and resolution of which requires the prompt coordinated activities of several authorities or persons involved by them, the application of a command organisation different from usual and the involvement of more persons and means than usual.</p> <p>A risk of an emergency is a situation where on the basis of an objective assessment of the circumstances it may be considered likely that an event or a chain of events or an interference with a vital service may escalate into an emergency in the near future.</p> <p>Plan is a document which describes activities for recovering a vital service in the case of an interference or interruption.</p> <p>Risk class means the probability of the realisation of a scenario and the estimated severity of its consequences.</p> <p>Risk assessment means a document in which the risks of the continuity of a vital service are assessed and preventive measures for preventing an interference with or interruption of the vital service are planned.</p> <p>Scenario means the expected course of an event caused by the realisation of a threat which affects critical activities.</p>	<p><i>Emergency Act (Article 2 p 1 and 2).</i></p> <p>Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan (Article 2 p 10-13).</p>
Scope (Art 3.3)		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Energy (electricity, gas and oil) and transport (road, rail, Air, inland waterways, Ocean and short-sea shipping and ports) sectors.	<i>Directive 2008/114.</i>
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The Ministry of Economic Affairs and Communications who is responsible for transport and energy sector is responsible for verifying the existence of such infrastructure.	<i>The law does not establish ECI identification procedure. It's organisational.</i>
Application of the procedure for the identification of ECI (as per Annex III)	The Ministry of Economic Affairs and Communications leaded this process. Ministry formed working group and applied EC guidelines.	<i>The law does not establish ECI identification procedure. It's organisational.</i>
Step1 – Application of sectoral criteria	For identifying transport and energy ECI Estonia used EC guidelines. The Commission together with the Member States developed guidelines for the application of the cross-cutting and sectoral criteria and approximate thresholds. The sectoral criteria are classified.	EC guidelines.
Step 2 – Application of the definition of critical infrastructure	The definition of CI was implicitly applied within the process.	
Step 3 – Application of the transboundary element of the definition of ECI	Impact on other MS was evaluated through MS contacts and operator knowledge. Estonia applied EC guidelines. For example. In 2010 Ministry of Economic Affairs and Communications formed Working Group of Experts of the on identification of the European Critical Infrastructure (ECI) according to the Council Directive 2008/114/EC in association with the particular stakeholders.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>There have been several meetings. On 26 August a Working Group electricity expert met his Latvian and Lithuanian colleagues in Vilnius. He had opportunity to discuss the subject with is Lithuanian and Latvian colleague.</p> <p>On 12 October Working Group got official letter from Finland.</p> <p>The added value of the Directive for Estonia is that they had good opportunity to use step-by step approach to identify and designate European Critical Infrastructure. Formation Working Group gave us also good chance to discuss about problems which are connected with essential or critical infrastructures at national level.</p>	
<i>Step 4 – Application of the cross-cutting criteria</i>	Estonia used guidelines prepared by EC	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	Estonia used EC guidelines. The Commission together with the Member States developed guidelines for the application of the cross-cutting and sectoral criteria and approximate thresholds.	
Identification of potential ECI on an ongoing basis (Art 3.1)	Is carried out on an ongoing basis as needed.	
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	Ministry of Economic Affairs and Communications (responsible for transport and energy) in co-operation with operators.	
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	<p>Ministry of Economic Affairs and Communications (responsible for transport and energy) informs other MS.</p> <p>Estonia undertook communication with other MS through pre-existing contacts with the neighbouring MS.</p>	
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	<p>Ministry of Economic Affairs and Communications lead discussion with other MS.</p> <p>In 2010 Ministry of Economic Affairs and Communications formed working group. Working group involved Finland, Lithuania and Latvia experts.</p>	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	Ministry of the Interior. Formal letter.	
Agreement for the designation of the ECI (Art. 4.3)	This kind agreement requires the consent of both parties.	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	Ministry of the Interior. Formal letter. Ministry of the Interior informed the Commission as was required by the Directive. There was no response from the Commission once the reports were submitted.	
Informing the owner/operator of the designated ECI (Art. 4.5)	In transport and energy sector Ministry of Economic Affairs and Communications. Formal letter.	
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The provider of a vital service prepares a continuity risk assessment and plan for planning the ensuring of the continuity of the vital service, for risk assessment and for restoring the continuity. A service provider who is required to prepare a risk assessment and a plan for the first time shall submit these to the organising authority for approval pursuant to the procedure provided by the Emergency Act no later than within a year as of the moment it meets the characteristics of a service provider provided by law.	<i>Emergency Act (Article 39 p 1)</i> <i>Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan (Article 3 p 2)</i>
Verification that the OSP or equivalent is in place	The provider of a vital service submits the continuity risk assessment and plan for approval to the authority organising the continuity of the vital service.	
Verification that the OSP or equivalent is	The authority organising the continuity of the vital service verifies the compliance of the continuity risk assessment and plan with the requirements provided by law and approves the	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
appropriately and regularly reviewed	<p>continuity risk assessment and plan within 30 days after receiving the continuity risk assessment and plan.</p> <p>The authority organising the continuity of the vital service may extend the deadline for the approval of the continuity risk assessment and plan by 30 days with good reason.</p> <p>The authority organising the continuity of the vital service does not approve a continuity risk assessment and plan if the filed documents do not meet the requirements, the descriptions and assessments in the documents are insufficient, they do not comply with actual circumstances or on the basis of the documents it is not possible to sufficiently ensure the continuity of the vital service.</p> <p>The authority organising the continuity of the vital service sends the continuity plan to an authority who will be involved or probably involved in the restoration of the vital service in case of an interruption of the service for obtaining the opinion of that authority. The Bank of Estonia sends the continuity risk assessment and plan of the provider of the vital services to the Financial Supervision Authority for giving an opinion.</p> <p>A service provider shall assess whether a risk assessment and a plan are up to date at least once every two years or whenever critical activities, threats or other significant circumstances affecting the provision of the vital service change. If necessary, the service provider shall initiate the updating of the risk assessment and the plan and shall present it to the organising authority for approval pursuant to the procedure provided by the Emergency Act.</p> <p>If in the course of the assessment referred it becomes clear that the risk assessment and the plan are up to date and they need not be updated, the service provider shall inform the organising authority thereof.</p> <p>If the service provider has failed to update the risk assessment and the plan due to changes in the significant circumstances and to submit these to the organising authority for approval, the organising authority has the right to demand that the service provider initiate the updating of the risk assessment and the plan and submit the updated risk assessment and plan to the organising authority for approval.</p>	<p>Emergency Act (Article 40)</p> <p>Requirements and procedure for a continuity risk assessment</p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		<i>and plan of a vital service, for the preparation thereof and the implementation of a plan (Article 4)</i>
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The Emergency Act requires vital service providers to implement protection measures which also include SLO equivalent requirements.	
Function of the SLO (Art. 6.1)	See above.	
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	See above.	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	See above.	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations		
Performance of threat assessments within ECI subsector within one year following the designation of ECI		
Reporting of generic data on summary basis on the types of risks, threats and		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
vulnerabilities to the Commission per ECI subsector		
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	Ministry of the Interior choose staff who carry out CIP POC duties.	
MS body(-ies) serving as ECIP contact point		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<i>Hädaolukorra seadus – Emergency Act</i>	Link.
Scope of national CIP policy		
Sectors of critical importance	<p>The Ministry of Economic Affairs and Communications shall organise the continuity of the following vital services:</p> <ol style="list-style-type: none"> 1) Electricity supply; 2) Natural gas supply; 3) Liquid fuel supply; 4) Ensuring the operability of national roads; 5) Phone service; 6) Mobile phone service; 7) Data transmission service; 8) Digital identification and digital signing. <p>The Ministry of Social Affairs shall organise the continuity of emergency care for the purposes of the Health Services Organisation Act.</p>	<p><i>Emergency Act (Article 36).</i></p> <p>Sectoral laws:</p> <p>ehitusseadustik,</p> <p>elektrituruseadus,</p> <p>elektroonilise side seadus,</p> <p>isikut tõendavate dokumentide seadus,</p> <p>kaugkütteseadus,</p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>The Bank of Estonia shall organise the continuity of the following vital services:</p> <ol style="list-style-type: none"> 1) payment services; 2) cash circulation. <p>Local authorities who organise services provided by a provider of a vital service and on whose territory lives over 10,000 residents organise in their administrative territory the continuity of the following vital services:</p> <ol style="list-style-type: none"> 1) district heating; 2) ensuring the operability of local roads; 3) water supply and sewerage. <p>Estonia identified vital services (critical infrastructure) using specific methodology. According methodology the services were rated in the following categories:</p> <ol style="list-style-type: none"> 1. Number of service users or number of people benefitting from the service (during the year). 2. Necessity for use by private individuals or companies throughout the year. 3. Service replaceability (subcategories a) replacement timeframe, b) equivalency of the alternative.) 4. Connection to other socially important services (vital services and services of general interest) (subcategories a) how many services are influenced? b) extent of impact on connected services.) 5. Is the service itself an alternative to other socially important services (vital services and services of general interest)? 6. Timeframe of perceiving the consequence. 7. Influence on the life and health of the person in need of the service. <p>Based on these criteria, Estonia identified 14 vital services (critical infrastructure). All this sector set down in Emergency Act.</p> <p>After that Estonia identified operator's criteria's. This operators hold most important infrastructure in Estonia. Criteria's set down in sectoral laws.</p>	<p>krediitiasutuste seadus,</p> <p>maagaasiseadus,</p> <p>tervishoiuteenuste korraldamise seadus,</p> <p>vedelkütuse seadus,</p> <p>ühisveevärgi- ja kanalisatsiooni seadus.</p>
Number of national CI	14 – vital services	<i>Emergency Act (Article 36)</i>
Number of national CI operators	140	<i>MOI</i>
Responsibilities allocated to Ministries, bodies, and offices		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Definition of scope and objectives of the national CIP strategy	<p>For the protection of national CI are responsible:</p> <ol style="list-style-type: none"> 1. Ministry of the Interior; 2. Authorities organising continuity of vital services; 3. Vital services operators. <p>The Ministry of Interior is responsible for the coordination of arrangements for the sustainability of vital services at the national level. Ministry of the Interior is responsible for vital services protection policy making.</p> <p>Other ministries, local government and Bank of Estonia in co-operation with vital services provider are responsible for the continuous operation of the vital services that fall under their responsibility. For example, Ministry of Economic Affairs and Communication is responsible for the continuous operation of gas and electricity supply, Ministry of Social Affairs for medical care etc.</p> <p>Operators play a key role. Vital services operators are responsible for capability of the provider to ensure continuous operation and to quick restore continuous operation after an interruption of the vital service.</p> <p>Authorities organising continuity of vital services establish requirements for the operators. For example obligation hold power generator or stocks, requirements for service recovery time, information exchange, personnel, technical and ICT systems etc.</p> <p>Operators compose risk assessment and plan. During risk assessment process operators planning measures that prevent interruptions of the vital service, including reduce the dependency on other vital services, essential contract partners, suppliers and information systems through duplicating technical systems, contracts, staff and other means important to the provision of the service, using alternative solutions, having and stocking necessary resources and other similar actions.</p> <p>The risk analyses and plans unfold all the activities that need to function for the service as a whole to operate, the resources that the company needs in order to continue operation, the possible threats and scenarios which could result in disruptions, which precautionary measures could/should be taken to mitigate the discovered risks and much more.</p> <p>Operators risk assessments and plans are input for organising authorities to compose national emergency response plans.</p>	Emergency Act (Article 37 and 38).

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	The main responsibilities for identifying the vulnerabilities of each sector are described below:	
Coordination of ministries, bodies and offices concerned	<p>Obligations of authorities organising continuity of vital services:</p> <ol style="list-style-type: none"> 1) coordinate the ensuring of the continuity of the vital service, considering the risk dependency of vital services; 2) establish requirements for the continuity of a vital service; 3) advise providers of vital services; 4) exercise supervision over ensuring the continuity of vital services, including over the implementation of measures that prevent interruptions of vital services; 5) approve the continuity risk analyses and plans of providers of vital services; 6) coordinate the resolution of an emergency, prepare an emergency response plan and organise risk communication and crisis management exercises <p>Provider of a vital service is required to:</p> <ol style="list-style-type: none"> 1) prepare the continuity risk assessment and plan of the vital service provided thereby; 2) implement measures that prevent interruptions of the vital service, including reduce the dependency on other vital services, essential contract partners, suppliers and information systems through duplicating technical systems, contracts, staff and other means important to the provision of the service, using alternative solutions, having and stocking necessary resources and other similar actions; 3) ensure the capability to guarantee the continuity of and to quickly restore the service provided thereby during an emergency or another similar situation, including in the event of a technical failure or an interruption of the supply or another vital service; 4) immediately notify the authority organising the continuity of the vital service of an interruption of the vital service, a risk of an interruption, an event significantly interfering with the continuity of the vital service or an impending risk of such an event; 5) participate in resolving an emergency according to the emergency response plan; 6) provide the authority organising the continuity of the vital service with information on the provision of the vital service at the request thereof; 7) organise exercises in order to verify the continuity of the vital service provided thereby at least once every two years; 8) perform other obligations provided by legislation for ensuring the continuity of the vital service. 	<i>Emergency Act (Article 37-38)</i>
Communication with owners/operators	Authorities organising continuity of vital services communicate with operators.	<i>Emergency Act (Article 37)</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	<p>Authorities organising continuity of vital services carries out supervision over ensuring the continuity of vital services, including over the implementation of measures that prevent interruptions of vital service. Its mean that authorities exercise state supervision over vital service providers.</p> <p>Ministry of the Interior exercise administrative supervision over the compliance with Emergency Act and legislation established on the basis thereof. Its mean that Ministry of the Interior controls activities of authorities organising continuity of vital services.</p> <p>Rescue Board exercise administrative supervision over local authorities.</p> <p>Republic of Estonia Information System Authority exercise administrative or state supervision over the compliance with electronic security of provision of vital service.</p> <p>In order to exercise the state supervision provided by Emergency Act, law enforcement agencies may apply the special measures of state supervision provided for in §§ 30–32, 49 and 50–53 of the Law Enforcement Act on the basis and pursuant to the procedure provided for in the Law Enforcement Act. For example: Questioning and requiring of documents, summons and compelled attendance, examination of movable, entry into premises, examination of premises, taking into storage of movable etc.</p> <p>Upon failure to comply with a precept, the upper limit of penalty payment for each imposition thereof pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act is 2000 euros.</p>	Emergency Act (Article 41, 45, 46) Law Enforcement Act (Article 30-32, 49-53).
Other relevant aspects of national authorities involved in CIP protection	-	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	The law determines the conditions under which a person acting as an operator becomes a provider of Critical infrastructure (described in the table above). Each operator name contact person for authorities organising continuity of vital services.	Emergency Act (Article 38 p 1 and 2)
- Preparation of a security plan	It is described in the table above	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
- Review of the plan (timing)	It is described in the table above	
- Reporting incidents	According Emergency Act operators must immediately notify the authority organising the continuity of the vital service o of an interruption of the vital service, a risk of an interruption, an event significantly interfering with the continuity of the vital service or an impending risk of such an event. In case of cyber incident operator must inform Information System Authority.	<i>Emergency Act (Article 38)</i> <i>Cybersecurity Act (article 8)</i>
- Exchange of information	Information exchange is a routine regular activity. Common channels/format: e-mail, telephone, meetings.	<i>Hädaolukorra seadus(Article 37-38)</i>
Other distinctive features of the national framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Operators must implement all hazards approach in their risk assessment and plan.</p> <p>Estonia does not have CIP ISO, IEC, EVS etc. standards, but has legal requirements for operators. The requirements for the continuity of a vital services establish the head of the authorities organising the continuity of the vital services.</p> <p>The main strategy document for national internal security as a whole is the Internal Security Development Plan 2015 – 2020 (Unfortunately only available in Estonian: https://valitsus.ee/sites/default/files/content-editors/arengukavad/taiendatud_siseturvalisuse_arengukava_2015-2020.pdf). This also covers the field of vital services.</p> <p>At this moment Ministry of the Interior preparing new strategy for 2020-2023.</p> <p>Cybersecurity Estonia has Cyber Security Strategy 2014–2017. At this moment Ministry of Economic Affairs and Communications preparing new strategy for 2019-2022. 23.05.2018 came into the force Cybersecurity Act. Vital services providers are subjects of this Act.</p>	<p>https://www.siseministeerium.ee/en</p> <p>https://www.riigiteataja.ee/en/eli/523052018003/consolide</p>

Finland

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>No formal transposition Law, national CIP procedures were reviewed to comply with the Directive.</i>	<i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report</i>
Definitions (Art 2)		
'critical infrastructure'	<i>No formal transposition</i>	
'European critical infrastructure'	<i>No formal transposition</i>	
'risk analysis'	<i>No formal transposition</i>	
'sensitive critical infrastructure protection related information'	<i>No formal transposition</i>	
'protection'	<i>No formal transposition</i>	
'owners/operators of ECI'	<i>No formal transposition</i>	
Other relevant national definitions	<i>No formal transposition</i>	
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	See table below (concerning national CIP policy)	
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The National Emergency Supply Agency, Ministry of Economic Affairs, Ministry of Transport and Communications and Ministry of the Interior	<i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report</i>
Application of the procedure for the identification of ECI (as per Annex III)	The abovementioned authorities have identified potential ECI according to the cross-cutting criteria in the sectors and subsectors defined in article 3.	
<i>Step1 – Application of sectoral criteria</i>		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<i>Step 2 – Application of the definition of critical infrastructure</i>		
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>		
<i>Step 4 – Application of the cross-cutting criteria</i>		
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)		
Identification of potential ECI on an ongoing basis (Art 3.1)	There is no formalised timing for reconsidering national CI and identifying other ECI. The cross-sectoral and cross-administrative co-operation between Finnish authorities concerning CI is on-going.	
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	Not applicable.	
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	See above.	
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	See above.	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	See above.	
Agreement for the designation of the ECI (Art. 4.3)	See above.	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	See above.	
Informing the owner/operator of the designated ECI (Art. 4.5)	See above.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly		
Verification that the OSP or equivalent is in place	See above.	
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	Procedures are in place at sector level. For example, electricity transmission and distribution network recovery plans are part of the business specific contingency planning in accordance with the Electricity Market Act. The task of supervising the contingency plans of the electricity and natural gas network operators, including the recovery plans, rests with the Energy Authority (ref. Acts 587/2017, 590/2017).The National Emergency Supply Organisation has an important role to play in, for example, risk assessments and stakeholder co-operation. Similarly, the preparedness arrangements in the transport and logistics sectors are based both on sector specific legislation (Act 320/2017 for rail and air transport) and voluntary business agreements and activities.	
Function of the SLO (Art. 6.1)	See above.	
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	See above.	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	See above.	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations		
Performance of threat assessments within ECI subsector within one year following the designation of ECI	See above.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	See above.	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The appointment of ECIP contact points has been discussed horizontally in a cross-sectoral manner between relevant actors.	
MS body(-ies) serving as ECIP contact point	The National Emergency Supply Agency and Ministry of the Interior.	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<p><i>Act on the Measures Necessary to Secure Security of Supply (1390/1992)</i></p> <p><i>Government decision on the security of supply goals of 5 December 2013, Finnish Statute Book 857/2013</i></p> <p><i>Government decision on the security of supply goals is currently being updated.</i></p>	
Scope of national CIP policy		
Sectors of critical importance	<p>The latest decision of the Council of State on the objectives of security of supply (857/5.12.2013) states that security of supply is based on international markets and domestic measures and resources.</p> <p>The objective is to ensure the continuity of production and infrastructure vital to society under all circumstances in such a way that the living conditions of the population and the critical functions of society are secured also in the event of disruptions and emergencies, including a state of defence.</p> <p>The objectives are divided into two categories: securing critical infrastructure and securing critical production and services.</p>	<i>Government decision on the security of supply goals of 5 December 2013, Finnish Statute Book 857/2013</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>Critical infrastructure includes:</p> <ul style="list-style-type: none"> • Energy production, transmission and distribution networks • Data-communication systems, networks and services (including mass communication) • Financial services • Transport and logistics • Water supply • Construction and maintenance of infrastructure • Waste management in special circumstances <p>Critical production and services include:</p> <ul style="list-style-type: none"> • Food supply • Health care and basic services • Industry • Production and services supporting military defence 	
Number of national CI	n.a.	
Number of national CI operators	n.a.	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	The objective is to ensure the continuity of production and infrastructure vital to society under all circumstances in such a way that the living conditions of the population and the critical functions of society are secured also in the event of disruptions and emergencies, including a state of defence.	"Government decision on the security of supply goals" Given in Helsinki, nr 857/5.12.2013.
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy		
Coordination of ministries, bodies and offices concerned	National Emergency Supply Agency (NESA) is responsible for coordinating measures for safeguarding continuity of critical infrastructure and critical production in Finland. The NESA promotes and co-ordinates public authorities' readiness to manage and guide the national economy in emergency situations	"Government decision on the security of supply goals" Given in Helsinki, nr 857/5.12.2013.
Communication with owners/operators		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	The ministries responsible for the most important functions of society shall recognise the most important ICT structures, services, technical maintenance and related expertise and data storages, together with the National Emergency Supply Organisation (NESO). The related risks, vulnerabilities and international dependencies, as well as their effects, must be recognised and evaluated.	"Government decision on the security of supply goals" Given in Helsinki, nr 857/5.12.2013.
Other relevant aspects of national authorities involved in CIP protection	The NESO ensures the functioning of the national technical infrastructures, safeguards the production of necessary goods and services under emergency conditions, analyses threats against security of supply and drawing up plans for countermeasures	"Government decision on the security of supply goals" Given in Helsinki, nr 857/5.12.2013.
Responsibilities allocated to operators of national CI		
- Appointment of a security officer		
- Preparation of a security plan	Critical infrastructure protection and security of supply in Finland are an integrated part of the comprehensive security concept and aims at securing the continuity of critical economic functions and critical infrastructures required for citizens' basic livelihood and national defence under all circumstances. The Finnish model for economic security is based on well-functioning markets and a competitive economy. The majority of critical production, services and infrastructures are provided by private sector operators. Consequently, co-operation between the public and private sectors is a key success factor for securing these critical functions. For this motive, a broad variety of private sector operators and relevant public authorities form a co-operation network called the National Security of Supply Organisation (NESO). Participation in the work of NESO is voluntary for private sector organisations. Whereas the focus is strongly on voluntary public-private co-operation, also sector-specific regulation exists, e.g. in the energy sector.	
- Review of the plan (timing)		
- Reporting incidents		
- Exchange of information		
Other distinctive features of the national CIP framework		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Cybersecurity measures: The aim of Finland's national cyber security strategy is to respond to cyber threats, strengthen the overall security of society and ensure the smooth functioning of the cyber domain in all circumstances. The Strategy presents 10 objectives that, when implemented, provide Finland with the capability nationally to control the intentional and unintentional adverse effects of the cyber domain as well as to respond to and recover from them. One of the objectives is that Finland shall strengthen its national cyber security by participating actively and effectively in international discussions and co-operation on cyber security. The Foreign Ministry coordinates this international activity. The Security Committee monitors the implementation of Finland's Cyber Security Strategy. The implementation guide for the Cyber Security Strategy has been updated for 2017–2020 to respond to the changes in the cyber security environment.</p> <p>The Comprehensive security approach The Security Strategy for Society 2017 is a government resolution that harmonises the set of national principles regarding preparedness and guides the preparedness actions taken by the administrative branches. - Comprehensive Security is a Finnish preparedness co-operation model in which the vital functions of society are looked after through co-operation between the authorities, the business community, organisations and citizens.</p> <p>The Internal Security Strategy In the Strategy, internal security refers to those aspects of society that ensure everyone can enjoy the rights and freedoms guaranteed by the rule of law without fear or insecurity caused by crime, disorder, accidents or national or international events. The Strategy includes a foresight section describing the forces of change that are likely to influence internal security in Finland in the near future. The Strategy's action plan has eight sets of measures and a total of 39 actions for managing these forces of change and thus enabling the objective of the Strategy to be achieved.</p>	<p><i>Suomen kyber turvallisuusstrategian toimeenpano-ohjelma 2017 - 2020; The Security Committee; 2017</i></p> <p><i>Security Strategy for Society 2017.</i></p> <p><i>Internal Security Strategy 2017.</i></p>

France

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Defense Code and the General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of September 26, 2008, later amended by the General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014</i> <i>MEMBER STATE DOES NOT CONSIDER NATIONAL TRANSPOSITION NECESSARY</i>	
Definitions (Art 2)		
'critical infrastructure'	Critical Infrastructure: Any establishment, installation or work whose damage or unavailability or destruction as a result of malicious acts, sabotage or terrorism could, directly or indirectly: endanger the war or economic potential, security or survival capacity of the nation, as its activity is difficult to substitute or replaceable; or seriously jeopardise the health or life of the population.	<u>General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014</u>
'European critical infrastructure'	European Critical Infrastructure: Critical infrastructure located in EU Member States whose disruption or destruction would have a significant impact on at least two Member States.	
'risk analysis'	N/A	
'sensitive critical infrastructure protection related information'	N/A	
'protection'	N/A	
'owners/operators of ECI'	N/A	
Other relevant national definitions	N/A	
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Sectors of Critical Importance: 12 sectors in four areas of responsibility: - Basic Human Needs: Food, Water management, Health - Sovereign activities: Civilian activities, Legal activities, Military activities - Economic activities: Energy, Finance, Transport - Technological infrastructure: Communication, technologies and broadcasting, Industry, Space & research	<u>THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,</u>
Identification of the ECI (Art. 3)		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
MS body(-ies) responsible for the identification of potential ECI	For the sectors to which the Directive applies, the coordinating ministries concerned carry out, in liaison with the operators and with the methodological support of the SGDSN, a sector analysis to identify the infrastructures that meet the criteria mentioned above (definition of Critical Infrastructure), both in France and in other MS (potential ECI).	<i>General Instruction</i> <i>Inter-ministerial N. 6600</i> <i>SGDN/PSE/PPS of January 7, 2014</i> (Article 7.3)
Application of the procedure for the identification of ECI (as per Annex III)		
<i>Step1 – Application of sectoral criteria</i>	ECI in France are normally selected from the identified CI. In the opposite case, the designated infrastructure must at least be globally covered by an OSP (pursuant to the national CIP legislation or have this procedure applied beforehand). In any other case, the infrastructure cannot be designated ECI. The requesting Member State shall be informed thereof.	<i>General Instruction</i> <i>Inter-ministerial N. 6600</i> <i>SGDN/PSE/PPS of January 7, 2014</i> (Article 7.2)
<i>Step 2 – Application of the definition of critical infrastructure</i>	Sectoral analysis aimed at identifying infrastructures meeting the criteria mentioned above (see definition of CI, above), both in France than in the other Member States (potential ECI).	<i>General Instruction</i> <i>Inter-ministerial N. 6600</i> <i>SGDN/PSE/PPS of January 7, 2014</i> (Article 7.2)
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	The work of identifying ECI abroad is undertaken during the drafting of the National Security Directives and OSPs, in all sectors of activity, as part of the analysis of international interdependencies.	<i>General Instruction</i> <i>Inter-ministerial N. 6600</i> <i>SGDN/PSE/PPS of January 7, 2014</i> (Article 7.2)
<i>Step 4 – Application of the cross-cutting criteria</i>	Connected to sectoral analysis.	<i>General Instruction</i> <i>Inter-ministerial N. 6600</i> <i>SGDN/PSE/PPS of January 7, 2014</i> (Article 7.2)
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	Thresholds are defined on a case by case basis, in accordance with the national thresholds defined in the National Security Directives.	<i>General Instruction</i> <i>Inter-ministerial N. 6600</i> <i>SGDN/PSE/PPS of January 7, 2014</i> (Article 7.3)
Identification of potential ECI on an ongoing basis (Art 3.1)	Ongoing identification is based on the drafting and revision of national security directives and OSPs.	<i>General Instruction</i> <i>Inter-ministerial N. 6600</i> <i>SGDN/PSE/PPS of January 7, 2014</i> (Article 7.2)
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	SGDSN, though French law specifies that the Directive does not impose any particular rules or methods for this, so the agreement can simply take the form of an informal exchange of letters between the MS.	<i>General Instruction</i> <i>Inter-ministerial N. 6600</i> <i>SGDN/PSE/PPS of January 7, 2014</i> (Article 7.3)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	SGDSN - The discussion can simply take the form of an informal exchange of letters between the MS.	General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.3)
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	For the designation of ECI, a dialogue should be sought between the Member States concerned, with the possible support of the Commission. The SGDSN is the contact point for the protection ICE, responsible for coordinating issues related to the application of the Directive both within the Member State and with other Member States and the Commission. The discussion can simply take the form of an informal exchange of letters between the MS.	General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.3)
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	SGDSN – channels are not specified	General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.3)
Agreement for the designation of the ECI (Art. 4.3)	An agreement is considered achieved when the coordinating ministry informs ICE operators located in France of the choice made, specifying the IC's identification number.	General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.3)
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	SGDSN, channels not specified	General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.3)
Informing the owner/operator of the designated ECI (Art. 4.5)	Coordinating Ministry. Once the agreement has been obtained, the coordinating ministry informs by a designation letter ICE operators located in France of the choice made, specifying the IC's identification number.	General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.4)
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	<p>CIP operators must draw up both an operator security plan (OSP), which describes the operator's security policy and organisation, and specific protection plans for each critical infrastructure identified.</p> <p>The OSP is subject to the approval of the commission: either inter-ministerial or zonal (in the case of operators whose scope of activity does not exceed the area of responsibility of the defence zone). Specific protection plans for each critical infrastructure are approved by the Department level Prefect.</p>	<p>General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.2)</p> <p>THE CRITICAL INFRASTRUCTURE</p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Verification that the OSP or equivalent is in place	Verification is performed through inspections coordinated by the Zone Prefect	PROTECTION IN FRANCE, SGDSN, 2017,
Verification that the OSP or equivalent is appropriately and regularly reviewed	Verification is performed through inspections coordinated by the Zone Prefect	
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	Once designated, operators must assume several types of responsibility: appointing a security liaison officer (who has the necessary clearance and shall represent the operator to the administrative authority) and drawing up both an operator security plan (OSP), which describes the operator's security policy and organisation, and specific protection plans for each critical infrastructure identified.	THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,
Function of the SLO (Art. 6.1)	CIP operators must appoint a security liaison officer (with security clearance), who shall represent the operator to the administrative authority for all questions relating to facility security and security plans (inter alia OSPs) .	THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	The operator shall inform the administrative authority of the name of the person responsible for exercising the function of security liaison officer. This name is listed in the annex of the OPS.	<i>General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.2)</i>
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	<p>As the linchpins of this system, critical operators must analyse the risks to which they are exposed and apply the protection measures within their remit – particularly the VIGIPIRATE plan. The development of the VIGIPIRATE strategy employs a top-down strategy in which the government is guiding a national-level risk assessment programme for each sector. The SLO is main interlocutor of the coordinating minister.</p> <ul style="list-style-type: none"> • The objectives for this risk assessment are set by the SGDSN together with other ministries. These objectives were then sent to operators of vital importance (identified by SGDSN together with the ministries) that maintain services / activities of vital importance. Each ministry developed the list of vital operators for its sector of responsibility and then initiated the risk assessment process in that sector. • Once identified as a "critical operator", the designated operators must then execute a risk assessment against the objectives and threats identified by the ministry and validated by SGDSN. • Verification is performed through inspections coordinated by the Zone Prefect • France is divided in 13 defence and security zones (including over-sea territories). The zone prefect is the territorial stakeholder in charge of coordinating the CIP system. His/her responsibilities include organisation, 	THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>support for préfectures and informational liaison between the central and local levels. He/she also coordinates inspections of critical infrastructure within his area of jurisdiction.</p> <ul style="list-style-type: none"> the so-called "background checks" procedure enables the CI operators to ask the administrative authority to check that the characteristics of the person wishing to access his critical infrastructure are not at odds with the security of the site; 	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	SGDSN	<i>the General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.1)</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	SGDSN – main content of threat assessment not specified	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	SGDSN– main content of summary not specified	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.1) specifies that the SGDSN is responsible for coordinating issues related to the application of the Directive both within the Member State and with other Member States and the Commission.	<i>General Inter-ministerial Instruction N. 6600 SGDN/PSE/PPS of January 7, 2014 (Article 7.1)</i>
MS body(-ies) serving as ECIP contact point	SGDSN	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	Same as table above. The policy on the critical infrastructure protection is enshrined in the Defence Code (in particular Articles R. 1332-1 to 1332-42, taken on the basis of Articles L. 1332-1 à 1332-7). It provides the legislative and regulatory framework for involving operators of critical infrastructures, whether public or private, in the national system of protection against terrorism, sabotage and malicious acts and	<ul style="list-style-type: none"> Defence Code – Articles L. 1332-1 to L. 1332-7, L. 2151-1 to L. 2151-5 and R. 1332-1 to R. 1332-42.

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	for analysing risks and applying measures that concern them in accordance with public authorities' decisions.	<ul style="list-style-type: none"> General Inter-ministerial Instruction N. 6600 on the security of activities of vital importance of January 7, 2014
Scope of national CIP policy		
Sectors of critical importance	Same as table above.	THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,
Number of national CI	1438	
Number of national CI operators	299	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	Developed and coordinated by the General Secretariat for Defence and National Security (SGDSN), the critical infrastructure protection (CIP) policy provides a framework in which public or private critical operators can assist in implementing the national security strategy in terms of protection against malicious acts (terrorism, sabotage) and natural, technological and health risks. As the linchpins of this system, critical operators must analyse the risks to which they are exposed and apply the protection measures within their remit – particularly the VIGIPIRATE plan. The 2013 White Paper on Defence and National Security establishes this policy as a means of strengthening the Nation's resilience.	THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	Competent Ministries are tasked with drawing up the National Security Directive for each sector (and subsector) by stating which challenges, vulnerabilities and threats must be taken on board and by defining the sector's security objectives.	THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,
Coordination of ministries, bodies and offices concerned	<p>By delegation of the Prime Minister, the General Secretariat for Defence and National Security (SGDSN) is responsible for the cross-government coordination and organisation of the system. It determines the scope of the CIP policy, particularly as regards method and doctrine. It approves the National Security Directives. It also lays down the cybersecurity rules that must be applied by critical operators.</p> <p>Ministries Ministries are tasked with drawing up the National Security Directive for each sector (and subsector) by stating which challenges, vulnerabilities and threats must be</p>	THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>taken on board and by defining the sector's security objectives. Ministries are also the operators' main points of contact.</p> <p>Ministry of Interior The Ministry of the Interior oversees the territorial organisation of the system so as to support the action of zone and <i>département</i>-level.</p> <p>Defence and security zone prefect France is shared in 13 defence and security zone (including over-sea territories). The zone prefect is the territorial stakeholder in charge of coordinating the CIP system. His responsibilities include organisation, support for <i>préfectures</i> and informational liaison between the central and local levels. He also coordinates inspections of critical infrastructure within his area of jurisdiction</p> <p>Department level prefect For each critical infrastructure, the <i>département</i>-level prefect approves the specific protection plan drawn up by the operator. He also drafts an external protection plan setting out the intervention and vigilance measures to take if this critical infrastructure should ever find itself under threat or attack.</p> <p>Critical operators Once designated, operators must assume several types of responsibility: appointing a security liaison officer (who shall represent the operator to the administrative authority) and drawing up both an operator security plan (OSP), which describes the operator's security policy and organisation, and specific protection plans for each critical infrastructure identified</p>	
Communication owners/operators with	Competent Ministries are also the operators' (via their security liaison officer) main points of contact.	THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	<p>Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)</p> <ul style="list-style-type: none"> - France is divided in 13 defence and security zones (including over-sea territories). The zone prefect is the territorial stakeholder in charge of coordinating the CIP system. His/her responsibilities include organisation, support for <i>préfectures</i> and informational liaison between the central and local levels. He/she also coordinates inspections of critical infrastructure within his area of jurisdiction. 	THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE, SGDSN, 2017,

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Other relevant aspects of national authorities involved in CIP protection	The external protection plan defines the planned vigilance, prevention, protection and response measures provided for by the public authorities, in particular by the security forces, under the authority of the Department level prefect. It thus describes the procedures for intervention on the CI in the event of an attack, in coordination with the operator.	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Same as table above	
- Preparation of a security plan	Same as table above CIP operators must draw up both an operator security plan (OSP), which describes the operator's security policy and organisation, and specific protection plans for each critical infrastructure identified.	
- Review of the plan (timing)	Same as table above	
- Reporting incidents	Operators are in contact (particularly regarding the level of threat and the implementation of the VIGIPIRATE plan within their establishment) with the coordinating ministry of their sector <i>via</i> their security liaison officer. The control of a point of vital importance by a defence and security commission also enables information to be reported.	
- Exchange of information	Same as table above	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Approach</p> <p>In 2013, the SGDSN launched a process for revising the national security directive. One of its objectives is to adopt an all-hazards approach so as to encourage operators to make preparations for every critical eventuality that may affect their staff, premises, networks and production facilities by drawing up a business continuity plan</p> <p>Review</p> <p>SGDSN and competent Ministries review the strategy as needed (last review in 2013)</p> <p>Business continuity planning</p>	<i>The Critical Infrastructure Protection in France</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>In 2013, the SGDSN launched a process for revising the national security directive. One of its objectives is to adopt an all-hazards approach so as to encourage operators to make preparations for every critical eventuality that may affect their staff, premises, networks and production facilities by drawing up a business continuity plan (BCP). These documents are a requirement on the part of critical infrastructure. The SGDSN has produced a methodological guide to drawing up BCPs, which the general public has been able to access since 2013</p> <p>Cybersecurity</p> <p>As early as 2008, the White Paper on Defence and National Security identified cyber-attacks as one of the main threats to defence and security. To tackle those new threats, Article 22 of the 2013 Military Programming Law now requires critical operators to reinforce the security of their information systems. These requirements apply to critical information systems identified by operators and involve reporting incidents, implementing a core set of security rules and making use of qualified detection service providers and products. The National Cybersecurity Agency (ANSSI) is in charge of implementing these provisions within the SGDSN and has worked closely with the ministries and operators to define rules that are at once effective, appropriate and sustainable for operators.</p>	

Germany

OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>National Law revising the energy industry regulation (entered into force on August 4, 2011 – Law amending the energy industry act - Energiewirtschaftsgesetz-EnWG) and Ordinance on the protection of transmission system (entered into force on January 10, 2012 - Verordnung zum Schutz von Übertragungsnetzen-ÜNetzSchV)</i>	
Definitions (Art. 2)		
'critical infrastructure'	"Critical infrastructure" : organisational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences' (CI-definition since 2003, fixed in National Strategy, referred to resp. implemented by law, e.g. Raumordnungsgesetz/ROG [Federal Regional Planning Act], Gesetz über den Zivilschutz und Katastrophenhilfe des Bundes/ZSKG [Civil Protection and Disaster Assistance Act], IT-Sicherheitsgesetz/IT-SiG [IT-Security Act])	<i>National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009</i> <i>§ 12g Abs. 1 Satz 1 EnWG</i>
'European critical infrastructure'	"European critical infrastructures" : installations whose disturbance or destruction may have significant effects in at least two Member States "... Anlagen oder Teile von Anlagen des Übertragungsnetzes, deren Störung oder Zerstörung erhebliche Auswirkungen in mindestens zwei Mitgliedstaaten der Europäischen Union haben kann (europäisch kritische Anlage)"	<i>Protecting Critical Infrastructures – Risk and Crisis Management. A guide for companies and government authorities, Berlin 2008.</i>
'risk analysis'	systematic procedure for identifying risk values.	<i>Issue addressed in § 1 Abs. 2 ÜNetzSchV</i> <i>Issue addressed in § 12g Abs. 4 EnWG in context with § 6 ÜNetzSchV</i>
'sensitive critical infrastructure protection related information'	n.a.	<i>BBK-Glossar, Ausgewählte zentrale Begriffe des Bevölkerungsschutzes</i> <i>(www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/B)</i>
'protection'	n.a.	
'owners/operators of ECI'	n.a.	
Other relevant national definitions	See BBK Glossary for Civil Protection	

OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		and 8 Praxis BS BBK Glossar.pdf? blob=publicationFile)
Scope (Art. 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	- Due to the result of the identification process only the energy sector sub-sector electricity is in scope	§ 12g EnWG in context with ÜNetzSchV
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	Federal Ministry for Economic Affairs and Energy (BMWi) (clarification: The Federal Network Agency (BNetzA) does not decide on potential ECI. Only the „designation“ according to Art. 4 of the Directive is done by BNetzA according to § 12g EnWG).	
Application of the procedure for the identification of ECI (as per Annex III)	For the procedure of the identification of ECI, BMWi has relied on the "Non-Binding Guidelines for the application of the Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection".	
Step1 – Application of sectoral criteria	see above	
Step 2 – Application of the definition of critical infrastructure	see above	
Step 3 – Application of the transboundary element of the definition of ECI	see above	
Step 4 – Application of the cross-cutting criteria	see above	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	see above	

OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Identification of potential ECI on an ongoing basis (Art 3.1)	Every two years	§ 1 Abs. 1 Satz 1 ÜNetzSchV
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	Federal Network Agency (BNetzA) Cooperating: Federal Ministry of the Interior, Building and Community (BMI) / Federal Office of Civil Protection and Disaster Assistance (BBK)	§ 12g EnWG
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	The relevant ministry of the member state with the potential ECI contacts the responsible ministry of the member state that might be concerned of a loss of the potential ECI.	
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	If a plant is to be designated as an ECI, a consultation pursuant to Directive 2008/114 / EC shall be carried out beforehand by the Federal Ministry for Economic Affairs and Energy. The relevant ministry of the member state with the potential ECI contacts the responsible ministry of the member state that might be concerned of a loss of the potential ECI. The query and the following discussions can take place by e-mail, by letter, by telephone or by a personal meeting.	§ 2 ÜNetzSchV
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	BMI as the CIP PoC has to be involved in order to fulfil the prescribed information duty. But this happens on the basis of information by the sector-responsible ministry that must be streamlined into accordance with this duty.	
Agreement for the designation of the ECI (Art. 4.3)	The agreement is considered to be achieved when a bi-lateral agreement has been signed by the involved member state(s).	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The competent ministry informs BMI in its function as PoC about the number of designated ECI per sector and the number of MS dependent on each designation; the PoC communicates the results to the EC	
Informing the owner/operator of the designated ECI (Art. 4.5)	The competent ministry (DE: BMWi / BNetzA)	

OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	No later than four weeks after the Federal Network Agency has identified an ECI, the operator of a shall submit to the Federal Network Agency a safety plan to protect the transmission network.	§ 4 and 5 ÜNetzSchV
Verification that the OSP or equivalent is in place	The security plan shall be reviewed by the Federal Network Agency within four weeks of its submission. If the safety plan complies with the requirements, the Federal Network Agency issues a corresponding confirmation to the operator of the system. Otherwise, it will immediately inform the operator as to which gaps exist and shall set an appropriate deadline for remedying.	
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	Federal Network Agency	§ 3 ÜNetzSchV
Function of the SLO (Art. 6.1)	The SLO is the contact person and ensures that the relevant authorities receive security related information. Furthermore the SLO shall provide information concerning the TSO report (TSOs have to provide the Federal Network Agency with a report in preparation for the regulatory determination of ECI biennially) and security plans (no later than four months after the regulatory determination of ECI, the operators of ECI have to provide the Federal Network Agency with a detailed security plan).	§ 3 section 2 ÜNSchutzV (12g EnWG; § 4 ÜNSchutzV)
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	No later than four months after the regulatory determination of ECI, the operators of plants/installations which are classified as ECI have to prove to the Federal Network Agency the designation of a SLO.	§ 3 section 1 ÜNSchutzV
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	No later than two weeks after the determination of the Federal Network Agency the operator of a European critical facility of the Federal Network Agency for the protection of the transmission network has to prove the selection of a SLO.	§ 3 ÜNetzSchV
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	n.a.	
Performance of threat assessments within ECI subsector within one year following the designation of ECI	An ongoing threat assessment is carried out to identify the most critical elements of energy infrastructure.	

OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	BMI as PoC on the basis of information by BMWi (BNetzA). Main content is the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds and the number of designated ECI.	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	By organisational decree	
MS body(-ies) serving as ECIP contact point	BMI	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<ul style="list-style-type: none"> National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009 2016 Cybersecurity Strategy (Cyber-Sicherheitsstrategie für Deutschland); 2016), replacing Cyber-Security Strategy of 2011 IT Security Act (IT-SiG) in context with the Ordinance on addressing to critical infrastructures (BSI-Kritisverordnung) Several recommendations for operators e.g. on physical protection or risk and management (Baseline Protection Concept, Risk and crisis management (see above "risk analysis"). Methodology for the identification of critical infrastructures: This methodology is the background for the proceeding in the addressing of the IT-SiG by the BSI-Kritisverordnung in combination with sectoral and sub-sectoral analyses and is basis for the self-assessment of potential (national) critical infrastructures in every respect. The brochure "Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten" is linked via https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_20_Praxis_BS_Schutz_Kritis_Identifizierung.pdf?__blob=publicationFile 	
Scope of national CIP policy		
Sectors of critical importance	<ul style="list-style-type: none"> Energy Information technology and telecommunications 	<i>National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> • Transport and traffic • Health • Water • Food • Finance and insurance industry • Government and public administration • Media and culture <p>(Agreement on federal level as of 2011, replacing the agreement of 2003)</p>	<i>in context with the list of sectors and subsectors of 2011)</i>
Number of national CI	<p>In Germany, there is no list of Critical Infrastructures.</p> <p>With respect to the cyber dimension of CIP during the implementation process of NIS-Directive critical services were identified as well as assets necessary for identified critical services (see BSI-Kritisverordnung). Until now there are ca. 1.700 critical infrastructures of ca. 800 operators according to this announcement duty</p>	
Number of national CI operators	<p>In Germany, there is no list of CI operators.</p> <p>With respect to the cyber dimension implementing the NIS Directive operators have to identify themselves as CI operators using the criteria of the BSI-Kritisverordnung</p>	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	<p>In Germany, critical infrastructure protection is a task to be performed jointly by government, companies and/or operators and also by civil society. The focus of CIP is on security of supply. The guiding principles regarding critical infrastructure protection are, in particular</p> <ul style="list-style-type: none"> • trusting co-operation between the state and business and industry at all levels; and • the requirement for, and suitability and proportionality of, the measures taken and the use of resources made for increasing the level of protection 	<i>National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	As is stated in the CIP-Strategy, "critical infrastructure protection calls for joint action by the various federal government departments within their respective areas of responsibility, and by the various tiers of government (i.e. Federation, federal states [Länder], etc.) in accordance with the distribution of competence as provided under the Basic Law. The protection of CI in Germany has to be organised and performed above different administrative levels"	<i>Braubach, et.al., CIP in Germany. Co-operation and recommendations as main driving forces, Global Security 2014</i> <i>National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009</i>
Coordination of ministries, bodies and offices concerned	The BMI provides inter-departmental co-ordination of the central national-level CIP measures.	<i>National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009</i>
Communication owners/operators with	<p>Since 2007 there is a strong public-private partnership between public authorities and CI operators (operators of the 8 "private-driven" sectors, called UP KRITIS (UP: implementation plan/ Umsetzungsplan of a former National Plan for the protection of CII, replaced by the first Cyber-Security Strategy 2011) The UP KRITIS follows the all-hazard approach, even IT-Security is the main focus.</p> <p>The UP KRITIS consists of (sub-)sectoral working groups (<i>Branchenarbeitskreise</i>) as well as cross-sectoral thematic WG (<i>Themenarbeitskreise</i>) For more information see "UP KRITIS - Public-Private Partnership for Critical Infrastructure Protection. Basis and Goals"</p>	<p>www.kritis.bund.de</p> <p>www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf?__blob=publicationFile</p>
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	<p>Infrastructure companies are regularly invited to take part in the LÜKEX series of national table-top exercises (Länderübergreifende Krisenmanagement Exercise - a cross-State crisis management exercise) launched in 2004 so that they can familiarise themselves with, exercise and further develop, the structures and measures developed for crisis management by governmental and private partners as a 'module' of the national-level security preparedness system.</p> <p>Moreover, the federal authorities take part in many activities under the national programme "Research for Civil Security" (<i>Forschung für die zivile Sicherheit</i>) which was launched in 2007 by the Federal Government as part of the HighTech Strategy for Germany and is in steady prolongation by diverse research programmes and funds. In association with the academic community, industry and infrastructure operators, innovative solutions for civil security are being investigated and developed.</p>	<i>National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Other relevant aspects of national authorities involved in CIP protection	<p>The Federation, the Länder and local governments are required jointly to enhance and implement critical infrastructure protection in their respective areas of responsibility. This purpose is served by a structured implementation procedure at these three tiers of government; this procedure comprises the following work packages, which in part are implemented in parallel, and is based on the co-operative approach adopted by the Federal Administration with the involvement of the other major players, i.e. operators and the relevant associations:</p> <ol style="list-style-type: none"> 1. definition of general protection targets; 2. analysis of threats, vulnerabilities, and management capabilities; 3. assessment of the threats involved; 4. specification of protection targets, taking account of existing protective measures; analysis of existing regulations and, where applicable, identification of additional measures contributing to goal attainment; if and where required, legislation. <p>Similar to the federal level, most of the states ("Länder") have established a coordinating unit for CIP and are working together with the Federal Ministry of Interior in a structured way (so called AG KOST KRITIS).</p>	<i>National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009</i>
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Companies designated as a European or a national CI have to appoint a security officer	
- Preparation of a security plan	Companies designated as a European or a national CI have to appoint a security officer	
- Review of the plan (timing)	Security plans of companies designated as a European or a national CI are reviewed on a regular basis (by an auditor or the competent authority)	
- Reporting incidents	Companies designated as a national CI (and partially also European CI) have to report (cyber-driven) incidents	IT-SiG
- Exchange of information	<p>Germany's CIP strategy is based on a cooperative approach. Such co-operation includes exchanges of information among all parties involved and the development of action concepts co-ordinated with the relevant infrastructure providers and operators. One of the most important platforms for the exchange of information between state and ECI operators is the UP KRITIS.</p> <p>The Federal Administration is committed to a co-operative approach and expects that important jointly developed analytical findings, framework recommendations</p>	<i>National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>and protection concepts will be implemented, in accordance with the security requirements, by infrastructure providers and operators and other important players, such as (trade) associations or standardisation committees. If identified substantial security deficiencies in critical infrastructure sectors are not remedied on the basis of voluntary commitments by the providers and operators or if, due to the emergence of new threats and risks, existing legal provisions do not offer adequate protection, the Federation reserves the right, within its jurisdiction, to optimise the protection of the respective infrastructures by amending existing legislation or enacting new legal regulations.</p> <p>This was done by the IT-Security Act (=BSI Act (BSI-Gesetz) § 2 Abs. 10, §§ 8a-8e, § 10).</p>	IT-SiG
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Approach: all hazards approach - Critical infrastructure may be exposed to various threats which must be included both in risk and threat analyses and in the selection of options for action. The overall spectrum of threats may be described as follows:</p> <ul style="list-style-type: none"> • Natural events: • Technical failure/ human error • Terrorism, crime, war <p>Business security: enforcement of standards, norms and regulations (e.g. the BSI Information Security Standards as a basic recommendation for action addressed to critical infrastructure operators; or the regulations of the German Gas and Water Supply Association (DVGW) on risk management in the field of drinking water supply).</p> <p>Cybersecurity: Germany launched cyber-security strategy in 2016, calling for specific measures to protect critical infrastructures from IT-related threats.</p> <p>In preparation and implementation of the NIS policy of EU, Germany has launched the IT-SiG.</p>	<p><i>National Strategy for Critical Infrastructure Protection (CIP Strategy), Berlin, 17 June 2009</i></p> <p><i>For Cybersecurity</i> <i>2016 Cybersecurity Strategy (Cyber-Sicherheitsstrategie für Deutschland 2016)</i></p>

Greece¹

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Article 1</i>	<i>Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Article 1</i>
Definitions (Art 2)		
'critical infrastructure'	"Critical infrastructures" are the assets, systems or parts thereof which are essential to preserve vital functions of society, health, safety, the economic and social well-being of its members, whose disruption or destruction would have a significant impact on the country, and would result of the inability to maintain these functions;	<i>Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Article 2</i>
'European critical infrastructure'	"European Critical Infrastructure" is a critical infrastructure in the Greek territory or in another MS whose disruption or destruction would have a significant impact on Country and at the same time in one or more MS. The significance of the impacts is assessed on the basis of cross-cutting criteria.	
'risk analysis'	"Risk analysis" is the analysis of threats in order to assess the vulnerabilities and its potential impact of the disruption or destruction of CI.	
'sensitive critical infrastructure protection related information'	"Sensitive critical infrastructure protection related information" is data on critical infrastructure, which in the event of disclosure could be used to	

¹ **Comment by POC:** The Center for Security Studies (KE.ME.A.) implements a funded action under the title "Targeted actions for enhancing the protection of national characterised European critical infrastructure". The action includes a series of supplementary activities and deliverables, aiming to provide a commonly accepted level of security and safety in critical infrastructures (CI). Deliverables of the action are:

1. Coordination/information Center. A center is under construction that will belong to KE.ME.A. and it will serve as the contact point between the C.I. and the Authorities/Organisations. It is in the process of purchasing software.

2. Templates of Operator Security Plan. This will be ready (end of 2018) and it will consist of five (5) different plans: Risk Assessment Plan, Vulnerability assessment plan, Security Operational Plan, Emergency Security Plan and Business Continuity Plan.

3. Exercises. Four (4) table top exercises/1 per year (2017-2020) are planned. The first and the last exercises are cross sector (energy and transport). The second (2018) will take place in December and will only engage players of the energy sector, whereas in 2019 the exercise will focus on transport sector.

The infrastructures, although they are not yet characterised and designated, they will be determined through the constant co-operation of the Entities/Organisations responsible for the security and safety matters. In this framework KE.ME.A. cooperates with the respective Ministries (Ministry of Environment and Energy, Ministry of Infrastructure, Transport and Networks) in order to determine the national C.I. per sector. In transport sector progress has been made about a list of the characterised National Critical Infrastructures. In Energy sector, we are in the process of identifying the N.C.Is and then we will characterise them. The above actions, on a national level helped us to set up a co-operation framework between all the involved actors, thus leading to the enhancement of the resilience of the infrastructures, against multiple risks (all hazards approach). KE.ME.A. developed a list that consist all the nominated Liaison Officers of possible National Critical Infrastructures, that is constantly updated.

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	design and execute actions aimed at shutting down or damaging/destroying critical infrastructure facilities.	
‘protection’	“ protection ” means all activities aimed at ensuring the operational-integrity, continuity and integrity of CI to prevent, mitigate and neutralise threats, risks or vulnerabilities	
‘owners/operators of ECI’	“ Owners/operators of ECI ” are entities that responsible for investments and / or for the daily operation in a particular asset element, system or part thereof, which is defined as ECI.	
Other relevant national definitions		
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	List of sectors in scope Transportations Aviation Road transport Train transport Maritime transport (Ocean and short-sea shipping and ports) Maritime transport (Inland waterways) Energy Gas Electricity Oil	<i>Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Articles 3 & 11</i>
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The Centre for Security Studies (KE.ME.A.)/Ministry of Citizen Protection, identifies possible ECI which meet the horizontal and sectoral criteria	<i>Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Article 3</i>
Application of the procedure for the identification of ECI (as per Annex III)	The key steps of the procedure are defined below	
Step1 – Application of sectoral criteria	Sectoral criteria apply to the first choice of critical infrastructure within a sector.	<i>Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N.</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Step 2 – Application of the definition of critical infrastructure	Apply the definition of critical infrastructure. Significant impact is evaluated is assessed either by the use of national methods and with sectoral criteria.	39 entered into force on January 12, 2011, Article 3
Step 3 – Application of the transboundary element of the definition of ECI	For the infrastructure that passed the first two stages cross border element is applied.	
Step 4 – Application of the cross-cutting criteria	For the European critical infrastructure that passed the first three steps the cross cutting criteria are applied. The infrastructures that do not meet the cross cutting criteria are not considered ECI.	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	The cross cutting criteria shall include the following loss criterion; <ul style="list-style-type: none">Economic impact criterion (evaluation as the importance of financial loss and / or degradation of products or services, potential environmental impacts);Public impact assessment (evaluation as regards the impact on public confidence, physical distress and disruption of the socio- The Exact minimum thresholds applicable to cross-cutting are determined on a case-by-case basis by KE.ME.A.	
Identification of potential ECI on an ongoing basis (Art 3.1)		
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	KE.ME.A. characterises critical infrastructure located in Greece as an ECI after an agreement with the competent authorities of the Member States likely to be significantly affected	Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Article 4
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	KE.ME.A communicates with the Member States that could be potential affected by European Critical infrastructure in Greece.	
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	KE.ME.A engages bilateral and multilateral consultations with the competent authorities of the other Member States that may be affected significantly from an ECI.	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	When KE.ME.A recognises that in territory of another State there is an infrastructure that may have an impact on Greece but that has been not designated has an ECI it notifies to the Commission of its intention to start a bilateral or multilateral consultation with the Member State where is located the ECI.	
Agreement for the designation of the ECI (Art. 4.3)		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	KE.ME.A is responsible for communicating each year to the European Commission the sector and the number of the Member States where are located ECI.	
Informing the owner/operator of the designated ECI (Art. 4.5)	KE.ME.A is responsible for communicating to the owner or manager of the critical infrastructure that it has been designated as ECI.	
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	KE.ME.A	Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Article 5
Verification that the OSP or equivalent is in place	KE.ME.A. checks whether ECI located on Greek territory have OSPs or equivalent measures to address the issues identified in Article 11 of Annex 2 (these are the same mentioned in the Directive). If it is established that there is an OSP or equivalent plan and that this is regularly updated, no further action is required. The OSP must cover at least: 1. identification of significant assets 2. conducting a risk analysis based on the main threat scenarios, the vulnerabilities of each asset, as well as potential risks; and 3. identification, selection and prioritisation of countermeasures and procedures, distinguished between permanent and graduated security measures	
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	KE.ME.A. checks whether ECI located on Greek territory have a SLO. If it finds that this link exists, no further action is required. In absence of a SLO for the designated ECI, KE.ME.A. shall, by any measures deemed necessary, ensure the definition of a SLO.	Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Article 6
Function of the SLO (Art. 6.1)	The SLO acts as a security link between KE.ME.A and the infrastructure operator / owner.	
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	KE.ME.A. checks whether ECI located on Greek territory have a SLO. If it finds that the SLO exists, no further action is required. In absence of a SLO for the designated ECI, KE.ME.A shall, by any measures deemed necessary, ensure the definition of a SLO.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	KE.ME.A shall develop and implement an appropriate communication procedure on a case by case basis with the security link, with the aim of exchanging appropriate information on identified risks and threats in relation to each ECI. The communication procedure shall be without prejudice to national requirements concerning access to critical and classified information.	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	KE.ME.A.	<i>Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Article 7</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	KE.ME.A. performs a threat assessment in relation to the sub-sectors of the ECI located on Greek territory within one year of the designation.	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	KE.ME.A. produces a summary report every two years to the Commission concerning categories of risks, threats and vulnerabilities. Per each ECI subsector. The reports are classified as confidential.	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	KE.ME.A. was appointed as the national contact point, after a decision that was made by a group of experts, consisted of representatives from all the involved Organisations/Entities.	<i>Adaptation of Greek legislation to the Directive 2008/114/EC through the Presidential Decree N. 39 entered into force on January 12, 2011, Article 10</i>
MS body(-ies) serving as ECIP contact point	KE.ME.A.	

NATIONAL CIP FRAMEWORK ²		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	The main document is the transposition directive mentioned above.	
Scope of national CIP policy		
Sectors of critical importance	N/A	

² **Comment by POC:** At the moment Greece does not have a national legislation dedicated to the Protection of Critical Infrastructures. The progress that is described above was made in co-operation between the involved Ministries. We are in the process of introducing a new law that will establish a National Internal Security Strategy. Part of this strategy will be the protection of the N.C.Is. (this will cover all the above described steps/identification, designation etc.). National Cyber Security Strategy will also be part of the Internal Security Strategy, covering the provisions of NIS Directive.

NATIONAL CIP FRAMEWORK ²		
Key dimension	Content	Source
Number of national CI	N/A	
Number of national CI operators	N/A	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	N/A	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	N/A	
Coordination of ministries, bodies and offices concerned	N/A	
Communication with owners/operators	N/A	
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	N/A	
Other relevant aspects of national authorities involved in CIP protection	N/A	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	N/A	
- Preparation of a security plan	N/A	
- Review of the plan (timing)	N/A	
- Reporting incidents	N/A	
- Exchange of information	N/A	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures 	Cybersecurity In Greece the National Cyber Security Authority (NCSA) was not established yet in Ministry of Digital Policy Telecommunications and Media. The Directorate that will be the NCSA has not been adequately staffed, to achieve its purpose, in order to succeed in coordinating all competent Ministries and independent authorities of Greece and to take all necessary	

NATIONAL CIP FRAMEWORK ²		
Key dimension	Content	Source
- Channels used for information exchange	steps towards a secure Greek Cyber space. The National CERT, handles all critical incidents.	

Hungary

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	1249/2010. (XI.19.) Government Decision on government tasks to be carried out in order to comply with Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection CLXVI. Act on the identification and designation of critical systems and facilities	
Definitions (Art 2)		
'critical infrastructure'	" critical infrastructure ": a vital component designated based up on the fact that its loss would have a significant impact in Hungary due to the lack of continuous supply of vital social functions	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 1)
'European critical infrastructure'	" European Critical infrastructure ": European Critical Infrastructure designated under this Act is the element whose loss would have a significant impact on at least two EEA States, also in view of cross-sectoral interdependence	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 1)
'risk analysis'	" Risk analysis ": Investigating of threats and risk factors to estimate the vulnerability of the system elements to rate the consequences of their disruption or destruction.	65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról (Section 1)
'sensitive critical infrastructure protection related information'	N/A	
'protection'	" Protection ": all activities aimed to ensure the function, continuity and integrity of the CI, as well as all activities aimed to mitigate threats, risks, vulnerability or neutralisation	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 1)
'owners/operators of ECI'	" Owners/operators of ECI " means any natural or legal person or entity without legal personality who is the owner or operates on (E)CI	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról,

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		<i>kijelöléséről és védelméről (Section 1)</i>
Other relevant national definitions	<p>"Sectoral criterion": criteria, thresholds, technical or functional characteristics that relate to the effect of a disruption or destruction of a constituent element of a CI within identified sectors (see below).</p> <p>"Horizontal criterion": criteria, thresholds, technical or functional characteristics which relate to the effect of loss/damage to a CI concerning loss of human life, health effects, and social impacts on the environment.</p> <p>"Network and information system": This refers to (a) the electronic communications network, (b) any device or group of connected or connected devices, one or more of which is automated to manage digital data on a program</p> <p>"Security events": all the events that produce a negative impact on the security of networks and information systems,</p> <p>"Security event management": Procedures for detecting, analysing and isolating security events and responding to them.</p>	<p>2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 1)</p>
Scope (Art 3.3)		
<p>Sectors and sub-sectors in scope:</p> <ul style="list-style-type: none"> - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports) 	<p>Energy (oil exploration, refining, storage and distribution, natural gas exploitation, storage delivery and distribution; electricity production, transmission and distribution)</p> <p>ICT (IT systems and networks, internet infrastructure, wire and wireless services, radio, satellite, broadcasting, postal services)</p> <p>Transport (road, rail, air, inland waterways, logistic centres)</p> <p>Water (drinking water, quality control of water, sewage collection and treatment, protection of water basin, flood protection)</p> <p>Agriculture (agriculture, food production, distribution networks)</p> <p>Healthcare (hospital care, rescue management, medical stocks, bio-labs, health insurance services)</p> <p>Social Insurance (social insurance services, networks, registers)</p> <p>Finance (payment, securities clearing and accounting infrastructures and systems bank and loan institution security)</p> <p>Law and order- Government (governmental facilities, devices public administration services, justice administration)</p> <p>Public Safety (national defence facilities, devices, networks, infrastructures of law enforcement agencies)</p>	<p>Government Resolution 2080/2008 (VI. 30.) on the National Programme for Critical Infrastructure Protection, Appendix 1</p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	Home Defence (national defence facilities and networks)	
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	<p>The potential CI/ECI can be identified through two channels:</p> <p>(a) following the submission of an identification report made on the basis of an identification procedure, which is determined by the Government and carried out by the operator,</p> <p>(b) on the basis of a proposal by a public law body (hereinafter referred to as the "proposing authority").</p> <p>The identification process is managed on a sector-by-sector basis. Each sector is overseen by a sectorally competent public authority, which is responsible for the CI identification process on the basis of points "a" and "b", above.</p>	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Article 3)
Application of the procedure for the identification of ECI (as per Annex III)	See below	
<i>Step1 – Application of sectoral criteria</i>	The sectorally competent public authority identifies potential national CI or ECI (or the withdrawal of such designation) on the basis of sectoral criteria, following submission of the identification report.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Article 3)
<i>Step 2 – Application of the definition of critical infrastructure</i>	Performed by the sectorally competent public authority. Further details not provided in the transposition legislation.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Article 3)
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	The conclusion of an international treaty to declare a European system of vital organisation is initiated by the Ministry responsible for disaster response, together with the sectorally competent ministry.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Article 3)
<i>Step 4 – Application of the cross-cutting criteria</i>	The sectorally competent public authority applies, to the national CI or potential ECI the cross-cutting criteria. The identification by the sectorally competent public authority shall be formalised within 70 days of the receipt of the identification report. This shall be performed on the basis of the applicable administrative procedure for each sector and on the basis of cross-cutting criteria. The sectorally competent public authority shall also	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Article 3)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	determine the time limit for the development of the OSP and any additional requirements for the operator.	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	<p>These are defined for each sector by specific government decrees. For example:</p> <ul style="list-style-type: none"> Government Decree 249/2017. (IX. 5.) On the Identification and Protection of Critical Assets and Infrastructure for the ICT sector: critical threshold identified if loss of service would affect more than fifty thousand persons, or if the asset is regarded as a universal communications service. In case of broadcasting services, the criteria is that it must be received over 95% of Hungarian territory and should be irreplaceable in case of loss of service. 	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Article 14)
Identification of potential ECI on an ongoing basis (Art 3.1)	Not specified in transposition documents.	
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	<p>Ministry of Interior (NDGDM) and sectorally competent public authorities:</p> <p>The Government empowers the Minister of the Interior to include ministries concerned by the sectors covered by Council Directive 2008/114 in bilateral or multilateral discussions on the identification and designation of critical infrastructures in Europe with the contact points designated by the MS of the European Union, the agreements with the EC and the implementation of the Directive.</p>	1249/2010. (XI.19.) Government Decision on government tasks to be carried out in order to comply with Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Article 3)
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	Ministry of Interior and sectorally competent public authorities	1249/2010. (XI.19.) Government Decision on government tasks to be carried out in order to comply with Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Article 3)
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	Ministry of Interior and sectorally competent ministries.	1249/2010. (XI.19.) Government Decision on government tasks to be carried out in order to comply with Council Directive 2008/114 /

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	The conclusion of international treaties to declare an ECI is initiated by the Minister of Interior, together with the sectorally competent public authority.	<i>EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Article 3)</i>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	Ministry of Interior and sectorally competent ministries.	<i>1249/2010. (XI.19.) Government Decision on government tasks to be carried out in order to comply with Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Article 3)</i>
Agreement for the designation of the ECI (Art. 4.3)	The sectorally competent public authority shall take a decision within thirty days of the entry into force of the international treaty on the designation of an ECI in accordance with the rules of the administrative procedure. In the Decision, the obligations of the operator of the ECI, their deadline for their implementation and control shall be determined in accordance with the international treaty.	<i>2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Article 2/A)</i>
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	Minister of the Interior Minister, of National Development, Minister of National Economy, Minister for Foreign Affairs	<i>1249/2010. (XI.19.) Government Decision on government tasks to be carried out in order to comply with Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Article 7)</i>
Informing the owner/operator of the designated ECI (Art. 4.5)	Sectorally competent public authorities.	<i>1249/2010. (XI.19.) Government Decision on government tasks to be carried out in order to comply with Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructures</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		<i>and the assessment of the need to improve their protection (article 4)</i>
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The ECI or CI operator shall elaborate, within the deadline set in the decision of the sectorally competent public authority, which shall not be shorter than sixty days after the notification of the designation decision, an OSP and send it to the sectorally competent public authority, via paper copies and on an electronic medium. The OSP shall be developed in accordance with the content and formal requirements specified in the designating decision issued by the sectorally competent public authority.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 4)
Verification that the OSP or equivalent is in place	The OSP is subject to formal and substantive scrutiny by the sectorally competent public authority. In case of a deficiency, the operator is called upon to fill the gap. The sectorally competent public authority shall send the revised OSP to the operator. The OSP shall identify the security measures that are designed and operated to ensure the protection of the CI/ECI, and the provisional measures to be taken in accordance with the various risk and threat levels. The ECI or the CI operator modifies the OSP if there is a change affecting the activity, operation or protection of the asset. On-site inspections shall check the ECI / CI at least every two years on-the-spot checks. On-the-spot checks shall be conducted taking into account national security considerations.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 4)
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The ECI/CI shall ensure the employment of the security liaison officer and shall continue to provide the necessary conditions for its activities. The authority responsible for ensuring that the SLO or equivalent is in place is the sectorally competent public authority.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 4)
Function of the SLO (Art. 6.1)	The task of the SLO is to maintain contacts between the operator and the authorities involved in the designation procedure. An SLO may be designated by a person with no criminal record who has a qualification as defined in a government decree.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 4)
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	On the spot checks.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 4)
Establishment of an appropriate communication mechanism between the	The sectorally competent public authority shall include CI/ECI operators in the national CI registry.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 4)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
relevant Member State authority and the SLO (Art. 6.4)	<ul style="list-style-type: none"> - The registry is a list of CI operators. - The registry administrator shall delete the operator from the list of operators providing basic services when the sectoral designating authority decides to withdraw the designation of the national critical system entity. - The registry shall review and, where appropriate, specify the list of core service providers every two years before reporting to the EC. 	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	<p>National Registry The body designated for this purpose by the government decree (referred to as the "registration authority") registers and manages</p> <ul style="list-style-type: none"> - the name, address or address of the operator, the mailing address, company registration number or personal entrepreneurial registration number, statistical number and tax identification number, representative's name, telephone and fax number, - the natural person identification data, telephone and telefax number, e-mail address, specialisation qualification of the security liaison person, the serial number of the certificate of qualification, - The designation of national CI and ECI, - the operator safety plan, - the decision of the sectorally competent public authority to designate a ECI/CI <p>The purpose of managing this data specified in paragraph concerns:</p> <ul style="list-style-type: none"> - the identification procedure, the designation procedure, the procedure for withdrawal of designation, - ensuring that official controls on the fulfilment of the obligations relating to the protection of critical constituents are ensured, - to ensure regular official control of the compliance with the conditions laid down during the designation procedure. - The registry shall review and, where appropriate, specify the list of core service providers every two years before reporting to the EC 	<p>2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 4)</p>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	The Government submits an annual report on sectoral number of ECI per Sector and the number of MS of the European Union that depend on ECI	
Reporting of generic data on summary basis on the types of risks, threats and	The Government submits a report to the European Commission on the types of vulnerabilities, threats and risks that threaten the sectors in which	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
vulnerabilities to the Commission per ECI subsector	European Critical Infrastructure has been identified, as provided for in the Directive	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The Home Secretary of the Ministry of Interior as an ECIP Contact Point coordinates issues related to the protection of critical infrastructure in Europe with the ECIP Contact Points of the European Union and the European Commission.	<i>1249/2010. (XI.19.) Government Decision on government tasks to be carried out in order to comply with Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (article 2)</i>
MS body(-ies) serving as ECIP contact point		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<i>2012. évi CLXVI. Törvény, "a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről"</i>	
Scope of national CIP policy		
Sectors of critical importance	<ol style="list-style-type: none"> 1. Energy <ol style="list-style-type: none"> a. Electricity b. Oil industry c. Gas industry 2. Transport <ol style="list-style-type: none"> a. Road transport b. Air transport c. Inland water ways d. Logistics centres 3. Agriculture <ol style="list-style-type: none"> a. Agriculture b. Food industry c. Distribution networks 4. Health <ol style="list-style-type: none"> a. Active impatient care b. Resource management 	<i>Annex 4 - CLXVI. Act</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> c. Health reserves and blood stocks d. High-security biological laboratories e. Pharmaceutical wholesale 5. Social Insurance <ul style="list-style-type: none"> a. Social insurance services, information systems related to the use of social security benefits, registers 6. Finance <ul style="list-style-type: none"> a. Commercial, payment and clearing and settlement infrastructures and systems for financial instruments b. Banking and credit institution security c. Cash supply 7. Information and Communication technology <ul style="list-style-type: none"> a. Internet infrastructure and internet access service b. Wired and wireless electronic communications services, wired and wireless communications networks c. Radio telecommunications d. Space communications e. Broadcasting f. Postal services g. IT government, electronic networks 8. Water <ul style="list-style-type: none"> a. Drinking water supply and distribution b. Surface and groundwater quality control c. Sewer drainage and cleaning d. Protection of water resources e. Flood protection dams 9. Law- government <ul style="list-style-type: none"> a. Government systems, facilities, tools b. Administrative services c. Justice 10. Public safety <ul style="list-style-type: none"> a. Infrastructure of law enforcement agencies 11. Home defence <ul style="list-style-type: none"> a. Defence systems and facilities 	
Number of national CI	270	
Number of national CI operators	166	
Responsibilities allocated to Ministries, bodies, and offices		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Definition of scope and objectives of the national CIP strategy	The Ministry of the Interior, National Directorate General for Disaster Management is responsible for the CIP in Hungary.	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	See table above	
Coordination of ministries, bodies and offices concerned	Coordination of ministries, bodies and offices involved: The National Directorate General for Disaster Management, Ministry of the Interior (NDGDM), is the main body involved in the protection of critical infrastructure. NDGDM is a law enforcement body with a national competence. Its main mission is preventing disasters as an authority; carrying out rescue operations in civil emergencies; organising and controlling protection activities; eliminating the negative consequences of emergencies and performing reconstruction and rehabilitation.	NDGDM official website - http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_intro&lang=eng
Communication with owners/operators		
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	The on-site inspection authority shall check the national critical infrastructure at least every five years onsite inspections. Onsite inspections shall be conducted taking into account national security considerations.	Section 8, Art. 3
Other relevant aspects of national authorities involved in CIP protection		
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	See table above	
- Preparation of a security plan	See table above	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
- Review of the plan (timing)	See table above	
- Reporting incidents	The operator shall immediately inform the on-call service of the territorial body of the professional disaster management body and the sectoral authority designated by law in the event of exceptional occurrences. If the risk associated with an exceptional occurrence has not been investigated in the OSP, the Operator will modify the OSP in order to address the emerging risk in accordance with paragraph.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Section 4)
- Exchange of information	See table above	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>According to the implementation of the ECI directive in Hungary the Identification, designation and protection of the critical infrastructure Act No 166/2012 (Act on CIP) has been established, which is regulating an all hazard cross sectoral approach. Furthermore the Information security Act No 50/2013 (InfoSec Act) is responsible to raise the awareness and resilience level for the IT security standards of the designated critical infrastructure operators.</p> <p>In the Hungarian legal framework the definition of a critical infrastructure element has a close legal connection with the definition used by NIS Directive for 'operator of essential services'.</p>	

Italy

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Decreto Legislativo 11 April 2011, n. 61: Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione. (11G0101)</i>	<i>Decreto Legislativo 11 April 2011, n. 61: Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione. (11G0101)</i>
Definitions (Art 2)		
'critical infrastructure'	Critical infrastructure (IC): infrastructure, located in one Member State of the European Union that is essential for the society's vital functions, health, security and economic and social well-being of the population. Furthermore an infrastructure is considered critical when its damage or destruction would have a significant impact in that State, due to the impossibility of maintaining such functions.	<i>Decreto Legislativo 11 April 2011, n. 61: Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione. (11G0101)(Article 2)</i>
'European critical infrastructure'	European Critical Infrastructure (ECI): infrastructure located in EU Member States whose damage or destruction would have a significant impact on at least two Member States. The relevance of the impact is evaluated in inter-sectorial terms including the inter-sectorial effects related to other kinds of infrastructures.	
'risk analysis'	Risk analysis: assessment of the vulnerability of an ICE with respect to the various possible threats and foreseeable consequences of its damage or destruction.	
'sensitive critical infrastructure protection related information'	Sensitive information about ICs: data and news, related to ICs, which, if disclosed, could be used to plan and execute actions aimed at damaging or destroying such infrastructures	
'protection'	Protection: activities aimed at ensuring the functionality, continuity and integrity of an ECI, or to reduce the possibility of its damage or destruction	
'owners/operators of ECI'	Owner: public or private actor which owns the infrastructure; Operator: public or private actor responsible for the functioning of the infrastructure	
Other relevant national definitions	Negative external effects: negative effects due to the loss of functionality of an infrastructure and to the loss of its capability in supplying goods or services. Intrinsic negative effects: negative effects which, in case of damage or destruction of an infrastructure, affect the infrastructure itself and the environment	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Scope (Art 3.3)		
<p>Sectors and sub-sectors in scope:</p> <ul style="list-style-type: none"> - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports) 	<p>Sectors: Energy; Transport.</p> <p>Sub-sector Energy:</p> <ul style="list-style-type: none"> - Electricity, including: infrastructure and plants for the production and transmission of electricity and supply of electricity; - Oil, including: production, refining, treatment, storage and transportation of oil through oil pipelines; - Gas, including: production, refining, treatment, storage and transport of gas through oil pipelines and LNG terminals; <p>Sub-sector transport:</p> <ul style="list-style-type: none"> - Road transport; - Rail transport; - Airplane transport; - Inland Water Ways; - Ocean shipping, short sea shipping and ports 	<p><i>Decreto Legislativo 11 April 2011, n. 61: Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione. (11G0101) (Annex A)</i></p>
Identification of the ECI (Art. 3)		
<p>MS body(-ies) responsible for the identification of potential ECI</p>	<p>ECI are identified by the <i>Nucleo interministeriale di situazione e pianificazione</i> (NISP). NISP is established at the Presidency of the Council of Ministers and composed of representatives from various ministries.</p> <p>NISP is supported by the "responsible structure" which has been identified in the Critical Infrastructures Secretariat (SIC), which is embedded within the office of the Military Councillor of the Presidency of the Council of Ministers. The responsible office was identified through a Decree of the President of the Council of Ministers, issued on 17/05/2011.</p>	<p><i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (article 4)</i></p> <p><i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 212; Data di pubblicazione: 12/09/2011; Decreto del Presidente del Consiglio dei Ministri del 17 maggio 2011, Individuazione della "struttura responsabile" di cui all'articolo 4, comma 3, del decreto legislativo 11 April 2011, n. 61. (11A11813)</i></p>
<p>Application of the procedure for the identification of ECI (as per Annex III)</p>	<p>Workflow: The identification is performed in several stages.</p>	<p><i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU:</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<ol style="list-style-type: none"> 1) The CI must satisfy the first criterion, that is to say, fall within the targeted sectors (energy and transportation). 2) Procedure for identifying the critical infrastructure on the basis of the definitions adopted in the Legislative Decree 61/2011, Article 2 (see section above on definitions). 3) Verification of the cross-border impact, i.e. if potential damage to an infrastructure could negatively affect another MS. The assessment of any negative impact follows cross-sector criteria due to the close relationship that exists between different sectors. This impact can be assessed in terms of victims, economic/financial losses and "possible consequences on the population in terms of trust in institutions, physical suffering and disruption of daily life, considering the loss of essential services" [art. Legislative Decree 61/2011]. 4) Identification as ECI only for those infrastructures that have a level of cross-cutting criticality. 	<p>102; <i>Data di pubblicazione:</i> 04/05/2011, <i>Decreto Legislativo 11 April 2011, n. 61 (article 6, 7)</i></p> <p><i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 212; Data di pubblicazione:</i> 12/09/2011; <i>Decreto del Presidente del Consiglio dei Ministri del 17 maggio 2011, Individuazione della "struttura responsabile" di cui all'articolo 4, comma 3, del decreto legislativo 11 April 2011, n. 61. (11A11813)</i></p>
<i>Step1 – Application of sectoral criteria</i>	<p>Sectoral identification</p> <p>The responsible structure (NISP) in collaboration with the Ministry of Economic Development - for the energy sector -and with the Ministry of Infrastructure and Transport and supervised entities - for the transport sector - also taking account of the guidelines developed by the European Commission, determines the limit of the sector evaluation criterion beyond which the infrastructure can be potentially critical.</p> <p>The Ministry of Economic Development and the Ministry of Infrastructure and Transport, identify and communicate to NISP:</p> <ul style="list-style-type: none"> • The infrastructures located in the national territory to be assessed according to the limit of the sectoral criteria evaluation • Infrastructure located in other EU Member States which, within the same sector that may be of significant interest. 	<p><i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 212; Data di pubblicazione:</i> 12/09/2011; <i>Decreto del Presidente del Consiglio dei Ministri del 17 maggio 2011, Individuazione della "struttura responsabile" di cui all'articolo 4, comma 3, del decreto legislativo 11 April 2011, n. 61. (11A11813) (Article 5)</i></p>
<i>Step 2 – Application of the definition of critical infrastructure</i>	<p>Any infrastructure located in the national territory and identified in accordance, for the purposes of its designation as an ECI, must be essential for the maintenance of the vital functions of society, health and safety and the economic and social well-being of the population.</p> <p>In this matter, for the identification of ECI, is applied the definition of CI.</p>	<p><i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 212; Data di pubblicazione:</i> 12/09/2011; <i>Decreto del Presidente del Consiglio dei Ministri del 17 maggio 2011, Individuazione della "struttura responsabile" di cui all'articolo 4, comma 3, del decreto legislativo 11 April 2011, n. 61. (11A11813) (Article 6)</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	NISP applies the transboundary element. The methodology is specified in Art 7 of Decreto Legislativo 11 April 2011, n. 61. (11A11813). On a regular basis there is a formal exchange with neighbouring countries aimed at identifying infrastructures that may be considered as critical from both countries.	<i>Gazzetta Ufficiale della Repubblica Italiana; articolo 7, del decreto legislativo 11 April 2011, n. 61, Article 7 (11A11813)</i>
<i>Step 4 – Application of the cross-cutting criteria</i>	In order to define a European Critical Infrastructure, a cross-cutting evaluation has to be applied: <ul style="list-style-type: none"> • The possible victims, in terms of number of deaths and wounded; • The possible economic consequences, in terms of financial losses, deterioration of goods or services and environmental effects; • The possible consequences for the population, in terms of trust in the institutions, physical suffering and disruption of everyday life, also considering the loss of essential services 	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 212; Data di pubblicazione: 12/09/2011; Decreto del Presidente del Consiglio dei Ministri del 17 maggio 2011, Individuazione della "struttura responsabile" di cui all'articolo 4, comma 3, del decreto legislativo 11 April 2011, n. 61. (11A11813) (Article 6)</i>
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	Procedures for defining thresholds criteria: The NISP, on the basis of the ECI definition, also on proposal of the responsible structure, and taking into account the guidelines established by the European Commission, settles the cross-cutting criteria beyond which the infrastructure is defined as potentially critical.	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 212; Data di pubblicazione: 12/09/2011; Decreto del Presidente del Consiglio dei Ministri del 17 maggio 2011, Individuazione della "struttura responsabile" di cui all'articolo 4, comma 3, del decreto legislativo 11 April 2011, n. 61. (11A11813) (Article 6)</i>
Identification of potential ECI on an ongoing basis (Art 3.1)	The ICE identification and designation mapping process is reviewed periodically, at least every 5 years.	<i>Decreto Legislativo 11 April 2011, n. 61: Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione. (11G0101) (Article 9)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	<p>NISP is composed of representatives from:</p> <ul style="list-style-type: none"> • Ministry of Interior • Ministry of Foreign Affairs • Ministry of Defence • Ministry of Economy • Ministry of Health • Security Intelligence Department (DIS) • Civil Protection • Ministry of Economic Development • Ministry of Infrastructure and Transport 	<i>Gazzetta Ufficiale della Repubblica Italiana; Data di pubblicazione: Decreto del Presidente del Consiglio dei Ministri 5 maggio 2010, (Article 4) e successiva modifica.</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	<ul style="list-style-type: none"> • Critical Infrastructures Secretariat (SIC) informs NISP. • The process is updated in an interagency fashion within NISP. 	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 4, 7, 8)</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	<p>Critical Infrastructures Secretariat (SIC).</p> <p>Institutional communication channels are used.</p>	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 7)</i>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	<p>Critical Infrastructures Secretariat (SIC).</p> <p>Institutional communication channels are used.</p>	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 10)</i>
Agreement for the designation of the ECI (Art. 4.3)	<p>Whenever there is an agreement from the MS in whose territory the designated ECI is located, SIC, in co-operation with the Ministries for Foreign Affairs, Interior and Defence, as well as with the Department of Civil Protection of the Presidency of the Council of Ministers, having heard the Ministry of Economic Development, for the energy sector, and the Ministry of Infrastructure and Transport, for the transport sector, prepares, for the purposes of agreement with the representatives from the other concerned MS, an agreement to designate as ECI the identified infrastructure. The agreement is achieved with the signing by the representatives from the member states involved.</p>	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 8)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The responsible for the communication is Critical Infrastructures Secretariat (SIC). Institutional communication channels are used.	Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 7)
Informing the owner/operator of the designated ECI (Art. 4.5)	Critical Infrastructures Secretariat (SIC). Institutional communication channels are used.	Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 10)
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	Critical Infrastructures Secretariat (SIC)	Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 12 and annex b)
Verification that the OSP or equivalent is in place	Operator's security plan: drawn up by the SLO, together with <ul style="list-style-type: none">the Ministry of Economic Development, for the energy sector;the Ministry of Infrastructure and Transport, for the sector transport;the Ministry of Interior and Defence;the Department of Civil Protection of the Council Presidency of Ministersthe owner/operatorthe NISP/SIC within 12 months after the ECI is designated. This plan must include: <ul style="list-style-type: none">An identification of the key elements of the designated ECI;A risk assessment;Identification of permanent measures (for continuous use, such as physical defences, crisis management plans, communication systems, etc.) and of measures that can be activated ad hoc on the basis of observed risks; The plan must also give due consideration to measures included in other legislation on safety and security including D.Lgs 17/08/1999, n. 334, as updated by D.Lgs 21/09/2005, n. 238. This involves an internal emergency plan, identification of domino effects and setup of an external emergency plan (so as to limit risks of incidence to the general populace) The OSP must be completed within one year from designation of the infrastructure as ICE, and revised at least every five years.	
Verification that the OSP or equivalent is appropriately and regularly reviewed		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	Where there is an OSP in place, SLOs for the Ministry of Infrastructure (transport) and Economic Development (Energy), in co-operation with SIC and the Civil Protection Agency ensure that the OSP is in line with the minimum requirements set out in annex b. The ways the public entities verify that the OSP is in place are not specified.	
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The infrastructure operator communicates the name of the official of SLO to the responsible Prefect and to the owner and responsible of the structure, which also informs the contact point designed by The Ministry of Economic Development, for the energy sector, the Ministry of Infrastructure and Transport, for the sector transport, the Ministry of Interior and Defence, as well as the Department of Civil Protection of the Council Presidency of Ministers.	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 12)</i>
Function of the SLO (Art. 6.1)	The contact point designed for each ECI by the ministries and the Department of Civil Protection of the Council Presidency, and the structure responsible cooperate with the operator and the owner of the ICE, also through the SLO in matters of safety, in carrying out risk analysis and in drafting or updating the subsequent Operator Security Plan, which must respect the minimum parameters agreed at EU level and listed in Annex B.	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 12)</i>
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	A mechanism to verify the existence of SLO is not specified	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	The Ministry of Economic Development, for the energy sector, the Ministry of Infrastructure and Transport, for the sector transport, the Ministry of Interior and Defence, as well as the Department of Civil Protection of the Council Presidency of Ministers identify a contact point who communicate with SLO	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 12)</i>
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	Critical Infrastructures Secretariat (SIC)	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 14)</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	Threat assessment Once an ECI is designated, NISP will assess the possible threats to the sub-sector in which it operates. This analysis must be carried out within a year and SIC is tasked with informing the EC. In every sector where there is a designated ECI, NISP performs a risk analysis every two years.	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 14)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	NISP, based on information reported by Competent administrations will: a) within one year of designation of an ECI, draw up an assessment of possible threats to the subsector in which the designated ECI operates and inform the EC. b) every two years it processes the general data on different types of risks, threats and vulnerabilities of the sectors in which there is an ECI and communicates such data to the EC	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 14)</i>
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	Art. 13 of Decreto Legislativo 11 April 2011, n. 61, establishes a national contact point in NISP for other MS and the EC, also acting as an intermediary for information exchange to other national bodies such as Prefects and ECI operators, concerning the sharing of best practices, training opportunities and any technical developments. The Interministerial Unit Situation and Planning (NISP), was established with the Decree of the President of the Council of Ministers on 5 May 2010, published in the Official Gazette no. 139 of 17 June 2010. The NISP is responsible for the functions specified in this law.	<i>Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 (Article 13)</i>
MS body(-ies) serving as ECIP contact point	NISP as contact point is responsible for acquiring best practices and methodologies available in the field of protection, making them available to the public entities.	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	Italy does not have an overarching strategy for CIP, and has adopted a “case by base” approach, identifying ICs among the national operators of those services that are now universally recognised as critical. The institutions responsible for the protection of the CI have therefore worked in public-private collaboration with variable geometries depending on the needs and situations detected as critical or potentially such. This structure, has allowed the country to make important decisions to launch policies and postures of protection in step with the times and technologies	N/A
Scope of national CIP policy		
Sectors of critical importance	Sectors covered have not been formalised in a law.	
Number of national CI	It is not defined the specific number	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Number of national CI operators	Number of the operators is not defined	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	<p>External Protection Plans for CI</p> <p>Bodies responsible for implementing actions and measures to guarantee the protection of ECI Article. 11(1):</p> <ul style="list-style-type: none"> • Ministry of the Interior, • Ministry of Defence, • Department of Civil Protection of the Presidency of the Council of Ministers, • Ministry of Economic Development (Energy) • Ministry of Infrastructure and Transport (Transport). <p>Each ministry appoints one of its own officials, identified among the service personnel of their administrations, for each ECI.</p> <p>At the local level, responsibility falls under the territorially responsible prefect.</p>	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	Same as described in the table above	
Coordination of ministries, bodies and offices concerned	Same as described in the table above	
Communication with owners/operators	Same as described in the table above	
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	Same as described in the table above	
Other relevant aspects of national authorities involved in CIP protection		
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Same as described in the table above	
- Preparation of a security plan	Same as described in the table above	
- Review of the plan (timing)	Same as described in the table above	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
- Reporting incidents	In the law Gazzetta Ufficiale della Repubblica Italiana; Numero GU: 102; Data di pubblicazione: 04/05/2011, Decreto Legislativo 11 April 2011, n. 61 the procedure for incident reporting is not indicated	
- Exchange of information	Same as described in the Directive	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p><i>Cybersecurity</i></p> <p>After the Prime Minister Decree of January 2013, the Italian cyber security architecture was reshaped by two regulations: the Prime Minister Decree of February 2017, and the Legislative Decree 65/2018 transposing the EU Network and Information Systems (NIS) security Directive.</p> <p>Both these Acts assign to the Security Intelligence Department (DIS) the national cyber security governance, respectively establishing within it the Cyber Security Management Board (NSC) - competent for the prevention and management of national cyber incident and crises – and the Italian Single Point of Contact (SPoC), responsible for the national coordination of issues concerning the security of network and information systems, as well as for facilitating cross-border co-operation at EU level.</p> <p>As for the national strategic posture, this is outlined in the “National Strategic Framework for Cyberspace Security” of December 2013, and in the “National Plan for Cyberspace Protection and ICT Security” of March 2017, that aims at further developing the strategic guidelines envisaged by the National Strategic Framework.</p>	<p>-Prime Minister Decree of January 2013</p> <p>-Legislative Decree 65/2018</p> <p>-National Strategic Framework for Cyberspace Security (December 2013)</p> <p>-National Plan for Cyberspace Protection and ICT Security (March 2017).</p>

Latvia

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Ministru kabineta 2010.gada 01.jūnija noteikumi Nr.496 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība"</i> (This Regulation prescribes the procedures for the identification of critical infrastructure, including European critical infrastructure, and planning and implementation of security measures)	
Definitions (Art 2)		
'critical infrastructure'	"Critical infrastructure" : is objects, systems or parts thereof located in the Republic of Latvia, which are of significance for ensuring the implementation of important public functions, as well as human health protection, security, economic or social welfare and destruction of or interferences in the operation of which would significantly affect the implementation of State functions	<i>Nacionālās drošības likums; Section 22</i>
'European critical infrastructure'	A critical infrastructure may be recognised as a European critical infrastructure, if disruption to the activity of the relevant critical infrastructure or destruction thereof would significantly affect at least two Member States of the European Union and an agreement has been reached with the relevant Member States of the European Union	<i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība, Art. 19</i>
'risk analysis'		
'sensitive critical infrastructure protection related information'		
'protection'		
'owners/operators of ECI'		
Other relevant national definitions		
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Specific sectors not indicated, the sectors are likely connected to the ministries which compose the Commission of Intermediary Institutions for State Security	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	<p>The Commission of Intermediary Institutions for State Security is an advisory collegial institution, which evaluates and improves the critical infrastructure, including European critical infrastructure, the aggregate of systems and security measures. The proposal regarding determination of CI comes from the responsible sectoral ministries or members of the Commission of Intermediary Institutions for State Security. The Commission shall evaluate these proposals.</p> <p>The Commission is composed by:</p> <ul style="list-style-type: none"> - The Ministry of Defence - The Ministry of Foreign Affairs - The Ministry of Economics - The Ministry of Finance - The Ministry of Interior - The Ministry of Transport - The Ministry of Justice - The Ministry of Health - The Ministry of Environmental Protection and Regional Development - The Security Police - The Bank of Latvia - Defence Intelligence and Security Service - The National Armed Forces - Constitution Protection Bureau - State Fire-fighting and Rescue Service - The State Police - The Information Technologies Security Incidents Response Institution 	<p><i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība; Article 6 (emended by Grozījumi Ministru kabineta 2010.gada 1.jūnija noteikumos Nr.496 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība" Ministru kabineta 25.06.2013. noteikumi Nr. 333/LV, 122 (4928), 27.06.2013); Art. 4.1 and 4.2</i></p>
Application of the procedure for the identification of ECI (as per Annex III)	The Commission receives proposals from the responsible sectoral ministries, the Security Police, the Constitutional Protection Bureau the Military Intelligence and Security Service and prepares the submissions to the Cabinet of Ministers of draft legislative acts on the allocation of critical infrastructure.	<p><i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība; Section II, Art. 3</i></p>
<i>Step1 – Application of sectoral criteria</i>	Not indicated in national transposition	
<i>Step 2 – Application of the definition of critical infrastructure</i>	Not indicated in national transposition	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	See list of definitions	
<i>Step 4 – Application of the cross-cutting criteria</i>	The cross-cutting criteria are: 1. casualties criterion (assessed in terms of the potential number of fatalities or injuries); 2. economic effects criterion (assessed in terms of the significance of economic loss or degradation of products or services, including the loss of essential services, alternatives for the provision of services and disruption of services and length of restoration thereof); 3. public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services, alternatives for the provision of services and disruption of services and length of restoration thereof).	<i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība; Article 21</i>
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	The cross-cutting criteria thresholds are based on the severity of the impact of the disruption or destruction of a particular critical infrastructure.	<i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība; Article 21</i>
Identification of potential ECI on an ongoing basis (Art 3.1)	Not indicated in national transposition	
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	The Commission of Intermediary Institutions for State Security	<i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība ; 23</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	The Ministry of the Interior, on the basis of proposals from the Commission, informs the EC and the MS of the European Union that may have a significant impact on any potential ECI, and the reasons why it has been identified as a potential European Critical Infrastructure	<i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība ; 23</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	The Ministry of the Interior coordinates bilateral or multilateral negotiations with other Member States of the European Union that can have a significant impact on a potential European Critical Infrastructure.	<i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība ; 23</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	The Commission of Intermediary Institutions for State Security shall inform the European Commission regarding the necessity to ensure bilateral or multilateral negotiations with the other European Member States, which may be significantly affected by the potential European critical infrastructure	Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība ; Art. 4.5.3
Agreement for the designation of the ECI (Art. 4.3)	Not indicated in national transposition	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The Commission reports annually to the EC on the number of ECI identified in each sector and on how the other MS depend on each of the identified ECI	Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība ; Article 4.6
Informing the owner/operator of the designated ECI (Art. 4.5)	The Security Police, the Constitution Protection Bureau or the Defence Intelligence and Security Service, shall inform the owner or lawful possessor of a critical infrastructure / ECI.	Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība; Article 24
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The Security Police, the Constitutional Protection Bureau or the Military Intelligence and Security Service	Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība; Art. 27
Verification that the OSP or equivalent is in place	On the basis of the results of screening, the relevant State intelligence and security service shall provide recommendations regarding implementation of the security measures to the owner or lawful possessor of the critical infrastructure or European critical infrastructure.	
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The owner or lawful possessor of a critical infrastructure or a European critical infrastructure shall appoint a person responsible for the security of the infrastructure and determine the tasks thereof.	Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība ; Article 25; Article 29
	The Security Police, the Constitutional Protection Bureau or the Military Intelligence and Security Service shall examine and approve the nomination of the SLO	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Function of the SLO (Art. 6.1)	The SLO of the critical infrastructure shall: 1. plan security measures of the critical infrastructure; 2. in co-operation with the Security Incidents Response Institution (Constitution Protection Bureau and the Information Technologies Security Incidents Response Institution) ensures assessment and management of the current risks of the critical infrastructure.	<i>Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība; Art. 7</i>
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	The Constitution Protection Bureau shall examine and approve the conformity of the person responsible for the security of the critical infrastructure	<i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība ;</i>
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	Not indicated in national transposition	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	The Commission of Intermediary Institutions for State Security	
Performance of threat assessments within ECI subsector within one year following the designation of ECI	Not indicated in national transposition	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The Commission shall, on the basis of the report by the Security Police, the Constitution Protection Bureau and the Defence Intelligence and Security Service, prepare once every two years information for the EC regarding the types of risks, threats and vulnerabilities in each European critical infrastructure sector and submit it to the Cabinet for approval;	Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība; Section II, Art. 4.7
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The Commission of Intermediary Institutions for State Security is the body responsible for the relevant communication with the European Commission	
MS body(-ies) serving as ECIP contact point		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<i>Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība</i> <i>Nacionālās drošības likums</i>	<i>Publicēts: "Latvijas Vēstnesis", 25 (4423), 15.02.2011.</i> <i>Publicēts: "Latvijas Vēstnesis", 473/476 (2384/2387), 29.12.2000, "Ziņotājs", 3, 08.02.2001.</i>
Scope of national CIP policy		
Sectors of critical importance		
Number of national CI	n.a.	
Number of national CI operators	n.a.	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	Critical infrastructure shall be classified as follows: 1) especially important critical infrastructure of State level (Category A critical infrastructure), destruction of or reduction of operational capabilities of which significantly endangers State administration and national security; 2) important critical infrastructure of State level (Category B critical infrastructure), destruction of or reduction of operational capabilities of which hinders State administration and endangers public and national security; 3) critical infrastructure of local governments and sectors (Category C critical infrastructure), destruction of or reduction of operational capabilities of which hinders administration of local government activities or sectors, as well as endangers public security. 4) A separate critical infrastructure, destruction of or reduction of operational capabilities of which would significantly affect at least two European Union Member States, may also be determined as a European critical infrastructure.	<i>Nacionālās drošības likums; Section 22; Art. 4</i>
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	The Commission shall, not less than once a year, prepare an informative report for submission to the Cabinet regarding the security situation of the critical infrastructure;	<i>Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība; Art. 4.3</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Coordination of ministries, bodies and offices concerned	The responsible sectoral ministries, the Security Police, the Constitution Protection Bureau and the Defence Intelligence and Security Service shall identify the possible critical infrastructure and submit proposals to the Commission of Intermediary Institutions for State Security regarding inclusion thereof in the aggregate of critical infrastructure;	Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība; Art. 18
Communication with owners/operators	In order to ensure more expedient exchange of information regarding security incidents of information technologies, the Security Incidents Response Institution and the owner or legal possessor of the critical infrastructure may agree upon a technological solution that automatically compiles and forwards the relevant information.	<i>Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība; Art. 13</i>
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	The Cabinet shall determine the procedures for surveying critical infrastructure, including European critical infrastructure, and for planning and implementation of security measures. The Security Incidents Response Institution may perform inspections upon request of the Constitution Protection Bureau. A reason for the inspection requested must be indicated in the request.	<i>Nacionālās drošības likums; Section 22; Art. 6</i> <i>Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība; Section III; Art. 17</i>
Other relevant aspects of national authorities involved in CIP protection		
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	See table above	
- Preparation of a security plan	The owner or legal possessor of critical infrastructure, shall ensure planning and implementation of security measures.	<i>Nacionālās drošības likums; Section 22; Art. 4</i>
- Review of the plan (timing)		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
- Reporting incidents		
- Exchange of information	The owner or legal possessor of critical infrastructure, including European critical infrastructure, shall determine the status of restricted access information for documents governing internal security measures	<i>Nacionālās drošības likums; Section 22; Art. 5</i>
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 		

Luxembourg

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.</i>	<i>Journal Officiel du Grand-Duché de Luxembourg; A – N° 45 15 mars 2012</i>
Definitions (Art 2)		
'critical infrastructure'	'Critical infrastructure' means an asset, system or part thereof, located in Member States of the EU, which is essential for the maintenance of the vital functions of society, health, safety, security, and the economic or social well-being of citizens, the disruption or destruction of which would have a significant impact in a Member State due to the failure of these functions	
'European critical infrastructure'	"European critical infrastructure" or "ECI" means a critical infrastructure located in Member States of the EU whose disruption or destruction would have a considerable impact on at least two Member States. The significance of this impact is assessed in terms of cross-cutting criteria. This includes the effects resulting from cross-sectoral dependencies compared to other types of infrastructure	
'risk analysis'	"Risk analysis" : review of relevant threat scenarios to assess critical infrastructure vulnerabilities and the potential impacts of their disruption or destruction;	
'sensitive critical infrastructure protection related information'	"Sensitive critical infrastructure protection related information" means information on a critical infrastructure that, in the case of disclosure, could be used to plan and implement actions aimed at causing the disruption or destruction of critical infrastructure installations	
'protection'	"Protection" means all activities aimed at ensuring the proper functionality, continuity and integrity of a critical infrastructure to prevent, mitigate or neutralise a threat, risk or vulnerability;	
'owners/operators of ECI'	'European Critical Infrastructure Owners/Operators' means those entities responsible for investments in, and/or in the day-to-day operation of, a particular asset, system or part of it, designated as ECI	
Other relevant national definitions	"Cross-cutting criteria" means the number of victims (potential number of deaths or injuries); the economic impact (magnitude of economic losses and/or degradation of products or services, including the potential impact on the environment); the impact on the population (impact on public confidence, physical suffering and disruption of daily life, including the disappearance of essential services).	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	Thresholds for cross-cutting criteria are based on the severity of the impact of the disruption or destruction of a given infrastructure.	
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	The Regulation applies to the energy and transport sectors and their respective subsectors. I. Energy 1. Electricity 2. Oil 3. Gas II. Transport 1. Road transport 2. Rail transport 3. Air transport 4. Inland navigation 5. Deep sea and short sea shipping (cabotage) and ports	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.</i> (Annex 1)
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	HCPN (<i>Haut-Commissariat à la Protection Nationale</i>) The mission of the HCPN, in collaboration with the Ministries, administrations and services, is to identify ECI that meet both cross-cutting and sectoral criteria in accordance with the procedure set out in Annex II (see below) and taking into account the non-binding guidelines developed by the European Commission on the application of cross-cutting and sectoral criteria and thresholds to be used to identify ECI	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 4</i>
Application of the procedure for the identification of ECI (as per Annex III)	To identify potential ECI and to designate them as ECI, the HCPN applies a procedure in consultation with the competent ministerial departments. The potential ECI that does not meet the requirements of one of the stages is considered "Non ECI" and is excluded from the procedure.	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Annex II)</i>
<i>Step1 – Application of sectoral criteria</i>	HCPN shall apply the sectoral criteria in order to make a first selection among the critical infrastructures existing within a sector.	
<i>Step 2 – Application of the definition of critical infrastructure</i>	HCPN shall apply the definition of critical infrastructure (see list of definition) to the potential ECI identified in Step 1. The severity of the impact is determined by applying the national methods for the identification of critical infrastructures or on the basis of intersectoral criteria. For infrastructures providing an essential service, the existence of	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	alternatives, as well as the duration of the shutdown/recovery are taken into account.	
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	HCPN shall the transboundary element of the definition of ECI (see list of definition) to the potential ECI. For infrastructures providing an essential service, the existence of alternatives, as well as the duration of the shutdown/recovery are taken into account.	
<i>Step 4 – Application of the cross-cutting criteria</i>	HCPN shall apply cross-cutting criteria to remaining ECI. Cross-cutting criteria take into account the severity of the impact and, for infrastructures providing an essential service, the existence of alternatives, as well as the duration of the shutdown/recovery.	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	"Cross-cutting criteria" means the number of victims (potential number of deaths or injuries); the economic impact (magnitude of economic losses and/or degradation of products or services, including the potential impact on the environment); the impact on the population (impact on public confidence, physical suffering and disruption of daily life, including the disappearance of essential services). Thresholds for cross-cutting criteria are based on the severity of the impact of the disruption or destruction of a given infrastructure.	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 3</i>
Identification of potential ECI on an ongoing basis (Art 3.1)	The HCPN shall proceed on permanent basis to the identification of potential ECI.	<i>Art. 4 (1) b)</i>
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	HCPN is responsible for proceeding to the designation of a potential ECI located on the national territory as an ECI, after agreement, first, with the Minister in charge of the respective sector and, secondly, with the Member States that are likely to be significantly affected by the infrastructure.	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 4.(1) e)</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	The identification of potential ECI that pass through all stages of the procedure is communicated to Member States that may be significantly affected by those infrastructures.	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		<i>désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 4. (1) d)</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	The HCPN informs the Member States that may be significantly affected by an ECI of the existence of this infrastructure and the reasons for its designation as a potential ECI, and to enter into bilateral or multilateral discussions with the competent authorities of those Member States;	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 4.d</i>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	There is no such provision; however, the HCPN would be the competent authority.	
Agreement for the designation of the ECI (Art. 4.3)	HCPN is responsible for proceeding to the designation of a potential ECI located on the national territory as an ECI, after agreement, initially, with the Minister in charge of the respective sector and, secondly, with the Member States that may be significantly affected by the infrastructure.	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 4(1) e)</i>
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The HCPN is responsible for informing the EC once a year of the number of designated ECI by sector and the number of Member States concerned by each of them.	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 4. (1) g)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Informing the owner/operator of the designated ECI (Art. 4.5)	HCPN informs the owner or operator of the critical infrastructure of its designation as ECI	Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 4.f
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The HCPN shall verify that each ECI operator has put in place an OSP or equivalent measures.	Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 5
Verification that the OSP or equivalent is in place	The HCPN shall verify that each CI operator has put in place the OSP or equivalent measures. The OSP is reviewed after one year as of the designation of the ECI or another HCPN-approved period. Afterwards, the owner or operator of the ECI updates the OSP on a regular basis.	Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 5
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The HCPN shall verify that each CI operator has put in place a security liaison officer or equivalent.	Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 6

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Function of the SLO (Art. 6.1)	The designated SLO acts as a point of contact for any security-related matters with the HCPN.	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 6</i>
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	The HCPN shall verify that each ECI operator has put in place a security liaison officer or equivalent.	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 6</i>
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	The HCPN shall put in place an appropriate communication mechanism with the security correspondent or the equivalent person in order to exchange the relevant information concerning the identified risks and threats facing the ECI.	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 6</i>
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	HCPN	<i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 3 c), Art. 4.(1) h)</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	The HCPN is responsible for carrying out a threat assessment of the ECI sub-sectors within one year of the designation of a critical infrastructure located in the national territory as ECI within these sub-sectors.	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The HCPN is responsible for submitting to the European Commission every two years a report on the types of vulnerabilities, threats and risks encountered in each ECI sector with an ECI designated as such and located in the national territory.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	<p>According to Art. 4. (1) of the <i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, the HCPN shall be the national point of contact for the protection of ECI.</i></p> <p>Art. 3. (1) <i>in fine</i> of the Law of 23 July 2016 designates the HCPN as the point of contact for Luxembourg with European and international institutions and organisations and tasks it to ensure effective co-operation with these entities</p>	<p><i>Loi du 23 Juillet 2016, Haut-Commissariat à la Protection nationale, Publication: 28/07/2016, Art.3. (1).</i></p> <p><i>Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Art. 4</i></p>
MS body(-ies) serving as ECIP contact point	HCPN, under the authority of the Prime Minister, is the competent authority and point of contact for the protection of ECI	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<ul style="list-style-type: none"> • Law of 23 July 2016 establishing the Office of the High Commissioner for National Protection • The Concept for National Protection, as defined by the Law of 23 July 2016 • The National Strategy for Crisis Management, as provided for by Art. 3 (1) b) (1.) • Grand-Ducal Regulation of February 21, 2018 determining the procedures for the identification and designation of critical infrastructures • Grand-Ducal Regulation of February 21, 2018 laying down the structure of the security and business continuity plans for critical infrastructures • Grand-Ducal Decision of 9 May 2018 determining the organisation and the tasks of the governmental centre for computer emergency response 	<p><i>Law of 23 July 2016 establishing the Office of the High Commissioner for National Protection</i></p> <p><i>Grand-Ducal Regulation of February 21, 2018 determining the procedures for the identification and designation of critical infrastructures has identified the sectors in which CI are present.</i></p> <p><i>Grand-Ducal Regulation of February 21, 2018 determining the procedures for the identification and designation of</i></p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> Grand-Ducal Decision of 9 May 2018 on the governance of information security management <p>(National) critical infrastructure is defined as any asset, system or part thereof indispensable for safeguarding the vital interests or essential needs of all or part of the country or population, or which may face a particular threat. Any asset, system or part thereof that does not meet this definition may be identified and designated as CI if the operation of a CI depends on it. Also, a sector or part of a sector may be identified and designated as CI if the whole is considered as such even though not all of the elements meet the definition.</p> <p>Critical infrastructure protection includes all activities aimed at preventing, mitigating or neutralising the risk of a reduction or discontinuity in the availability of supplies or services essential for the safeguarding of vital interests or the essential needs of all or part of the country or population offered through the infrastructure and the external risk to which the infrastructure may be subject.</p>	<i>critical infrastructures has identified some sectors in which CI are present.</i>
Scope of national CIP policy		
Sectors of critical importance	<p>Sectors of Critical Importance: 9 sectors</p> <ol style="list-style-type: none"> Energy sector includes the production and distribution of electricity, the conditioning and gas distribution and storage and trading of oil; Information and communication technology sector extends on one side to areas of computer programming, computer facilities management, processing data services, hosting of information services and internet portals. The component of communication covers wired telecommunications, wireless telecommunications and satellite telecommunications; Finance sector includes the activities of the central bank, as well as the infrastructure and systems for the exchange, payment and settlement of financial instruments; Health sector counts the hospital activities, as well as the laboratories for medical analyses; Food sector includes the food supply, food production and food safety Water sector includes water collection, treatment and distribution, collection and treatment wastewater, as well as the collection, treatment and disposal of waste; 	<p><i>Law of 23 July 2016 establishing the Office of the High Commissioner for National Protection</i></p> <p><i>Grand-Ducal Regulation of February 21, 2018 determining the procedures for the identification and designation of critical infrastructures has identified some sectors in which CI are present.</i></p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>7. Transport sector consists of land transport (road and rail), transport by water (maritime and fluvial), air transport and post and mail activities;</p> <p>8. Chemical industry sector targets infrastructure handling dangerous substances;</p> <p>9. Public administration aims in particular at public prerogative services, such as the defence, justice, public order and security activities and emergency services.</p>	
Number of national CI	Non-public information.	
Number of national CI operators	Non-public information.	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	<p>Information on the national CIP strategy is provided by the law of 23 July 2016 providing for the creation of the High Commission for National Protection, by the parliamentary dossier n° 6475, and by the National Strategy for Crisis Management.</p> <p>The HCPN is responsible for identification and designation of CI. Therefore, the HCPN coordinates with the relevant sectoral authorities. The CI owner or operator is responsible for the protection of the CI. They shall provide to the HCPN their security and business continuity plan, including the security measures for the protection of the CI. The HCPN provides to the CI owner or operator recommendations on the described measures, which allow ensuring the protection of the CI, enhancing the resilience of the CI and facilitating the management of a crisis.</p>	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy		
Coordination of ministries, bodies and offices concerned	Coordination of Ministries: HCPN acts as coordinator	
Communication with owners/operators	The owners or operators of critical infrastructure shall make available to the HCPN all data requested for the purpose of the identification, designation and protection of critical infrastructure. This data includes all the information that is needed in the context of crisis prevention or management. Critical infrastructure data subject to registration, disclosure, declaration, enumeration, classification, authorisation or notification required by law or by the relevant regulations are communicated to the HPCN, at its request, by the	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>ministerial departments, administrations and State services that hold these data.</p> <p>The CI owner or operator is responsible for the protection of the CI. They shall provide to the HCPN their security and business continuity plan, including the security measures for the protection of the CI. The HCPN provides to the CI owner or operator recommendations on the described measures, which allow ensuring the protection of the CI, enhancing the resilience of the CI and facilitating the management of a crisis.</p> <p>The CI owner or operator shall notify the HCPN about any incident with a significant impact to the safety and sustainability of the operation of the CI.</p>	
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	In case of an imminent or actual crisis, the CI owner or operator shall provide (physical) access to the agents of the HCPN to any installations, premises, land, facilities forming part of the infrastructure.	
Other relevant aspects of national authorities involved in CIP protection	See answers above.	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Yes.	Art. 8 (2) Law 23.7.2016
- Preparation of a security plan	Yes.	Art. 8 (1) Law 23.7.2016
- Review of the plan (timing)	Yes.	RGD 21.2.2018
- Reporting incidents	Yes.	Art. 8 (3) Law 23.7.2016
- Exchange of information	Yes.	Art. 6. 8. Law 23.7.2016
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures 	<p>All-hazard approach, sectoral approach (9 sectors have been identified), top-down approach (cf. RECIPE).</p> <p>The national CIP framework is an integrated part of the national crisis management framework, an integrated part of the national concept for</p>	National Cybersecurity Strategy III, Approved and made enforceable by the Government on 26 January 2018.

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
<ul style="list-style-type: none"> - Channels used for information exchange 	<p>national protection, and is coherent with the national strategy for cyber security.</p> <p>The HCPN is the central national competent authority in charge of initiating, coordinating and ensuring the implementation of activities and measures relating to the identification, designation and protection of critical infrastructure.</p> <p>Recommendations by HCPN to security and business continuity plans of CI owners or operators inspired by ISO 22301:2012 (BCMS family, including and not limited to 22313, 22317) and ISO 31000:2018 (RM family, including and not limited to 31010).</p> <p>The Luxembourg government adopted the National Strategy on Cyber Security – version 3 - on 26 January 2018.</p>	

Malta

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114			
Provision		Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system		<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011</i>	
Definitions (Art 2)			
'critical infrastructure'	<i>Definitions in the next column are as per L.N. 434/2011. However please note that Legal Notice (L.N. 434/2011) requires a complete review. Said review is planned for 2019. Definitions, where different, will be updated in line with the recently transposed NIS Directive into local Malta Legislation i.e. L.N. 216/2018</i>	" critical infrastructure " or "CI" means an asset, system or part thereof located in Malta which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 2</i>
'European critical infrastructure'		" European critical infrastructure " or "ECI" means critical infrastructure located in Malta the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria which shall include effects resulting from cross-sector dependencies on other types of infrastructure.	
'risk analysis'		" risk analysis " means consideration of relevant threat scenarios in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure;	
'sensitive critical infrastructure protection related information'		" sensitive critical infrastructure protection related information" means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations;	
'protection'		" protection " means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability	
'owners/operators of ECI'		" owners or operators of CI " means those entities responsible for investments in, and, or day-to-day operation of, a particular asset, system or part thereof designated as a CI or an ECI under this Order;	
Other relevant national definitions		" Member State " means a Member State of the European Union	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114			
Provision		Content	Source
Scope (Art 3.3)			
<p>Sectors and sub-sectors in scope:</p> <ul style="list-style-type: none"> - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports) 	<p><i>As regards ECI's: Energy & Transport.</i></p> <p><i>Intention is to apply more sectors, as in L.N. 216/2018, when review of L.N. 434/2011 takes place.</i></p>	<p>The following sectors and subsectors are subject to the Order:</p> <p>(a) the energy sector which is divided into the following subsectors:</p> <ol style="list-style-type: none"> (1) electricity, comprising infrastructures and facilities for generation and transmission of electricity in respect of supply of electricity; (2) oil, comprising oil production, refining, treatment, storage and transmission by pipelines; (3) gas, comprising gas production, refining, treatment, storage and transmission by pipelines, and LNG terminals; <p>(b) the transport sector which is divided into the following subsectors:</p> <ol style="list-style-type: none"> (1) road transport; (2) air transport; (3) ocean and short-sea shipping; (4) ports. 	<p><i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 4</i></p>
Identification of the ECI (Art. 3)			
MS body(-ies) responsible for the identification of potential ECI		The Malta Critical Infrastructure Protection Unit within the Malta CIPD is the body responsible for the identification and designation of potential ECI	<p><i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 3</i></p>
Application of the procedure for the identification of ECI (as per Annex III)	<i>The cross cutting criteria is used to identify potential ECI's.</i>	<p>In identifying critical infrastructures which may be designated as an ECI, the Unit shall apply the following consecutive steps:</p> <ol style="list-style-type: none"> (1) In Step 1, the sectoral criteria are identified; (2) In Step 2, the definition of the term "critical infrastructure" are applied (3) In Step 3, the trans-boundary element of the definition of ECI" (4) In Step 4, the cross-cutting criteria are applied. 	<p><i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 4</i></p>
Step1 – Application of sectoral criteria	<i>As in previous reply.</i>	In Step 1, the sectoral criteria referred to in article 4 (see sectors and subsectors in scope) shall be applied in order to make a first selection of critical infrastructures within each sector. Specific mention is not made as to how this is implemented in practice.	<p><i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 4</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114			
Provision		Content	Source
Step 2 – Application of the definition of critical infrastructure	As in previous reply.	In Step 2, the definition of the term "critical infrastructure" is applied. Specific mention is not made as to how this is implemented in practice.	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 4</i>
Step 3 – Application of the transboundary element of the definition of ECI		The trans-boundary element of the definition of "ECI" shall be applied to the potential ECI that has passed the first two steps of this procedure. A potential ECI which does satisfy the definition shall follow the next step of the procedure. For infrastructure providing an essential service, the availability of alternatives and the duration of disruption or recovery or both shall be taken into account.	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 4</i>
Step 4 – Application of the cross-cutting criteria	As in previous reply.	In Step 4, the cross-cutting criteria set out in article 4(2) shall be applied to the remaining potential ECI. Such cross-cutting criteria shall take into account - <ol style="list-style-type: none"> 1. The severity of impact; 2. for infrastructure providing an essential service, the availability of alternatives; and 3. The duration of disruption or recovery or both. A potential ECI which does not satisfy the cross-cutting criteria shall not be considered to be an ECI	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 4</i>
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)		The thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Unit, and shall be based on the severity of the impact of the disruption or destruction of a particular critical infrastructure This is based on the level of disruption on the delivery of the essential services provided by the potential NCI/ECI. The fact that a disruption occurs, which disruption leads to a severe impact, for a non-acceptable duration, taking into consideration alternative solution/s as well as available recovery plans, are considered.	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011, Article 4</i>
Identification of potential ECI on an ongoing basis (Art 3.1)		The process of identifying and designating ECI under this Order shall be reviewed on a regular basis. The process is ongoing, at the same time it is reviewed on a yearly basis.	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; (Article 4)</i>
Designation of the ECI (Art. 4)			

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114			
Provision		Content	Source
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	Malta CIP Unit with CIPD as well as the Govt. Ministries within Public Administration having NCI's within their portfolio.	<p>Malta Critical Infrastructure Protection Unit.</p> <p>The Unit shall, in accordance with the procedure set out in the Schedule, identify potential European Critical Infrastructures in Malta which –</p> <ul style="list-style-type: none"> • Satisfy the cross-cutting and sectoral criteria set out in this article; and • Meet the definitions of the terms "critical infrastructure" and "European critical infrastructure" in article 2. 	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; (Article 4)</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)		<p>The Unit shall inform the relevant authorities in other Member States which may be significantly affected by a potential ECI about its identity and the reasons for its designation as a potential ECI.</p> <p>In the event an NCI is also declared as an ECI it will be declared as such following consultation and agreement with the respective CIP Competent Authority in the MS that may be impacted by a disruption occurring at the potential ECI.</p>	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; (Article 5)</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)		<p>Where a potential ECI is located in Malta, the Unit shall –</p> <ul style="list-style-type: none"> • Engage in discussions with the relevant authorities in other Member States which may be significantly affected by the potential ECI; and • Designate it as an ECI following an agreement between the Government of Malta and the Member States which may be significantly affected <p>The local Malta Competent CIP Authority, namely the CIP Unit within the CIPD will engage in discussions with the peer Competent Authority in the potentially affected MS/s.</p>	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; (Article 5)</i>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)		N/A	
Agreement for the designation of the ECI (Art. 4.3)		It is not specified how the agreement is achieved. It is specified only that when a potential ECI in the territory of Malta is identified	<i>Infrastructures and European Critical Infrastructures (Identification, Designation</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114			
Provision		Content	Source
		there is an agreement between the Government of Malta and the Member States. When the respective CIP Competent Authorities in the potentially impacted MS's agree in principle that an NCI under review is declared as an ECI.	and Protection) Order, 2011; (Article 5)
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)		The Unit shall inform the European Commission on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds. The channels used are not specified. The Malta CIP Unit will inform the Commission through DG-Home	Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; (Article 4) Article 4 (4)
Informing the owner/operator of the designated ECI (Art. 4.5)		Where an ECI is located in Malta, the Unit shall inform the owner or operator of the infrastructure concerning its designation as an ECI and such information shall be classified at an appropriate level. The channels used are not specified. Designation of an ECI is formally communicated to the owner/operator through the designated SLO of the designated NCI.	Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; (Article 5)
Operator Security Plan (Art. 5)			
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	See updated definition of an OSP in L.N. 216 of 2018	The Unit shall assess whether each designated CI and ECI located in Malta possesses an OSP or has in place equivalent measures addressing the issues identified below <ul style="list-style-type: none"> • The identification of important assets; • The conduct of a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; and • The identification, selection and prioritisation of counter-measures and procedures with a distinction between - <ul style="list-style-type: none"> ○ Permanent security measures, which identify indispensable security investments and means which are relevant to be employed at all times; and ○ Graduated security measures, which can be activated according to varying risk and threat levels. • That it include information concerning: <ul style="list-style-type: none"> ○ General measures such as technical measures, including installation of detection, access control, protection and prevention means; 	Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; (Article 6)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114			
Provision		Content	Source
		<ul style="list-style-type: none">Organisational measures, including procedures for alerts and crisis management;Control and verification measures;Communication;Awareness raising and training; andSecurity of information systems <p>The Unit shall ensure that the OSP or equivalent measures pursuant above are in place and are reviewed regularly within one year following designation of each CI and each ECI.</p>	
Verification that the OSP or equivalent is in place		If the Unit finds that an OSP or equivalent measures have not been prepared, it shall ensure, by any measures deemed appropriate, that the OSP or equivalent measures are prepared addressing the issues identified above.	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Articles 6-7</i>
Verification that the OSP or equivalent is appropriately and regularly reviewed			
		Verification of an OSP (drawing-up and maintenance) is preferably carried out through physical checks through discussions and in liaison with the designated SLO of the NCI/ECI concerned. The OSP is evaluated for its applicability via Simulation Exercising of the OSP from time to time.	<i>Article 3 (3) (f), etc...</i>
Security Liaison Officer (Art. 6)			
MS authority responsible for ensuring that the SLO or equivalent is in place		The Unit shall assess whether each designated ECI located in Malta possesses a Security Liaison Officer or equivalent who shall act as the point of contact for security related issues between the owner or operator of the ECI and the Unit.	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 8</i>
Function of the SLO (Art. 6.1)		Act as the point of contact for security related issues between the owner or operator of the ECI and the Unit.	
		Responsibilities of the SLO: As Point of contact between NCI/ECI and Competent Authority; the drawing up and maintenance of RA's and OSP's as well as the sharing/exchange of any necessary information as may be directed by the CIP Unit. For a profile of the SLO see Malta CIP Web-site .	
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	<i>Once an SLO is designated, that SLO forms part of the Sectoral Forum made up of NCI within such sector.</i>	If the Unit finds that a Security Liaison Officer or equivalent does not exist in relation to a designated ECI it shall ensure, by any measures deemed appropriate, that such a Security Liaison Officer or equivalent is designated:	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114			
Provision		Content	Source
	See MCIP Structure at Malta CIP Web-site where various sectoral and other forums are indicated.	Provided that compliance with any measure, including a European Union measure, which in a particular sector requires, or refers to a need to have, a Security Liaison Officer or equivalent shall be deemed to satisfy all the requirements under this article	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)		<p>The Unit shall implement an appropriate communication mechanism between itself and each Security Liaison Officer or equivalent, with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned. This communication mechanism shall be without prejudice to the requirements concerning access to sensitive and classified information laid down by any other law.</p> <p>A communication mechanism exist through the designated SLO for each and every designated NCI/ECI on a one-to-one basis and through the Sectoral forums. This is ongoing between the NCI/ECI and the SLO reviewing respective RA's and OSP's as well as the exchange of information.</p>	
Reporting (Art. 7)			
MS body(-ies) responsible for fulfilling reporting obligations		The Unit shall conduct a threat assessment in relation to CI and ECI subsectors within one year following the designation of critical infrastructure in Malta as a CI or an ECI within those subsectors.	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 9</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI		The evaluation of the respective RA's and OSP's including the results of any simulation exercising carried out through the year to evaluate the doability and applicability of the RA's and OSP's ensuring that identified risk-plans and potential disruption scenarios plans in OSP's are effective in the event of a disruption.	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector		Every two years the Unit shall submit to the European Commission a classified report containing generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI under 5. The specific content of the summary is not specified	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114			
Provision		Content	Source
		In the event ECI's are identified a summary list of risks, threats and vulnerabilities encountered will be documented per ECI sector.	
European critical infrastructure protection contact points (Art. 10)			
Appointment of a ECIP contact point	<i>How did the appointment of the ECIP contact point take place?</i>	The CIP Directorate (established in 2014), which coordinates the CIP Unit of the Ministry for Home Affairs and National Security acts as the European critical infrastructure protection contact point ("ECIP contact point") in Malta, and coordinates European critical infrastructure protection issues within Malta, with other Member States, and with the European Commission	<i>Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order, 2011; Article 3</i>
MS body(-ies) serving as ECIP contact point		The CIP PoC is appointed by Cabinet Office or by the Minister for Home Affairs and National Security. To-date this role has been assigned to the Director CIP. It is likely that this appointment will, in the near future, be embedded through legislation.	

NATIONAL CIP FRAMEWORK			
Key dimension		Content	Source
List of key measures on the protection of national Critical Infrastructures		Malta has a dedicated CIP Directorate which acts according the objectives defined by L.N. 434 of 2011 on Critical Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order as well as the objectives defined by L.N. 216 of 2018 on Measures for High Common Level of Security of Network and Information Systems Order of 2018. These Orders are the transposition of Council Directive 2008/114/EC of 8th December 2008 and Council Directive 2016/1148 of 6th July 2016 (better known as the NIS Directive), respectively.	https://maltacip.gov.mt/en/About/Pages/About-Us.aspx
Scope of national CIP policy			
Sectors of critical importance		The national critical infrastructure spreads over nine sectors. While not all sectors carry the same weight, any sector contains critical elements/assets that the	https://maltacip.gov.mt/en/About/Pages/About-Us.aspx

NATIONAL CIP FRAMEWORK			
Key dimension		Content	Source
		<p>loss or compromise of which would have a major impact on the availability or integrity of essential services that support the nation's security, economic stability and well-being of citizens. These are Energy, Finance & Industry, Food, Government, Health, Telecoms & Technology, Transport, Water and the Emergency Services.</p> <p>Energy, Transport, Telecoms & Digital Information, Health, Drinking Water, Food, Banking and Finance, Public Administration, and the Emergency Services</p> <p>See Malta CIPD Structure</p>	
Number of national CI		N/A	
Number of national CI operators		N/A	
Responsibilities allocated to Ministries, bodies, and offices			
Definition of scope and objectives of the national CIP strategy	<i>The Malta CIPD is the responsible competent authority for the protection of NCI's, NCII's, OES's and DSP's in Malta.</i>	Malta CIP strategy based on transposition of EU Directive 114/2008. The Malta CIP Unit, within the CIP Directorate of the Ministry for Home Affairs and National Security, is entrusted with a coordinating role of all Critical Infrastructure Protection and Emergency and Disaster Management issues on a national level.	Webpage of the Malta CIP Unit: https://maltacip.gov.mt/en/Pages/MaltaCIP.aspx
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy		<p>A fundamental role of the Malta CIP Unit is to direct and advise owners and operators of CI regarding the necessary internal systems to identify associated vulnerabilities, hazards and risks, and the planning for contingencies:</p> <ul style="list-style-type: none"> Ensuring that a risk assessment is carried out by all owners or operators of CI; 	https://homeaffairs.gov.mt/en/MHAS-Departments/MaltaCIPD/Pages/MaltaCIPD.aspx

NATIONAL CIP FRAMEWORK			
Key dimension		Content	Source
		<ul style="list-style-type: none"> Ensuring that each owner or operator of a CI draws up and maintains an Operator Security Plan 	
Coordination of ministries, bodies and offices concerned		The Malta CIP Unit coordinates amongst all stakeholders involved in the management of Critical Infrastructures (CI), Critical Information Infrastructures (CII), the Emergency & Security Services (Civil Protection, Police & AFM), Emergency Health Services, other organisations involved in national Emergency and Disaster Management, and the Government Contingency Centre, incorporating owners, operators, entities, departments and other bodies as may be directed.	https://maltacip.gov.mt/en/Pages/MaltaCIP.aspx
Communication with owners/operators		Same as described in the Directive	https://maltacip.gov.mt/en/Pages/MaltaCIP.aspx
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)		The Malta CIP Unit coordinates and supports general emergency preparedness plans capable of responding to national emergencies involving the emergency services (i.e. Civil Protection Department, Police, AFM, Health and other related stakeholders as may be required by specific national emergencies).	https://maltacip.gov.mt/en/CIP_Structure/Pages/CIP-Unit.aspx

NATIONAL CIP FRAMEWORK			
Key dimension		Content	Source
Other relevant aspects of national authorities involved in CIP protection		<p>The Malta Critical Infrastructure Protection (CIP) Directorate (CIPD) operates within the portfolio of the Ministry for Home Affairs and National Security (MHAS) in Malta. It acts according the objectives defined by L.N. 434 of 2011 on Critical Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order as well as the objectives defined by L.N. 216 of 2018 on Measures for High Common Level of Security of Network and Information Systems Order of 2018. These Orders are the transposition of Council Directive 2008/114/EC of 8th December 2008 and Council Directive 2016/1148 of 6th July 2016 (better known as the NIS Directive), respectively.</p> <p>The Malta CIP Directorate establishes the criteria for the identification and designation of Critical Infrastructures (CI's), Critical Information Infrastructures (CII's), and Operators of Essential Services (OES's) and maintains a national inventory</p>	<p>Malta Critical Infrastructure Protection Directorate</p> <p><i>Measures For High Common Level of Security of Network and Information Systems Order, 2018 Article 26</i></p>

NATIONAL CIP FRAMEWORK			
Key dimension		Content	Source
		<p>of critical assets within designated Critical Infrastructures and Critical Information Infrastructures. Moreover, the Directorate ensures, amongst others, that Critical Infrastructure (CI) and Critical Information Infrastructure (CII) owners or operators and Operators of Essential Services (OES):</p> <ul style="list-style-type: none"> ○ Conduct an appropriate Risk Assessment; ○ Draw and maintain an suitable Operator Security Plan (OSP); ○ Perform operational reviewing, updating and the necessary exercising of such plans (OSPs); ○ Share CI, CII information as may be required from time to time, and ○ Operators of Essential Services report incidents having a significant impact on the continuity of the essential services they provide <p>There shall be a National CSIRT autonomous CSIRT" means a self-organised CSIRT which provides a monitoring function of CSIRT services and alerts to its own business or other agencies, operators of essential services or digital service providers. CSIRT shall be responsible for risk and incident handling in accordance with a well-defined process. The Computer Security Incident Response Team works with Malta critical infrastructure protection in order to protect all the critical infrastructure</p>	
Responsibilities allocated to operators of national CI			
- Appointment of a security officer	Do operators of national CI need to meet these	The Unit shall assess whether each designated CI located in Malta possesses an OSP	https://maltacip.gov.mt/en/Pages/MaltaCIP.aspx
- Preparation of a security plan		Same as described the directive	https://maltacip.gov.mt/en/Pages/MaltaCIP.aspx

NATIONAL CIP FRAMEWORK			
Key dimension		Content	Source
<ul style="list-style-type: none"> - Review of the plan (timing) 	<p>obligations? And how?</p> <p>Already replied to in above replies.</p>	Same as described the directive	https://maltacip.gov.mt/en/Pages/MaltaCIP.aspx
<ul style="list-style-type: none"> - Reporting incidents 		Concerning Operators of essential services shall notify the CIIP Unit, without undue delay, of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the CIIP Unit to determine, any local or cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.	Measures For High Common Level of Security of Network and Information Systems Order, 2018 Article 11
<ul style="list-style-type: none"> - Exchange of information 		N/A	
Other distinctive features of the national CIP framework			
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p><i>A National Cyber Security Strategy is in place and a National Strategy on the security of network and information systems (L.N. 216/2018 Art. 8) will be taken in hand during 2019.</i></p> <p><i>The rest has been dealt with in the replies above.</i></p>	<p>Cybersecurity</p> <p>Malta CIP provides adequate early warnings/alerts and advice via CSIRTMalta concerning Cyber threats and incidents, reaching out to operators of Critical Information Infrastructures (CII) and ultimately to other sectors, businesses and citizens.</p> <p>Furthermore it was launched the initiative to underline and underscore the cyber security strategy through the Green book which, This Green Paper, along with its supporting document intends to inculcate an awareness of cyber security, its extent and its implications of which Malta, as an integral part of cyberspace, needs to consider. Launching cyber security on a national scale, essentially calls for a planned, collective and systemic approach, thus leading to the need of a National Cyber Security Strategy. Digital Malta – the National Digital Strategy for the period 2014-2020 recognises and proposes the fulfilment of such need. Thus, the Green Paper presents a high level,</p>	<i>MALTA NATIONAL CYBERSECURITY STRATEGY GREEN PAPER, 2015</i>

NATIONAL CIP FRAMEWORK			
Key dimension		Content	Source
		strategic approach for cyber security on a national scale, for detailed consultation. The consultation is intended to consolidate further the proposals, thus leading to the launch of the first National Cyber Security Strategy.	

Netherlands

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Amendment to the National CIP framework through the publication of the implementation program and requirement on the Official Gazette on the 23rd of December 2010</i>	
Definitions (Art 2)		
'critical infrastructure'	<i>No definition provided in transposition of Directive</i>	
'European critical infrastructure'	<i>No definition provided in transposition of Directive</i>	
'risk analysis'	<i>No definition provided in transposition of Directive</i>	
'sensitive critical infrastructure protection related information'	<i>No definition provided in transposition of Directive</i>	
'protection'	<i>No definition provided in transposition of Directive</i>	
'owners/operators of ECI'	<i>No definition provided in transposition of Directive</i>	
Other relevant national definitions		
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Sector of Critical Importance: - Energy (national transport and distribution of electricity, regional distribution of electricity, gas production, national transport and distribution of gas, regional distribution of gas, oil supply) - Transport (air traffic control, Geolocation and time information by GPS, vessel traffic service)	Critical Infrastructure Protection in The Netherlands
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The responsible ministry establishes general frameworks for the sectors that fall under its responsibility (in policy or in laws and regulations). The ministries are responsible for identifying potential ECI. The National Coordinator for Security and Counterterrorism is responsible for the overall management of CIP policies in the Netherlands.	Critical Infrastructure Protection in The Netherlands
Application of the procedure for the identification of ECI (as per Annex III)	See below	
<i>Step1 – Application of sectoral criteria</i>	Each responsible ministry annually assesses the impact of vital infrastructure in the Netherlands	<i>Mededeling inzake de implementatie van richtlijn</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		2008/114/EG, Staatscourant, 24/12/2010
<i>Step 2 – Application of the definition of critical infrastructure</i>	Not indicated in transposition documents	
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	Each responsible ministry annually assesses the impact of vital infrastructure in the Netherlands on other member states and on which infrastructure in other Member States the Netherlands depends.	Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010
<i>Step 4 – Application of the cross-cutting criteria</i>	Not indicated in transposition documents	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	Not indicated in transposition documents	
Identification of potential ECI on an ongoing basis (Art 3.1)	The sectorally responsible ministry, supported by the CIP contact point, will examine which infrastructure in the Netherlands could potentially be an ECI. The responsible ministry will also look at infrastructures located abroad on which the Netherlands is dependent, which should be considered as an ECI. In particular, each responsible ministry annually assesses the impact of vital infrastructure in the Netherlands on other member states and on which infrastructure in other Member States the Netherlands depends.	Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	The CIP contact point in the Netherlands informs other member states if there is a potential ECI. The Council of Ministers determines whether an ECI should be designated as such.	Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	By way of the interdepartmental joint committee and the CIP contact point, the impacted countries (Member States which are dependent on an infrastructure situated in the Netherlands) are informed by a formal letter and invited to consult with the responsible Dutch ministry the sector. This letter will be signed by the coordinating minister of the Ministry of Justice and Security and the responsible minister.	Booz & Company (2009), Study: stock-taking of existing critical infrastructure protection activities
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	The Ministry of Justice and Security, supported by sectoral ministry.	Booz & Company (2009), Study: stock-taking of existing critical infrastructure protection activities
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	If requested, the European Commission may play a mediating role in the negotiating process. The CIP contact point in the Netherlands informs other member states if there is a potential ECI.	Booz & Company (2009), Study: stock-taking of existing critical infrastructure protection activities

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Agreement for the designation of the ECI (Art. 4.3)	It will be agreed jointly (impacted countries and the Netherlands) whether the infrastructure concerned is an ECI or not. The decision whether an infrastructure in the Netherlands is critical at a European level will be taken in the Council of Ministers.	<i>Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010</i>
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	CIP CP in NL sends to the EC the number of designated ECI per sector and affected MS	<i>Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010</i>
Informing the owner/operator of the designated ECI (Art. 4.5)	Not indicated.	
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	Sectorally competent ministry	<ul style="list-style-type: none"><i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report.</i>
Verification that the OSP or equivalent is in place	OSP equivalent requirements in place prior to the directive, if OSP missing in an ECI, the sectoral Ministry ensures ones is put in place	<ul style="list-style-type: none"><i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report.</i>
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	If an ECI is identified, the responsible minister, in co-operation with the ECI, will ensure that a safety liaison officer is appointed.	<i>Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010</i>
Function of the SLO (Art. 6.1)	As per parameters of the Directive	
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	SLO equivalent requirements in place prior to the directive, if OSP missing in an ECI, the sectoral Ministry ensures ones is put in place	<ul style="list-style-type: none"><i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report.</i>
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	This is done on the basis of the Security Screening and Classification Act in accordance with the Civil Service Information Security Regulations - special information (Virbi). Communication procedures are put in place to Ensure confidentiality and a sufficient level of screening.	<i>Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	The CIP contact point is responsible	<i>Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	The European Commission receives an extract from the National Risk Assessment that the Netherlands carries out on a structural basis.	<i>Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010</i>
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The European Commission receives an extract from the National Risk Assessment that the Netherlands carries out on a structural basis. CIP CP in NL sends to the EC the number of designated ECI per sector and affected MS	<i>Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010</i>
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The CIP contact point was established on 1 February 2009 on the basis of the CIP CP NL Program of Requirements.	<i>Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010</i>
MS body(-ies) serving as ECIP contact point	ECIP: Ministry of Justice and Security The CIP contact point is a joint committee of the various ministries (explicitly not under the sole responsibility of the Ministry of the Interior and Kingdom Relations), and handles process management, support, archiving and coordination. In process terms, the CIP contact point comes under the Ministry of Justice and Security, NCTV.	<i>Mededeling inzake de implementatie van richtlijn 2008/114/EG, Staatscourant, 24/12/2010</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures		
Scope of national CIP policy		
Sectors of critical importance	As per table above	
Number of national CI	N.A.	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Number of national CI operators	N.A.	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	The Netherlands shifted from a sector approach to CIP to a process approach; this is because certain processes are viewed as being critical for Dutch society. The failure or disruption of such processes would result in severe social disruption and poses a threat to national security. These processes together form the critical infrastructure of The Netherlands. The impact of incidents involving critical infrastructure, the speed of technological developments, the change in threats and cyber threats and the increasing mutual interdependence of critical infrastructure necessitates a permanent focus on increasing and safeguarding its resilience.	Website - <i>Critical Infrastructure (Protection). National coordinator for Security and Counterterrorism, Dutch Ministry of Justice and Security:</i>
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	Primary responsibility for the continuity and resilience of critical processes is borne by the actual operators of critical processes. This includes gaining an insight into threats, vulnerabilities and risks, and developing and maintaining capacities that increase and safeguard the resilience of critical processes. The responsible ministry establishes general frameworks for the sectors that fall under its responsibility (in policy or in laws and regulations). The ministries, in association with the operators of critical processes, are responsible for safeguarding and inspecting capabilities related to critical infrastructure.	Website - <i>Critical Infrastructure (Protection). National coordinator for Security and Counterterrorism, Dutch Ministry of Justice and Security:</i>
Coordination of ministries, bodies and offices concerned	The fact that there are many, diverse stakeholders necessitates coordination and management. The National Coordinator for Security and Counterterrorism (NCTV) of the Ministry of Justice and Security is responsible for this management and ensures cohesion of resilience-increasing measures with and for all parties.	Website - <i>Critical Infrastructure (Protection). National coordinator for Security and Counterterrorism, Dutch Ministry of Justice and Security:</i>
Communication with owners/operators	Approximately 80% of critical processes are in the hands of private parties. Public private partnership is necessary to achieve supported policy. The critical infrastructure policy is shaped as much as possible in association with the operators of critical processes, knowledge institutes and the government.	Website - <i>Critical Infrastructure (Protection). National coordinator for Security and Counterterrorism, Dutch Ministry of Justice and Security:</i>
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	N.A.	
Other relevant aspects of national authorities involved in CIP protection		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Same as ECI	
- Preparation of a security plan	Same as ECI	
- Review of the plan (timing)	Same as ECI	
- Reporting incidents	Same as ECI	
- Exchange of information	Same as ECI	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Integrated approach for critical infrastructure protection was established in May 2015 as part of the National Safety and Security Strategy, developed by the Dutch Ministry for Security and Justice. The approach contains three steps.</p> <ul style="list-style-type: none"> - First, the approach identifies what is critical infrastructure, based on economic, physical and social impact criteria. Criteria were developed based on the National Risk Assessment process. The degree of criticality depends upon the consequences of a failure of the critical sectors identified. A distinction is made between category A where disruptions can have large impacts and cascading effects and category B where impacts can be lower, in order to reflect the diversity within critical infrastructure and to set priorities. - Secondly, a vulnerability assessment provides insight into the most important risks, threats, vulnerabilities and degree of resilience of this infrastructure. - The third step of the approach is to make agreements on maintaining or, where needed, increasing the resilience of the vital infrastructure. This enables a customised approach for resilience enhancement, based on risks, threats and vulnerabilities. 	<p>Website - <i>Critical Infrastructure (Protection). National coordinator for Security and Counterterrorism, Dutch Ministry of Justice and Security:</i></p>

Poland

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	ACT of 26 April 2007 on Crisis Management <i>Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans</i> <i>Regulation of the Council of Ministers of 30 April 2010 on National Critical Infrastructure Protection Programme</i>	
Definitions (Art 2)		
'critical infrastructure'	<p>"Critical infrastructure": should be understood as systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance to the security of the state and its citizens as well as serving to ensure the efficient functioning of public administration authorities, institutions and enterprises.</p> <p>Critical infrastructure includes the following systems:</p> <ul style="list-style-type: none"> • Energy, fuel and energy resources supply systems, • Communications, • Tele-information networks, • Financial, • Food supply, • Water supply, • Health protection, • Transport, • Rescue, • Ensuring the continuity of public administration activities, • Production, storage, storage and use of chemical and radioactive substances, including pipelines of dangerous substances 	<i>Act of 26 April 2007 on Crisis Management (article 3.2)</i>
'European critical infrastructure'	<p>"European Critical Infrastructure": understood as systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance to the security of the state and its citizens as well as serving to ensure the efficient functioning of public administration authorities, institutions and enterprises—which work in the field of ECI. To be more specific, the main fields are electricity, oil and gas and road, rail, air, inland waterways, ocean shipping, short sea shipping and ports, located in the territory of the European Union. Furthermore, to be considered a European Critical Infrastructure the disruption or destruction has to impact at least two Member State</p>	Act of 26 April 2007 on Crisis Management (article 3.2a)
'risk analysis'	<p>"Risk analysis": concerning risk analysis, the law describes the following definitions:</p> <ul style="list-style-type: none"> • security matrix shall be understood as a set of potential risks with an identification of the lead entity for their removal as well as cooperating entities; 	Act of 26 April 2007 on Crisis Management (article 3.9, 3.10, 3.11)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<ul style="list-style-type: none"> • map of threats shall be understood as a map showing the geographical area covered by the threat's scope and including various scenarios of events; • Risk map shall be understood as a map or description showing potential negative consequences of the threat's impact on people, the environment, property and infrastructure. 	
'sensitive critical infrastructure protection related information'	Confidential information protection regulations shall be applied to the Programme.	Act of 26 April 2007 on Crisis Management (article 5b.6)
'protection'	"Protection of critical infrastructure" : shall be understood as all steps aimed at ensuring the functionality, continuity and integrity of critical infrastructure in order to prevent threats, risks or vulnerabilities as well as limiting and neutralising their effects and quick reconstructing the infrastructure in case of failures, attacks and other events disrupting its appropriate functioning	<i>Act of 26 April 2007 on Crisis Management (article 3.3)</i>
'owners/operators of ECI'	"Owners/operators of ECI" : the owner and independent or dependent holder of sites, installations, equipment and services of the critical infrastructure	Regulation of the Council of Ministers of 30 April 2010 on National Critical Infrastructure Protection Programme (§1)
Other relevant national definitions	"civil planning" : shall be understood as: <ul style="list-style-type: none"> • overall organisational projects aimed at preparing the public administration to manage crisis; • planning within the scope of support for the Armed Forces of the Republic of Poland in the case of their use and planning the use of the Armed Forces of the Republic of Poland for conducting crisis management tasks. Civil planning tasks shall include: <ul style="list-style-type: none"> • working out the solutions in the event of destruction or disruption of critical infrastructure • ensuring the functioning and ability of reconstructing critical infrastructure. 	Act of 26 April 2007 on Crisis Management (article 3.4 and 4)
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	The procedures apply to the energy sector (Sub-sectors: Electricity, Oil, Gas)	<i>Act of 26 April 2007 on Crisis Management (article 6a and 6b)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The Director of the Government Centre for Security, in collaboration with the ministers and heads of central offices shall identify, on an ongoing basis, the potential ECI.	<i>Act of 26 April 2007 on Crisis Management (article 6a)</i>
Application of the procedure for the identification of ECI (as per Annex III)	The Director of the Government Centre for Security follows the identification procedure described below	<i>Act of 26 April 2007 on Crisis Management (article 6a)</i>
<i>Step1 – Application of sectoral criteria</i>	Application of sectoral criteria - the approximate thresholds identified both by the European Commission and the EU Member States which determine characteristic parameters or functions of the potential ECI.	<i>Act of 26 April 2007 on Crisis Management (article 6a)</i>
<i>Step 2 – Application of the definition of critical infrastructure</i>	Analysis aimed at understanding whether the potential ECI constitutes an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, security, protection, economic or social well-being of people, and whose disruption or destruction would have a significant impact on the Republic of Poland as a result of the failure to maintain the above functions.	<i>Act of 26 April 2007 on Crisis Management (article 6a)</i>
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	Assessment on whether the disruption or destruction of the potential ECI would have a significant impact on at least two Member States of the European Union	<i>Act of 26 April 2007 on Crisis Management (article 6a)</i>
<i>Step 4 – Application of the cross-cutting criteria</i>	Application of cross-cutting criteria – within the scope of the approximate thresholds identified by the European Commission and the Member States of the European Union, including: <ul style="list-style-type: none"> • Casualties criterion - assessed in terms of the potential number of fatalities or injuries; • An economic effects criterion - assessed in terms of the significance of economic loss and/or degradation of the quality of products or services; including potential environmental effects; • A public effects criterion – assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services. 	<i>Act of 26 April 2007 on Crisis Management (article 6a)</i>
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	The approximate thresholds are identified by the European Commission and the Member States of the European Union. Thresholds are ECI-specific, as they are the product of negotiation with MS, and are not publicly divulged.	<i>Act of 26 April 2007 on Crisis Management (article 6a)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Identification of potential ECI on an ongoing basis (Art 3.1)	A formalised timing to reconsider CI and identify other ECI is not provided in national regulations. This is an ongoing process done with collaborations with the ministers, heads of central offices and operators if applicable.	
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	Based on the results of the discussions (among the Director of the Government Centre for Security and the competent authorities of the Member States of the European Union) within the scope of potential ECI located on the territory of the Republic of Poland, the Council of Ministers shall designate, by resolution, the ECI.	<i>Act of 26 April 2007 on Crisis Management (article 6b)</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	The relevant authorities of the European Union Member States shall be informed by the Director of the Government Centre for Security about the potential European critical infrastructure which can significantly affect those Member States. The Director of the Government Centre for Security shall provide the name and the location of the potential European critical infrastructure as well as the reasons for its designation.	<i>Act of 26 April 2007 on Crisis Management (article 6b)</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	In order to designate the European critical infrastructure as well as the exact thresholds of the criteria the Director of the Government Centre for Security shall conduct discussions with the competent authorities of the Member States of the European Union: 1) on which the ECI located on the territory of the Republic of Poland could have a significant impact; 2) on whose territory the potential ECI is located that could significantly affect the Republic of Poland. It is not specified how the negotiation takes place and what channels and tools are used.	Act of 26 April 2007 on Crisis Management (article 6b)
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	In order to designate the European critical infrastructure as well as the exact thresholds of the criteria the Director of the Government Centre for Security shall conduct discussions with the competent authorities of the Member States of the European Union: 1) on which the ECI located on the territory of the Republic of Poland could have a significant impact; 2) on whose territory the potential ECI is located that could significantly affect the Republic of Poland. It is not specified how the negotiation takes place and what channels and tools are used.	<i>Act of 26 April 2007 on Crisis Management (article 6b)</i>
Agreement for the designation of the ECI (Art. 4.3)	It is not specified when the agreement is achieved	N/A
Communicating to the EC the number of designated ECI per sector and the number of MS	The Director of the Government Centre for Security shall provide with the European Commission: • each year with the information about the number of the critical infrastructures:	<i>Act of 26 April 2007 on Crisis Management (Article 6c)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
dependent on each designation (Art 4.4)	<ul style="list-style-type: none"> ○ In respect of which discussions have been conducted with the competent authorities of the Member States of the European Union. The above mentioned talks concern the thresholds of the cross-cutting criteria allowing the designation of the European critical infrastructure located on the territory of the Republic of Poland. ○ Concerning ECI located on the territory of the Republic of Poland that belong to the European critical infrastructure in the individual sectors, as well as about the number of Member States of the European Union affected by the abovementioned European critical infrastructure. 	
Informing the owner/operator of the designated ECI (Art. 4.5)	The Director of the Government Centre for Security shall inform owners and operators of designated ECI.	<i>Act of 26 April 2007 on Crisis Management (Article 5b Paragraph 4)</i>
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The owner is responsible for updating and creating the OSP. The OSP has to be signed by the "Voivodes" (Province) and the competent minister or the head of the central offices responsible for the sector of the ECI. The Voivodes have 14 days to sign the plan, while the responsible minister has 45 days for signing it. Following these steps, the plan has to be sent to the Government Centre for Security and the director of the Government Centre for Security has 90 days to sign the plan.	<i>REGULATION OF THE COUNCIL OF MINISTERS OF 30 APRIL 2010 ON CRITICAL INFRASTRUCTURE PROTECTION PLANS(Article 4)</i>
Verification that the OSP or equivalent is in place	The plans are updated depending on the needs, and at least once every two years. Furthermore, in the in the Act of 26 April 2007 on Crisis Management (Article 6) it is specified that the Council of Ministers shall determine, by means of a regulation, the conditions and procedures for ensure that the OSP in in place, taking into account a need to ensure the continuity of functioning of critical infrastructure	
Verification that the OSP or equivalent is appropriately and regularly reviewed	Plans are being filed to GCS for approval.	
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	<p>SLO is designated by the CI operator on GCS request.</p> <p>ECI owners and operators are required to appoint within 30 days of receipt of the information a person (or persons) responsible for maintaining contacts with entities competent for critical infrastructure protection.</p>	<i>Act of 26 April 2007 on Crisis Management (Article 6 Paragraph 5a)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Function of the SLO (Art. 6.1)	A person (persons) responsible for contacts with entities entrusted with critical infrastructure protection should receive/provide information about threats to given CI and have technical means to fulfil this task 24 hours a day. He/she should also have a widest possible knowledge about the critical infrastructure and its functioning	The National Critical infrastructure Programme Page 15
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	On-going information share and collaboration.	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)		
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	The Director of the Government Centre for Security	Act of 26 April 2007 on Crisis Management (Article 6c)
Performance of threat assessments within ECI subsector within one year following the designation of ECI	The information is classified.	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The Director of the Government Centre for Security shall report every two years to the Commission generic data on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated on the territory of the Republic of Poland. The information/content is classified.	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The Government Centre for Security is the contact point act as the national contact point with the European Union and NATO institutions and Member States in the field of critical infrastructure Protection. The EPCIP contact point is being designated by the Head of the GCS.	Act of 26 April 2007 on Crisis Management (Article 11 Paragraph 2.11)
MS body(-ies) serving as ECIP contact point		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<p>The measures implemented for protecting the CI:</p> <ul style="list-style-type: none"> National Crisis Management Plan as well as voivodeship (Province), powiat (sub-Province) and gmina (Municipality) crisis management plans which includes a description of threats and risk assessment of their occurrence, including those relating to critical infrastructure, risk maps and maps of threats. The Council of Ministers shall adopt, by a resolution, the National Critical Infrastructure Protection Programme, hereinafter referred to as 'the Programme' which aims at creating conditions for improving the security of critical infrastructure. owners and owners of independent and dependent critical infrastructure prepares and creating a critical infrastructure plan 	<p><i>Act of 26 April 2007 on Crisis Management (Article 5a-5b-6) and REGULATION OF THE COUNCIL OF MINISTERS OF 30 APRIL 2010 ON CRITICAL INFRASTRUCTURE PROTECTION PLANS (Article 1)</i></p>
Scope of national CIP policy		
Sectors of critical importance	Not listed.	N/A
Number of national CI	ca. 550 The list of national CI is classified	N/A
Number of national CI operators	There are 128 CI operators	N/A
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	<p>The bodies involved for the protection of CI are as follow:</p> <p>The Council of Ministers</p> <ul style="list-style-type: none"> Adopts, by a resolution, the National Critical Infrastructure Protection Programme, which aims at creating conditions for improving the security of critical infrastructure <p>The principal responsibility of the centre are explained as follow:</p> <ul style="list-style-type: none"> Prepares a list of objects, installations, facilities and services included in the critical infrastructure divided into systems Prepares detailed ways and measures of reacting to threats and limiting their results, Develops and updates of the National Crisis Management Plan in co-operation with the relevant organisational units of offices serving ministers and heads of central offices, Analysis and assessment of possible occurrence and development of threats, Monitoring of potential threats; Planning and programming critical infrastructure and European critical infrastructure protection tasks <p>The Ministries heading government administration departments and heads of central offices</p>	<p><i>Act of 26 April 2007 on Crisis Management (Article 11, 12, 14)</i></p> <p>and The national Critical infrastructure programme pag.15-17, 22-24</p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> Shall prepare the National crisis management plans, the plans shall be agreed on with the Director of the Centre Carrying out the periodic risk assessment Issuing opinions on National crisis management draft plans, <p>Voivode</p> <ul style="list-style-type: none"> Managing the monitoring, planning, response and removal of the results of the threats on the territory of the voivodeship; Collecting and processing the data as well as assessing the threats that occur in the voivodeship; Prepare a voivodeship crisis management plan Organising the implementation of critical infrastructure protection tasks; Organising the implementation of critical infrastructure protection tasks; developing the voivode's recommendations to poviats crisis management plans based on the analysis of threats in poviats <p>Poviats</p> <ul style="list-style-type: none"> Preparation of the poviats crisis management plan and its submission to the voivode for approval Approval of the gmina crisis management plan <p>The authority competent for crisis management issues on the territory of the gmina shall be the vojt (administrative officer of the municipality), mayor, or president of the city. Tasks include:</p> <ul style="list-style-type: none"> implementation of recommendations to the gmina crisis management plan; managing the monitoring, planning, response and removal of the threats on the territory of the gmina; <p>Special forces</p> <p>Serve a specific role in CI protection. They have developed forces and means at their disposal, aimed at the identification of threats caused by international activities of people. Exchange of information about such threats with CI operators and other entities competent in the matters of CI protection in a manner specified by the provisions of law and internal procedures, within the scope permitted under the provisions on classified information protection, is of key importance in the process of planning CI protection. A special role is allocated to the Internal Security Agency. According to Art. 12a of the Act of 26 April 2007 on Crisis Management, the Head of ISA, in the event of gaining access to information about a possibility of a crisis situation occurrence which is a consequence of an event of a terroristic nature, threatening the critical infrastructure, life or health of people, property of a significant value, national heritage or environment, may give instructions to authorities and entities threatened by such activities and provide them with necessary information aimed at prevention of threats. The Head of ISA informs the director of GCS of the above actions and supports public administration authorities in performing activities connected with prevention,</p>	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>counteracting and remedy of consequences of events of a terroristic nature. Public administration authorities are obliged to immediately provide the Head of the Internal Security Agency with information which is in their possession and which concerns threats to critical infrastructure of a terrorist nature.</p> <p>CI operators have the best knowledge and conditions to limit threats to CI, reduce its vulnerability to such threats and choose the most suitable strategy of their minimisation. They are obliged to:</p> <ul style="list-style-type: none"> • prepare and implement, based on the anticipated threats, plans for critical infrastructure protection and maintenance of their own reserve systems ensuring the security and maintaining the functioning of that infrastructure until the time of its full reconstruction, • appoint a person responsible for contacting entities entrusted with critical infrastructure protection, • immediately provide the Head of the Internal Security Agency with information concerning threats to critical infrastructure of a terrorist nature, • co-operate in the process of creation and implementation of the Programme. <p>CI operators also participate in the activities for the protection of CI through:</p> <ul style="list-style-type: none"> • active co-operation with public administration (at all levels) and other CI operators, • support of public administration (at all levels) with their expert knowledge concerning the functioning of CI in the planning process in case of a crisis situation, • exchange of information about threats with other CI operators, • improvement of skills and abilities of reaction in crisis situations, including proper education and organisation of personnel training, • provision of public administration and other CI operators with knowledge about dependencies and interdependencies between their own CI and the CI functioning in other sectors of economy, • identification of the best practices and standards which may help in the protection of CI, • share in promotion of educational programmes and training in the area of CI protection, • participation in training concerning crisis management and CI protection. 	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	The government centre for security, the Ministries heading government administration departments and heads of central offices, the voivode and the Poviats are responsible thought the national, voivodeship, poviats and gmina management plan for identifying the threats and the vulnerabilities	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Coordination of ministries, bodies and offices concerned	See the paragraph above	
Communication with owners/operators	<p>N/A</p> <p>The functionally-configured information exchange in the field of critical infrastructure take place in the following three areas:</p> <ol style="list-style-type: none"> 1) forum of critical infrastructure protection 2) on-going information exchange by means of direct contacts between the parties (mechanism of CI protection), 3) joint training, conferences, advisory services and organisation of practical exercises <p>Information exchange take place in a number of ways:</p> <p>through crisis management centres operating 24 hours a day and on-duty forces, within the crisis management system,</p> <p>ongoing, direct contacts between representatives of the parties, exchange of classified and unclassified information in a traditional manner and with the use of electronic systems of exchange of classified and unclassified information, periodic, joint meetings within the framework of critical infrastructure</p> <p>protection forums: a joint Internet platform established especially for the purpose of information exchange, presentation of experiences and knowledge in the area of CIP, co-operation within the forum, organisation of meetings, training, etc.</p>	The National Critical infrastructure Programme Page 32-33
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	<p>The voivode constitutes a point of transfer between the system and territorial perception of tasks in the area of critical infrastructure protection, while the services, forces and inspections subordinate to heads of provinces constitute an important element of planning in the event of interference with the functioning of CI located in the territory of the province. In view of the above, heads of provinces, trying to achieve the Programme goals, perform, for instance, the following tasks:</p> <ul style="list-style-type: none"> • organisation and service of a regional CI protection forum and taking part in the mechanism of CI protection within the scope described in the Programme, • participation in the process of evaluation of a crisis situation occurrence risk in the state, caused by the destruction of or interference with the functioning of the CI 	The national Critical infrastructure programme pag. 23

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>located in the territory of the province, by preparation and update of the "Partial report on threats to the state security",</p> <ul style="list-style-type: none"> co-operation with the provincial, county and commune self-governments in the implementation of tasks falling within the scope of crisis management and civil planning, based on the competence of the provincial self-government, co-operation with CI operators and relevant entities in matters concerning CI protection and support of activities aimed at the achievement of the Programme goals. 	
Other relevant aspects of national authorities involved in CIP protection	N/A	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	As described in the table above	<i>(Security Liaison Officer Art. 6)</i>
- Preparation of a security plan	As described in the table above	
- Review of the plan (timing)	As described in the table above	
- Reporting incidents	As described above	<i>The National Critical infrastructure Programme Page 16-17</i>
- Exchange of information	<p>Co-operation in the CI area means exchange of any information which may affect the achievement of the Programme goals and maintenance of regular contacts with the CI protection process participants.</p> <ul style="list-style-type: none"> The functionally-configured information exchange in the field of critical infrastructure will take place in the following three areas: forum of critical infrastructure protection on-going information exchange by means of direct contacts between the parties (mechanism of CI protection), joint training, conferences, advisory services and organisation of practical exercises. <p>The parties to the aforementioned information exchange will be CI operators and public administration. Experts may be invited to co-operation, representing various fields of science and practice, whose knowledge may constitute an added value within the framework of fulfilment of tasks connected with CIP.</p> <p>Information exchange will take place in a number of ways, through:</p>	<i>The national Critical infrastructure programme Pag 32</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> • crisis management centres operating 24 hours a day and on-duty forces, within the crisis management system, • on-going, direct contacts between representatives of the parties, • exchange of classified and unclassified information in a traditional manner and with the use of electronic systems of exchange of classified and unclassified information, • periodic, joint meetings within the framework of critical infrastructure protection forums, • a joint Internet platform established especially for the purpose of information exchange, presentation of experiences and knowledge in the area of CIP, co-operation within the forum, organisation of meetings, training, etc. 	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Cybersecurity</p> <p>The National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022 is a strategic document in a continued process of actions taken by the governmental administration, aimed at raising the level of cybersecurity in the Republic of Poland, including the Policy for the Protection of Cyberspace of the Republic of Poland adopted by the government in 2013.</p> <p>The National Framework of Cybersecurity Policy identifies, in particular:</p> <ul style="list-style-type: none"> • the ICT security objectives, • the main actors involved in the implementation of the national framework • of cybersecurity policy, • management framework for achieving the objectives of the national framework • of cybersecurity policy, • the need to prevent and respond to incidents and to restore services to normal after an incident, including the principles of co-operation between public and private sectors, • the approach to risk assessment, • educational, information and training programmes related to cybersecurity, • activities related to research and development plans in the field of ICT security, • directions of international co-operation in the area of cybersecurity. 	<p>NATIONAL FRAMEWORK OF CYBERSECURITY POLICY OF THE REPUBLIC OF POLAND Pag 6</p>

Portugal

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	Decreto-Lei n.º 62/2011 de 9 de Maio.	Diário da República n.º 89/2011, Série I de 2011-05-09
Definitions (Art 2)		
'critical infrastructure'	'Critical infrastructure' means a component, system or part thereof located in national territory which is essential for the maintenance of functions vital to society, health, safety and economic or social well-being, and whose disruption or destruction would have a significant impact given the impossibility of continuing to secure those functions;	Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 2)
'European critical infrastructure'	'European Critical Infrastructure' or 'ECI' means the critical infrastructure located in national territory whose disruption or destruction would have a significant impact on at least one other Member State of the European Union, the impact being assessed on the basis of cross-cutting dependencies in relation to other types of infrastructure.	
'risk analysis'	n.a.	
'sensitive critical infrastructure protection related information'	n.a.	
'protection'	n.a.	
'owners/operators of ECI'	n.a.	
Other relevant national definitions	n.a.	
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Energy <ul style="list-style-type: none">electricity production, transmission and distribution infrastructures and installations;infrastructures for the production, refining, treatment, storage and transport of oil by oil pipelines; andinfrastructures for the production, refining, treatment, storage and transportation of gas through natural gas pipelines and terminals Transportation <ul style="list-style-type: none">Road transport;	Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 3)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<ul style="list-style-type: none"> • Rail transport; • Air transport; • Inland waterways transport; • Maritime transport, including short-haul shipping and ports 	
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	It was the responsibility of the <i>Conselho Nacional de Planeamento Civil de Emergência (CNPCE)</i> to identify potential ECI that simultaneously meet both cross-cutting and sectoral criteria. Note that the functions of CNPCE were later transferred to ANPC (Autoridade Nacional de Proteção Civil, National Authority for Civil Protection), in 2012	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 4)</i>
Application of the procedure for the identification of ECI (as per Annex III)	The identification of potential ECI is made through the application of a procedure consisting of four phases. Potential ECI that do not meet the requirements of any of the stages of the procedure provided for in this article are not considered ECI.	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 4)</i>
Step 1 – Application of sectoral criteria	In the first stage of the procedure for the identification of potential ECI, sectoral criteria are applied to make a first selection of critical infrastructures within a given sector.	
Step 2 – Application of the definition of critical infrastructure	In the second stage of the identification procedure, the definition of critical infrastructure (see list of definitions) shall be applied to potential ECI. The significant impact shall be determined using national methods for identifying critical infrastructures and using cross-cutting criteria.	
Step 3 – Application of the transboundary element of the definition of ECI	In the third stage of the identification procedure, the transboundary element in the definition of ECI (see list of definitions) shall be applied to potential ECI which have completed the first two stages of the procedure.	
Step 4 – Application of the cross-cutting criteria	In the fourth stage of the identification procedure, the cross-cutting criteria are applied to potential ECI.	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	It was the responsibility of CNPCE to identify potential ECI that simultaneously meet both cross-cutting and sectoral criteria. These functions were later migrated to ANPC.	
Identification of potential ECI on an ongoing basis (Art 3.1)	n/a	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	The CNPCE and, from 2012 on, it became a responsibility of ANPC	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 6)</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	The CNPCE (now the ANPC) informs the Member States of the European Union: (a) of which ECI identified in accordance with Articles 4 and 5 which are likely to affect those States significantly; (b) the reasons for its designation as ECI.	
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	n/a	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	The competent authorities, if they consider that there is reason to believe that the Portuguese State may be significantly affected by a potential ECI not identified as such by another MS in whose territory it is situated, may initiate the process of communication to the EC so that bilateral or multilateral discussions on the identification and designation of such infrastructure as ECI.	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 9)</i>
Agreement for the designation of the ECI (Art. 4.3)	The potential ECI should be designated as such by the CNPCE, now by the ANPC, after obtaining agreement with the responsible entities of the Member States of the European Union that can be significantly affected by it.	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The CNPCE, now the ANPC, shall annually inform the European Commission of the number of ECI designated in each sector and of the number of European Union Member States depending on each designated ECI.	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 8)</i>
Informing the owner/operator of the designated ECI (Art. 4.5)	The CNPCE, now the ANPC, informs the owner or operator of the infrastructure of its designation as ECI.	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 8)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly		<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 10)</i>
Verification that the OSP or equivalent is in place	The operator security plan (OSP) of each ECI shall be prepared and revised annually by the operators and submitted to the prior opinion of the territorially competent security force and the National Authority for Civil Protection with a view to the validation of OSPs by the Secretary General of the Internal Security System. The operator security plan is connected with the ECI’s security and external protection plan, which is a responsibility of the territorially competent security force and civil protection.	
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	Each ECI shall have a Security Liaison Officer (SLO) designated by the owner/operator	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 11)</i>
Function of the SLO (Art. 6.1)	SLOs act as the point of contact for security issues between the owner/operator of ECI and the Secretary General of the Internal Security System	
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	The owner/operator of the ECI notifies the Secretary General of the Internal Security System and ANPC, through an official letter, of the nominated SLO.	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	It is the responsibility of the SLOs to exchange the information regarding the risks and threats identified in relation to the ECI in question, without prejudice to the regime of state secrecy.	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 11)</i>
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	The Secretary General of the Internal Security System	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Performance of threat assessments within ECI subsector within one year following the designation of ECI	The Secretary General of the Internal Security System, in liaison with the relevant security forces and services, shall undertake an assessment of the threats to critical infrastructure sub-sectors one year after their designation as ECI.	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Article 12)</i>
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The Secretary General of the Internal Security System shall transmit to the European Commission a biennial summary of general data on the risks, threats and vulnerabilities of each identified ECI.	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	In the case of ANPC, the nomination of the Contact Point was made by the Secretary of State for Internal Affairs	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Art.15)</i>
MS body(-ies) serving as ECIP contact point	CNPCE, now ANPC, is the contact point for the European Commission for the protection of European Critical Infrastructures and specifically for the designation of ECI, as well as safety issues. The Secretary General for the Internal Security System is the contact point for the protection of European Critical Infrastructures, in terms of the security of ICEs.	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<p>The provisions of the Decreto-lei 62/2011, de 9 de Maio shall apply, with the exception of the stages corresponding to the transboundary element, to the other national critical infrastructures.</p> <p>The measures consist mainly of:</p> <ul style="list-style-type: none"> • the obligation of having an Operator Security Plan, to be elaborated by the operator. • the obligation of having an external security plan to be made by the local security force and civil protection. • Also some recommendations regarding the threat evaluation that should be done by public entities (intelligence bodies). 	<p><i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Art.17)</i></p> <p><i>Boas Práticas de Resiliência de Infraestruturas Críticas - SETOR</i></p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> In the scope of the International Strategy for Disaster Reduction (United Nations), under the Sendai Framework 2015-2030, where the resilience of CI is a key issue and one of Sendai targets, a book was published containing a set of measures and Good Practices to increase the resilience of CI. The book was elaborated by a set of important operators of the Private Sector and State-Owned Companies in the Country and ANPC, who published the book. In the scope of the national strategy for counterterrorism, action plans were developed defining measures to take in case of a terrorist attack to CI. 	<p>PRIVADO E SETOR EMPRESARIAL DO ESTADO – 2017</p> <p>(Good Practices for the Resilience of CI – Private Sector and State-owned Companies – 2017)</p>
Scope of national CIP policy		
Sectors of critical importance	Same as Directive	
Number of national CI	162	
Number of national CI operators	12	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy		
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	<p>The Internal Security System makes a threat assessment to the subsectors and critical Infrastructures</p> <p>Several studies have been and continue to be developed concerning risks bound to affect CI, namely natural, technological and cyber risk. These studies take place in collaboration with Universities. Also studies continue to be developed on the important issue of interdependencies.</p>	
Coordination of ministries, bodies and offices concerned	<ul style="list-style-type: none"> The ANPC which depends on the Ministry of Interior – does the coordination concerning safety and disaster risk reduction. ANPC is also responsible for managing any civil protection and emergency preparedness and response in the event of a disaster. The Internal Security System makes the overall coordination regarding security entities (Law enforcement and intelligence) 	Lei de Segurança Interna (Lei 53/2008, de 29 de Agosto)

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
		<i>Lei de Bases da Protecção Civil. Lei n.º 27/2006, de 3 de Julho (com as alterações introduzidas pela Declaração de Rectificação n.º 46/2006, de 28 de Julho)</i>
Communication with owners/operators	<ul style="list-style-type: none"> • The Internal Security System, for security related issues; • The ANPC, for safety issues and disaster risk reduction subjects. 	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Art.11)</i>
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	n/a	
Other relevant aspects of national authorities involved in CIP protection	There is still another national authority much involved in CIP: The National Centre for Cybersecurity, which has very important competences in what cybersecurity is concerned, including the cyber threat to CI. It is also the national authority on the area.	<i>Decreto Lei n.º 69/2014, de 9 de Maio</i>
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Each Operator must appoint a SLO	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Art.11)</i>
- Preparation of a security plan	Each CI must have a OSP	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Art.10)</i>
- Review of the plan (timing)	Every year	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
		<i>Lei n.º 62/2011 de 9 de Maio (Art.10)</i>
- Reporting incidents	n/a	
- Exchange of information	The SLO and the Secretary General for the Internal Security System shall change information related to threats and risks.	<i>Diário da República n.º 89/2011, Série I de 2011-05-09, Decreto-Lei n.º 62/2011 de 9 de Maio (Art.11)</i>
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>The approach used in Portugal is all-hazards.</p> <p>Measures are discussed between the national authorities, the sector regulators and the operators.</p> <p>As said before, the measures to increase protection and resilience of CI are developed in the scope of several frameworks, such as the UNISDR Sendai Framework, the national strategy for counterterrorism, the national strategy for cybersecurity, and the Counter Terrorism and Counter Radicalisation Strategy</p>	

Romania

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<p><i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures</i></p> <ul style="list-style-type: none"> • <i>Approved and modified by Law 18/2011</i> • <i>Also modified by: Law 344/2015 and Law 225/2018</i> 	<ul style="list-style-type: none"> - Official Monitor no. 757 from 12nd of November 2010 - Official Monitor no. 183 from 16th of March 2011 - Official Monitor no. 970 from 28th of December 2015 - Official Monitor no. 677 from 3rd of August 2018
Definitions (Art 2)		
'critical infrastructure'	"National Critical infrastructure" - infrastructures essential for maintaining the vital functions of society, health, safety, security, social or economic wellbeing of persons and whose disruption or destruction would have a significant impact at national level due to the inability to maintain those functions;	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, Art. 3</i>
'European critical infrastructure'	"European Critical Infrastructure" - a national critical infrastructure whose disruption or destruction would have a significant impact on at least two MS of the EU. The severity of the impact is assessed from the point of view of cross-cutting criteria. It includes the effects resulting from the intersectoral relationships of dependency on other types of infrastructure	
'risk analysis'	"risk analysis" - analysing significant threat scenarios to assess the vulnerability and potential impact of disruption or destruction of NCI / ECI	
'sensitive critical infrastructure protection related information'	"sensitive information on Critical Infrastructure Protection" - information on critical infrastructure that could be used in the event of disclosure for the purpose of planning and carrying out actions to disrupt or destroy facilities of critical infrastructure	
'protection'	"Critical Infrastructure Protection" (CIP) - any activity aimed at ensuring the functionality, continuity and integrity of NCI / ECI in order to discourage, diminish and neutralise a threat, risk or vulnerability. In a non-exhaustive enumeration, the CIP includes the sequential activities on risk assessment and analysis, the protection of classified information, the development of security plans for critical infrastructure operators, the establishment of liaison officers and the way communications are made, and exercises, reports, re-evaluations and updates of the documents prepared	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
'owners/operators of ECI'	"owners/operators/managers of NCI/ECI" - those entities responsible for investing in an element, system or component thereof, designated as NCI or ECI under this Emergency Ordinance, and/or their current operation / management	
Other relevant national definitions	<p>"essential services" - those services, facilities or activities that are or may be required to provide a minimum standard of living and welfare of society and whose degradation or interruption of their provision as a result of disruption or destruction of physical system base, would significantly affect the safety or security of the population and the functioning of state institutions.</p> <p>"Critical Infrastructure Alert Network" (CIWIN) - a secure information and communication system designed to assist national institutions and other Member States to exchange information on vulnerabilities, appropriate measures to reduce them and risk mitigation strategies;</p> <p>"Responsible public authorities" - a public institution designated under the terms of this Ordinance which, according to the competencies and legal attributions, is responsible for the organisation and conducting activities in the fields corresponding to the sectors and sub - sectors of the critical infrastructure listed in annex no. 1 and responsible for at least one ICN / ICE designated.</p> <p>"operator security plan (OSP)" - strategic planning document, operative through associated procedures, developed for each NCI / ECI designated for management risks to the ICN / ICE, which defines the purpose, objectives, requirements and measures their security;</p> <p>"resilience of NCI/ECI" - its ability to absorb initial shock, to adapt as a result of producing a hazard or threat and to recover for continuing to provide the essential services to the society;</p> <p>"vital functions" - those services that are essential to the operation of the company, such as: government affairs management, international activities, national defence, internal security, the functioning of the economy and infrastructure, the security of the population's income and living standards.</p>	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	<ul style="list-style-type: none"> - Energy sector <ul style="list-style-type: none"> a. Electricity b. Oil c. Gas - Transport sector <ul style="list-style-type: none"> a. Road transport b. Rail transport c. Air transport d. Inland waterway transport e. Short sea shipping and ports 	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2018 (Annex 1)</i>
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	<ul style="list-style-type: none"> - National Centre for Coordination of Critical Infrastructure Protection - The responsible authority (Ministry/Sectoral Agency) 	
Application of the procedure for the identification of ECI (as per Annex III)	In accordance with the following procedure (see steps below), The National Centre for Coordination of Critical Infrastructure Protection and the responsible public authorities identify potential ECI that meet sectoral and cross-cutting criteria, in accordance with the owners/operators/administrators	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010 and 2018, Art. 9 and ART. 6^2</i>
<i>Step1 – Application of sectoral criteria</i>	<p>Step 1 - the responsible public authority applies to the designated potential ECI, the sectoral criteria to make a first selection of ECI within a sector;</p> <p>The sectoral criteria and related critical thresholds, defined according to the severity of the impact of disruption or destruction of a particular infrastructure, shall be established by the responsible public authorities, according to the areas of responsibility.</p> <p>Thresholds for the energy sectors have been defined in Ministerial Order no. 1178/2011.</p> <p>Thresholds for the energy sectors have been defined in Ministerial Order no. 387/2011.</p>	<p><i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010 S, Art. 9(2); Annex I</i></p> <p>Ministerial Order 1178/2011 to establish sectoral criteria and critical thresholds for sector "Energetic"</p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		Ministerial Order 387/2011 to establish sectoral criteria and critical thresholds for sector "transport"
<i>Step 2 – Application of the definition of critical infrastructure</i>	<p>Step 2 - the responsible public authority apply the definition of ECI (see list of definition)</p> <p>The importance of the impact is determined either by using the national methods of identifying the ECI or by cross-cutting criteria at an appropriate national level. In the case of an infrastructure providing essential service, consideration shall be given to the availability of alternatives as well as to the duration of disturbance/re-entry into service;</p>	<p><i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010 S, Art. 9(2); Annex II</i></p>
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	<p>Step 3 - the responsible public authority apply the transboundary element of the definition of ECI. A potential ECI that meets the definition is subject of the next stage of the procedure.</p> <p>In the case of an infrastructure providing essential service, consideration shall be given to the availability of alternatives as well as to the duration of disturbance/re-entry into service;</p>	
<i>Step 4 – Application of the cross-cutting criteria</i>	<p>Step 4 - the responsible public authority apply cross-cutting criteria to the potential ECI selected. Within the cross-cutting criteria, account is taken of the severity of the impact and, in the case of infrastructure providing essential services, the availability of alternatives and the duration of disturbance / re-entry into service.</p>	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	<p>Critical thresholds for cross-cutting criteria are defined according to the gravity of the impact of disruption or destruction of a CI. They are established by a Government decision.</p>	<p><i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2018, 2010 (Article 9)</i></p> <p><i>Government decision no. 1.154 of November 16, 2011 to approve the critical thresholds for the cross-sectoral criteria underlying the identification of potential national critical</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		<i>infrastructures and the approval of the Methodology for the application of critical thresholds related to cross-sector criteria and the determination of the level of criticality.</i>
Identification of potential ECI on an ongoing basis (Art 3.1)	<p>The responsible public authorities, together with the EC and the responsible authorities of the other Member States, shall assess, on the basis of biennial reports, the need for additional protective measures for ECI.</p> <p>The lists of NCIs approved through Government decision are being reviewed annually.</p>	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010, Art. 6(6)</i>
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	<p>The responsible public authorities propose the designation of ECI for the sectors they are responsible for.</p> <p>Coordination at national level of identification, designation and protection activities is carried out by the Prime Minister, through the designated advisor.</p> <p>Responsibility for organising and carrying out the necessary activities for implementation the specific legislation of the critical infrastructure protection domain belongs to the Ministry of Internal Affairs through the National Critical Infrastructure Protection Coordination Centre.</p> <p>CNCPIC ensures strategic planning, coordination, and permanent monitoring and control over the implementation stage of the activities, the national contact point in relation to other Member States of the European Union, the Commission, The European Union, the North Atlantic Treaty Organisation and other organisations and bodies, as well as the management for the national section of The Critical Infrastructure Warning and Information Network (CIWIN).</p>	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010, 2018, (Article 4)</i>
Informing other MS which may be significantly affected of the identity and	The responsible public authorities (ministry of transport and the ministry of economy, chiefly and respectively for the transportation and energy sector) shall, at the request of National Centre for Coordination of Critical Infrastructure Protection, engage in bilateral and / or multilateral discussions	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
reasons for designating a potential ECI (Art. 4.1)	with the other Member States that may be significantly affected by a potential ECI located within the national territory or which may affect significantly in the case of potential ECI located in other Member States.	<i>protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018, (Article 10)</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	The responsible public authorities shall, at the request of the Ministry of Internal Affairs, through the National Centre for Coordination of Critical Infrastructures, engage in bilateral and / or multilateral discussions with the other Member States that may be significantly affected by a potential ECI located within the national territory or which may affect significantly in the case of potential ECI located in other Member States.	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018, (Article 10)</i>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	If the responsible public authorities have reason to believe that the national territory could be significantly affected by a potential ECI located in another Member State but not identified as such by the Member State on whose territory it is located finds the potential ECI, informs the Prime Minister, through the State Councillor. Following its decision, the National Centre for Coordination of Critical Infrastructures informs the EC of Romania's intention to participate in bilateral and / or multilateral discussions on this issue with a view to requesting the Member State in whose territory the infrastructure is located be designated as ECI.	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 (Article 10 (5))</i>
Agreement for the designation of the ECI (Art. 4.3)	The designation of ECI is based on the written consent of the authorities competent in Romania and the Member States that could be significantly affected by the acceptance the Member State in whose territory the infrastructure to be designated as ICE is located, and is approved by Government Decision. Law 344/2015 specify that the designation of ECI is based on the written consent of the authorities competent in Romania and the Member States instead of designating through an agreement between Romania and the Member States . The term "agreement" has a more complex meaning in national legislation and it was making the designation process more bureaucratic.	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 (Article 10 (6))</i>
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The Minister of Internal Affairs, through the National Centre for Coordination of Critical Infrastructures, shall provide the EC with yearly information on the number of infrastructures per sector that have been designated on the thresholds of cross-sectoral criteria.	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		344/2015 and Law 225/2018, 2010,2018 (Article 6 (4))
Informing the owner/operator of the designated ECI (Art. 4.5)	The responsible public authorities shall inform the owner / operator / manager of ECI of its designation as ECI within 10 days of the entry into force of the designating act.	EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 (Article 10 (8))
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	Responsible public authorities	
Verification that the OSP or equivalent is in place	The responsible public authorities shall ensure, within one year of designation in the sector the responsibility of an infrastructure as NCI / ECI, that there is an OSP or an equivalent of it. In the case of the ECI, the term may be extended only in exceptional circumstances, with the agreement of the Prime Minister and the notification of the European Commission in this respect by the Ministry of Internal affairs through the National Centre for Coordination of Critical Infrastructures. The OSP shall be evaluated, tested and, if necessary, reviewed and updated by the owner / operator / of NCI`s / ECI`s manager periodically at intervals of no more than two years. The minimum requirements are provided in the Annex 3 of the Emergency Ordinance 98/2010 while the structure framework of the OSP is detailed in the Prime Minister's Decision no. 166 of 19.03.2013.	EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 (Article 11)
Verification that the OSP or equivalent is appropriately and regularly reviewed		DECISION no. 166 of 19.03.2013 approving the methodological norms for the accomplishment / equivalence / revision of the security plans of the national / European critical infrastructure owners / operators / administrators, the security plan's structure framework of the owner / operator / administrator of the National / European Critical Infrastructure and the duties of the security liaison officer link within the specialised department designated at the level of the responsible public authorities and

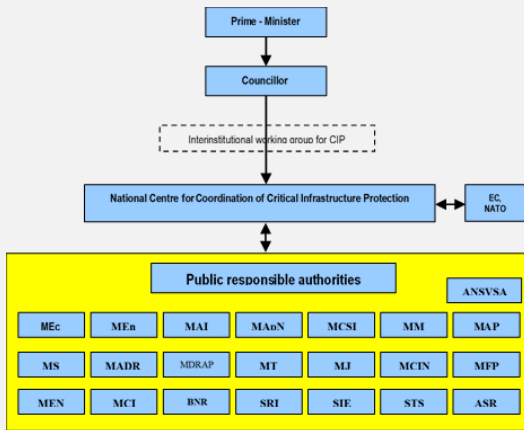
IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		<i>at the level of the owner / operator / national / European critical infrastructure manager</i>
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	<p>The responsible public authorities and each owner/operator / administrator designate, within their own structure, a specialised ECI compartment, which will also act as a contact point for issues related to critical infrastructure security between the owner / operator / administrator of ICN / ICE and the responsible public authorities.</p> <p>Each responsible public authority, as well as each owner / operator / administrator that have more than one NCI / ECI in their responsibility have an obligation to designate specialised structure / compartment that will also perform the role of a point of contact for security critical infrastructure issues between owners / operators / administrators and responsible public authorities.</p> <p>The structure / compartment is led by a liaison officer for security of NCI / ECI and is directly subordinated to the head of public authority responsible or the owner / operator / administrator of NCI / ECI.</p> <p>Within one year of the designation of an NCI / ECI, the responsible public authorities and owners / operators / administrators of NCIs / ECI have the obligation to ensure the training of the security liaison officer and the personnel designated to perform duties in CIP in the educational establishments for training and development professionally competent, under the law.</p> <p>NCI / ECI security liaison officers shall be evaluated and authorised periodically in the conditions established by the authorisation methodology approved by decision of the Prime Minister.</p>	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 (Article 8)</i>
Function of the SLO (Art. 6.1)	<p>SLOs act as contact point for issues related to ECI security.</p> <p>The responsible public authorities and owners / operators / administrators of NCIs / ECI who have under the responsibility of one NCI / ECI have the obligation to designate a security liaison officer that will also act as a contact point for issues related to security of critical infrastructure between owners / operators / administrators of NCIs / ECI and responsible public authorities.</p>	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	The main responsibilities of the SLO are provided in the Annex 2 and 3 of the Prime Minister's Decision no. 166 of 19.03.2013.	344/2015 and Law 225/2018, 2010,2018 (Article 8(2)) Prime Minister's Decision no. 166 of 19.03.2013
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	<p>The responsible public authorities and owners / operators / administrators of NCIs / ECI who have under the responsibility of one NCI / ECI have the obligation to designate a security liaison officer [...]</p> <p>M.A.I, through CNCPIC, ensures strategic planning, coordination, and permanent monitoring and control over the implementation stage of the activities regulated by this Emergency Ordinance no. 98 /2010.</p> <p>National Centre for Coordination of Critical Infrastructure Protection elaborates and proposes for approval, by decision of the Prime Minister, the Annual Plan of Verification of the state of implementation of CIP legislation by the responsible public authorities and owners / operators / administrators of NCIs / ECI;</p>	EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 (Article 8(2), article 4(3), Article. 6^1)
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	The responsible public authorities shall establish and implement an appropriate communication mechanism with the NCI / ECI Security Liaison Officers for the purpose of exchanging relevant data on identified risks and threats, while ensuring the security of sensitive information related to the protection of critical infrastructure, in accordance with the current regulations on access to classified information.	EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 (Article 8(4))
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	<p>Ministry of Internal Affairs, through The National Centre for Coordination of Critical Infrastructure Protection, submits to the European Commission, every two years, a summary report containing general information on types of risks, threats and vulnerabilities identified in each sector, where an ECI has been approved, and which are located on the national territory.</p> <p>Ministry of internal affairs, through National Centre for Coordination of Critical Infrastructure Protection, submits to the European Commission annual information on the number of infrastructure sectors that were subject to debates on the threshold of cross-cutting criteria.</p>	EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 (Article 6 (3) (4), (5))

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	This report shall be analysed within the inter-institutional working group for CIP, classified according to the information contained, according to the national law on classified information and forwarded to the European Commission under the signature of the Prime Minister.	
Performance of threat assessments within ECI subsector within one year following the designation of ECI	<p>The responsible public authorities shall, together with the owners / operators/managers, carry out an assessment of the risks and threats of the ECI subsectors within one year of the designation of critical infrastructure as ECI.</p> <p>The evaluation shall also include proposals on the need to improve the protection of the ECI and shall be submitted for approval to the Prime Minister. Subsequently, the evaluation is carried out annually.</p>	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 (Article 6(1))</i>
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The National Centre for Coordination of Critical Infrastructure Protection shall forward to the EC every two years a synthesis report with general data on the types of risks, threats and vulnerabilities identified in each of the sectors where an ECI was identified.	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 Art. 6 (3)</i>
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	National Centre for Coordination of Critical Infrastructure Protection ensures strategic planning, coordination, and permanent monitoring and control over the implementation stage of the activities, the national contact point in relation to other Member States of the European Union, the Commission, The European Union, the North Atlantic Treaty Organisation and other organisations and bodies, as well as the management for the national section of The Critical Infrastructure Warning and Information Network (CIWIN).	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 Art. 4 (3)</i>
MS body(-ies) serving as ECIP contact point	The EC will be immediately informed by The National Centre for Coordination of Critical Infrastructure Protection on the measures taken to transpose the provisions of the Directive,	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	Same as Directive	
Scope of national CIP policy		
Sectors of critical importance	<ul style="list-style-type: none"> • Energy sector <ul style="list-style-type: none"> a. Electricity, including nuclear energy b. Petroleum and petroleum derivative c. Natural gas and derivative d. Mineral resources • ICT sector <ul style="list-style-type: none"> a. Communication systems, networks and services b. Data processing, storage systems, including electronic public services c. Computer Security Infrastructure d. Communication systems and networks for the state cipher e. Radio-TV broadcasting infrastructures f. Postal services • Water, environment and forests <ul style="list-style-type: none"> a. Provision of drinking water and sewage; b. Qualitative and quantitative water control; c. Environment protection; d. Protection of the forest and hunting ground • Food <ul style="list-style-type: none"> a. Production and supply of food, ensuring food safety and security • Health <ul style="list-style-type: none"> a. Medical and hospital care b. Medicines, serums, vaccines, pharmaceuticals c. Bio-laboratories and bio-agents d. Medical emergency and health services • National security <ul style="list-style-type: none"> a. Defence of the country, public order and national security b. Integrated system for state border security c. Defence industry, production capacities and storage facilities d. Emergency situations e. Justice and prisons • Administration <ul style="list-style-type: none"> a. Services and administration • Transport <ul style="list-style-type: none"> a. Road transport b. Rail transport 	<i>EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018 Annex 1</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> c. Air transport d. Shipping • Industry <ul style="list-style-type: none"> a. Production, processing, storage and use of chemical substance and nuclear and radioactive materials b. Product/Dangerous Chemicals Pipes • Space and research <ul style="list-style-type: none"> a. Cosmic space b. Research • Finance and banks <ul style="list-style-type: none"> a. Taxes and fees b. Insurance c. Banks d. Stock Exchange e. Treasury and payment systems • Culture and national cultural heritage <ul style="list-style-type: none"> a. Public cultural institutions b. Protecting national cultural heritage. 	
Number of national CI	Sensitive information	
Number of national CI operators	Sensitive information	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	<p>The strategy aim is to provide the general framework for the critical infrastructure protection in order to promote national interests and to achieve the objectives assumed in the alliance to which Romania is a party.</p> <p>The strategy aims to:</p> <ul style="list-style-type: none"> a) establish the markers for national capacity continuous development of critical infrastructure protection; b) harmonise the national legislation with the European Union and NATO's legislation in the field; c) involve all national authorities in the field, as well as private sector partners, to formulate and implement all of the structural and procedural measures to ensure a coordinated action at national level for the identification, designation and critical infrastructures protection. <p>Strategic objectives:</p>	<i>HGR no. 718 of 13 July 2011 for the approval of the National Strategy on Critical Infrastructure Protection</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ol style="list-style-type: none"> 1. Ensuring consistency of the identification, designation and protection of national and European critical infrastructures; 2. Setting up and the operationalisation of a national early warning system by integrating all the networks and the existing organisational-informational capabilities; 3. Accurate the evaluation of the vulnerability level of critical infrastructure and identify the measures necessary to preventive intervention; 4. Develop the co-operation at national, regional and international level in the critical infrastructures field. 	
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	Annually, the National Centre for Coordination of Critical Infrastructure Protection with the support of the public authorities represented in The inter-institutional working group for CIP is developing The Risks, Threats and Vulnerabilities Report.	
Coordination of ministries, bodies and offices concerned	<p>The Romanian government founded the actual National Centre for Coordination of Critical Infrastructure Protection within Ministry of Internal Affairs in July 2010. Through Government Decision no. 1110 / 2010 it was set up The inter-institutional working group for CIP at the Government level, under the coordination of a councillor appointed by the Prime Minister.</p>  <pre> graph TD PM[Prime - Minister] --> C[Councillor] C --> IWG[Interinstitutional working group for CIP] IWG --> NCCIP[National Centre for Coordination of Critical Infrastructure Protection] NCCIP <--> ECNATO[EC, NATO] NCCIP <--> PRA[Public responsible authorities] subgraph PRA_Box [Public responsible authorities] direction TB Row1[MEc MEa MAI MAaN MCSI MM MAP] Row2[MS MADR MDRAP MT MJ MCIN MEP] Row3[MEN MCI BNR SRI SIE STS ASR] end ANSVSA[ANSVSA] </pre>	
Communication with owners/operators	Same as Directive	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	Coordination of activities at territorial level with operators / owners / administrators of NCIs / ECI is being done by the public responsible authorities.	
Other relevant aspects of national authorities involved in CIP protection		
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	<p>The responsible public authorities and each owner/operator are required to designate, within their own structure, a specialised NCI compartment, which will also act as a contact point for issues related to critical infrastructure security between the owner/operator of NCI and the responsible public authorities.</p> <p>Each responsible public authority shall ensure, within one year of the designation, that there is an OSP or equivalent and that they are periodically reviewed. The term may be extended in exceptional cases with the Prime Minister's agreement and the notification of the European Commission in this respect by the National Centre for Coordination of Critical Infrastructure Protection.</p> <p>Within one year of the designation of an NCI / ECI, the owners / operators / administrators of NCIs / ECI have the obligation to ensure the training of the security liaison officer and the personnel designated to perform duties in CIP in educational establishments for training and development professionally competent, under the law.</p> <p>NCI / ECI security liaison officers shall be evaluated and authorised periodically in the conditions established by the authorisation methodology approved by decision of the Prime Minister.</p>	EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018
- Preparation of a security plan	Each responsible public authority shall, within one year after the designation in their sector of responsibility of an infrastructure as designated NCI / ECI, ensure that an OSP or its equivalent exists and that are reviewed periodically.	EMERGENCY ORDINANCE no. 98 from 3rd of November 2010 on the identification, designation and protection of critical infrastructures, approved by Law 18/2011 and modified by Law 344/2015 and Law 225/2018, 2010,2018
- Review of the plan (timing)		
- Reporting incidents	The incidents produced at the level of a NCI/ECI are being reported to public responsible authorities and the National Centre for Coordination of	PRIME MINISTERS DECISION no. 166 of 19.03.2013 approving the

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	Critical Infrastructure Protection using as a template the Annex 6 of the Annex 2 from the Prime-minister decision no. 166 / 2013.	<i>methodological norms for the accomplishment / equivalence / revision of the security plans of the national / European critical infrastructure owners / operators / administrators, the security plan's structure framework of the owner / operator / administrator of the National / European Critical Infrastructure and the duties of the security liaison officer link within the specialised department designated at the level of the responsible public authorities and at the level of the owner / operator / national / European critical infrastructure manager</i>
- Exchange of information	<p>A Critical Infrastructure Alert Network (CIWIN) is used for the exchange of information concerning critical infrastructures. It is a secure information and communication system designed to assist national institutions and other Member States to exchange information on vulnerabilities, appropriate measures to reduce them and risk mitigation strategies.</p> <p>The exchange of information is also being done through The Interinstitutional Working Group for CIP established through Government Decision.</p>	<i>GD no. 1.110 of 3 November 2010 on the composition, tasks and organisation of the Interinstitutional Working Group on Critical Infrastructure Protection</i>
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Approach: all hazards.</p> <p>Review of the strategy: there are steps made at the level of the CNCPIC to draft a new national strategy for CIP.</p> <p>Measures for business security: all the subsequent legislation of the national implementation act of the Directive and the technical methodologies (3 laws, 7 Government Decision, 12 ministerial orders, 10 prime-minister decisions).</p> <p>Channels used for information exchange: the mechanism established within The Interinstitutional Working Group for CIP, e-mail and correspondence.</p>	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	Cybersecurity measures: integrated into the concept of “all hazards” approach.	

Slovakia

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre</i> http://www.zakonypreludi.sk/zz/2011-45	
Definitions (Art 2)		
'critical infrastructure'	"Critical infrastructure" : the infrastructure is identified as critical when it operates in the sector of engineering construction, public service and IT systems. Furthermore, it is considered critical infrastructure when the disruption or destruction of it could have adverse consequences for the economic and social state functions and the quality of life of the population.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 2)</i>
'European critical infrastructure'	"European Critical Infrastructure" : it is defined as CI whose disruption or destruction would have serious adverse consequences to another Member State of the European Union.	
'risk analysis'	"Risk Analysis" : it is a document which includes an assessment of the threat and the vulnerabilities which could cause the disruption and the destruction of the CI.	
'sensitive critical infrastructure protection related information'	"Sensitive information" concerning critical infrastructure are non-public information whose disclosure could cause the disruption or destruction of a CI.	
'protection'	"Protection" : CI are considered protected when measures are put in place to ensure the functionality, the integrity and the continuity of a critical infrastructure's activity in order to prevent, avert or mitigate the threat, which could cause distortion or destruction.	
'owners/operators of ECI'	"owners/operators of ECI" : an entrepreneur or who owns a critical infrastructure, or an operator who operates the critical infrastructure	
Other relevant national definitions	"Critical Infrastructure Sector" : the sector of the CI, which may include one or more critical infrastructures subsectors. "Sectorial criteria" : a set of technical and functional criteria and the thresholds applied in order to determine the presence of CI in one sector. "Cross-cutting criteria" : a set of criteria, which impact more than one sector and with given thresholds, which serve to identify the critical infrastructures. "European sectoral criteria" : a set of technical and functional criteria, which are used to determine the ECI on the basis of given thresholds. "European cross-cutting criteria" : a set of criteria with thresholds applied across the board to identify ECI.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Transport Air transport Energy Electricity Gas Oil and petroleum products	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Annex 3)</i>
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The body involved in the identification of ECI is the Ministry of interior, and in particular the Department of Civil Protection and Crisis Planning. They are supported in this activity by the sectorally-competent ministry. The Ministry of the interior (Department of Civil Protection and Crisis Planning), together with the responsible ministry (Ministry of Economy of the Slovak Republic, The Office of the Deputy Prime Minister for Investments and Informatisation, the Ministry of Transport and Construction of the Slovak Republic, the Ministry of the Environment of the Slovak Republic and the Ministry of Health of the Slovak Republic) and the competent Ministry of the other Member State are responsible for the ECI identification process. The Ministry of the interior may ask assistance to European Commission for determining the potential ECI.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 5)</i>
Application of the procedure for the identification of ECI (as per Annex III)	The procedures for identifying the ECI is conducted in four stages (see below):	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Annex 1)</i>
<i>Step1 – Application of sectoral criteria</i>	First stage: Sectorial criteria are applied for identifying the CI. If the CI meets the sectorial criteria, it is possible to proceed to the second stage.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Annex 1)</i>
<i>Step 2 – Application of the definition of critical infrastructure</i>	Second stage Cross-cutting criteria are applied to the CI that were approved in the first stage. If the CI meets the cross cutting criteria, it possible to be proceed to the third stage.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Annex 1)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	Third stage After the second stage, the transboundary element / European criteria are applied to identify potential ECI. Bilateral/multilateral negotiations.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Annex 1)</i>
<i>Step 4 – Application of the cross-cutting criteria</i>	Fourth stage From the potential ECI that passed third stage, the European cross cutting criteria are applied. If the ECI meets at least one European cross cutting criteria can be considered as ECI.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Annex 1)</i>
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	<i>It is not specified how the cross-cutting criteria thresholds are defined in practice.</i>	
Identification of potential ECI on an ongoing basis (Art 3.1)	The Central Critical Infrastructure authority has to reassess the CI on ongoing basis according to the sectoral criteria and cross-cutting criteria. Furthermore, The Central Critical Infrastructure has to reassess CI according to the European sectoral criteria and the European cross-cutting criteria.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 6)</i>
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	The Ministry of Interior, in particular Department of Civil Protection and Crisis Planning, together with the sectorally-competent ministry responsible and the relevant authority of the other Member State determine the European Critical Infrastructures	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 5)</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	Ministry of Interior (Department of Civil Protection and Crisis Planning) informs the involved Member States concerning the identification of potential ECI.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 6-Paragraph i)</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	<i>The authority responsible for discussing with the ministries of the other Member States is the Ministry of the Interior, in particular the Department of Civil Protection and Crisis Planning.</i> <i>The specific methods for negotiations are not specified.</i>	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 5)</i>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	<i>The Ministry of Interior can request to the European Commission to facilitate dialogue/negotiations between the Republic of Slovakia and another Member States where there could be an ECI that could have an impact the Republic of Slovakia.</i> <i>The particular channel used by the Ministry of Interior for communicating with the European Commission is not specified.</i>	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 5)</i>
Agreement for the designation of the ECI (Art. 4.3)	<i>It is not specified when the agreement can be considered achieved</i>	<i>N/a</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	<p>The Ministry of Interior and in particular the Department of Civil Protection and Crisis Planning communicates to the EC the number of ECI and the number of the Member States impacted by the ECI.</p> <p>The specific channel is not indicated in the legislation.</p>	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 5)</i>
Informing the owner/operator of the designated ECI (Art. 4.5)	<p>For each sector, the competent Central Critical Infrastructure Authority has to communicate to the operator when the ECI is designed.</p> <p>The channel used for communicating the designated ECI to the operator is not specified.</p>	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 6)</i>
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	For each, sector, the competent Central Critical Infrastructure Authority should verify if the OSP is in place.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article -6)</i>
Verification that the OSP or equivalent is in place	It is specified that the operator reviews the OSP on a rolling basis and, if necessary, updates the OSP, after prior notification by the relevant central authority	
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	<p>The operator has to designate a contact person for each ECI.</p> <p>Furthermore, article 6 specifies that the Central CI Authorities competent for each sector approves the SLO.</p>	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article6-9)</i>
Function of the SLO (Art. 6.1)	SLO shall ensure contacts between the operator of the ECI, the relevant central authorities and the Ministry of Interior, and in particular concerning the exchange of information on the threat of disturbance or destruction.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 11)</i>
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	It is not specified how the methodology for verifying if the SLO is in place. However, the law specifies that the SLO must be a natural person who has not been legally convicted of an offense, or is not considered to be operating in good faith. Integrity is evidenced by an extract from the criminal record not older than three months.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 11)</i>
Establishment of an appropriate communication mechanism between the	It is not specified if there is a communication system between the relevant Member State authority and SLO.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
relevant Member State authority and the SLO (Art. 6.4)		
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	The MS body responsible for fulfilling reporting obligation is the Ministry of Interior, and in particular the Department of Civil Protection and Crisis Planning	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 5)</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	The main contents of the threat assessment are not specified.	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The Ministry of the interior and in particular the Department of Civil Protection and Crisis Planning reports once every two years to the EC on the risks, threats and vulnerabilities in sectors where there is the European Critical Infrastructure. The content to be included in the summary is not specified.	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	It is not specified how the appointment the contact point took place.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 5)</i>
MS body(-ies) serving as ECIP contact point	The contact point is the Ministry of Interior and in particular Department of Civil Protection and Crisis Planning	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<p>The key measures that the Slovak Government implemented for guaranteeing protection are the following:</p> <p>National Program for Protection and Defence of the Critical Infrastructure in the Slovak Republic the programs underlined the following point:</p> <ul style="list-style-type: none"> ○ drawing up of Schedule of fulfilment of measures for protection of critical infrastructure in the Slovak Republic after adoption of Act on Critical Infrastructure ○ creation of interdepartmental program for securing of financial implementation of measures for protection of critical infrastructure in the Slovak Republic after the adoption 	Transport Critical Infrastructure in Slovak Republic

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> establishment of national guarantor for field of protection and defence of critical infrastructure in the period to 31st August 2008. The Ministry of Interior became the guarantor. 	
Scope of national CIP policy		
Sectors of critical importance	The National Program identified and elaborated in detail 8 basic sectors and 14 subsectors of the critical infrastructure (National program, 2008). The main sectors are listed in the table above.	Transport Critical Infrastructure in Slovak Republic
Number of national CI	N/A	
Number of national CI operators	N/A	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	Slovak Republic, as a part of NATO, pays permanent attention to the questions related to critical infrastructure and its protection. Until 2008, the legislation was only focused on the defence infrastructure. The Republic of Slovak created in 2008 the National Program for Protection and Defence of the Critical Infrastructure in the Slovak Republic in order to evaluate the current state and identify the most important infrastructure together with establishment of program steps for increasing of quality of the CI protection and defence. Subsequently, the Slovak Republic adopted legal standards (Law 45/2011) and measures leading to fostering the management of CI and securing the desired level of its security and protection.	Transport Critical Infrastructure in Slovak Republic
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	<p>Based on the law the threat and the vulnerabilities are indicated within the OSP.</p> <p>The operator has to practice at least every three years, according to the security plan, the model situation of threat of disruption or destruction of the element,</p>	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 9)</i>
Coordination of ministries, bodies and offices concerned	<p>In this sections it is described the main bodies responsible for identifying and controlling the CI</p> <p>The bodies responsible for defining CI are:</p> <ul style="list-style-type: none"> Government of Republic of Slovakia Ministry of the interior Sectorally competent Central Critical Infrastructure Authority <p>The Government of Slovakia:</p>	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Articles 4-5-6)</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> Decides to determine the Critical Infrastructure and its inclusion in the sector, as well as to remove the element from the sector. Approve the critical infrastructure concept in which it identifies the objectives, priorities and roles for the relevant period, as well as the ways in which they are implemented <p>The Ministry of the interior:</p> <ul style="list-style-type: none"> Develop, in co-operation with: <ul style="list-style-type: none"> The Ministry of Economy of the Slovak Republic; The Office of the Deputy Prime Minister for Investments and Informatisation The Ministry of Transport and Construction of the Slovak Republic, The Ministry of the Environment of the Slovak Republic The Ministry of Health of the Slovak Republic, A draft Critical Infrastructure Plan and send it to the Government Draw up, in co-operation with the ministers listed above, the draft cross-cutting criteria and European cross-cutting criteria Submit to the Government a proposal for sectoral criteria and European sectoral criteria Submit to the Government a proposal to identify the element and its inclusion in the sector, as well as a proposal to eliminate the element from the sector <p>Sectorally Competent Central Critical Infrastructure Authority</p> <ul style="list-style-type: none"> Prepare a proposal for the determination of the plan and its inclusion in the sector as well as a proposal for the elimination of the sector Verify the that the OSP is in place ensure its regular update; notify the Ministry of the extension of the deadline for the implementation of the OSP 	
Communication with owners/operators	The Sectorally Competent Central Critical Infrastructure Authority is responsible for communicating with the operator.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 6)</i>
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	The Ministry of the interior controls, in co-operation with the sectorally competent CI central authority, the performance of the operator's ECI obligations.	<i>Zákon č. 45/2011 Z. z. o kritickej infraštruktúre (Article 5)</i>
Other relevant aspects of national authorities involved in CIP protection	N/A	
Responsibilities allocated to operators of national CI		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
- Appointment of a security officer	Procedure described in the table above.	
- Preparation of a security plan	The review of OSP is described in the table above.	
- Review of the plan (timing)	It is not specified in the law.	
- Reporting incidents	<p>The operator is obliged to have or to provide the means, devices and tools necessary for the early recognition of emergencies, alerts and warnings, notification and convening of the relevant bodies, for dealing with serious industrial accidents and limiting their consequences. The Ministry shall keep a register of serious industrial accidents, containing brief data on major accidents:</p> <ul style="list-style-type: none"> • The date, business, place of occurrence of a major industrial accident, • The type of major industrial accident, its description, the type of hazardous substance present, • The extent and duration of a major industrial accident and how it is managed, • The source and principal cause of the occurrence of a major industrial accident, • The consequences of a major industrial accident on the life and health of people, the environment and property, • Measures taken <ul style="list-style-type: none"> ○ to limit or eliminate the consequences of a major industrial accident, ○ to prevent the recurrence of similar major industrial accidents. 	o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov (Article 20-and Article25)
- Exchange of information	N/A	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Cybersecurity</p> <p>On 17 June 2015, the Government of the Slovak Republic approved, by its Resolution no. 328/2015, the Cyber Security Concept of the Slovak Republic for years 2015-2020, aimed at proposing a new institutional framework of cyber security management in the Slovak Republic. This was made in response to the draft Directive of the European Parliament and of the Council on measures providing high joint level of network and information systems</p>	http://www.nbusr.sk/en/cyber-security/national-cyber-security-strategy/index.html

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	security in the Union and on identification of relevant national authorities for network and information system security.	

Slovenia

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Uredba o evropski kritični infrastrukturi</i> (<i>Decree on European Critical Infrastructures</i>)	<i>Uradni list RS; 35/2011;</i> <i>Publication date: 13/05/2011</i>
Definitions (Art 2)		
'critical infrastructure'	"Critical infrastructure" of national importance includes those facilities which are of key importance for the state and would have a significant impact on the disruption or destruction of their operation or serious consequences for national security, economy, basic social functions, health, safety and security and social well-being, estimated according to criteria determined by the Government of the Republic of Slovenia;	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 2</i>
'European critical infrastructure'	"European critical infrastructure (ECI)" means a critical infrastructure located in Member States and whose failure or destruction would have serious consequences assessed by cross-sectoral criteria in at least two Member States;	
'risk analysis'	"risk analysis" means addressing the relevant hazard scenarios in order to assess vulnerabilities and the possible consequences of failure or destruction of critical infrastructure;	
'sensitive critical infrastructure protection related information'	"sensitive critical infrastructure protection related information" shall be ECI data, the disclosure of which could be used to plan and implement activities in order to cause damage or destruction of ECI devices and systems;	
'protection'	"protection" means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructure operations in order to prevent, mitigate and neutralise threat, risks and vulnerability;	
'owners/operators of ECI'	"owners/operators of ECI" means public bodies, companies, institutions and other organisations responsible for investments in infrastructure capacity, system or part thereof designated as ECI under this Regulation or responsible for the operation of these capacity, system or part thereof;	
Other relevant national definitions	"Preparatory authorities" are national authorities that, together with owners and operators, plan preparations and measures to protect the ECI.	
Scope (Art 3.3)		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<p>Sectors and sub-sectors in scope:</p> <ul style="list-style-type: none"> - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports) 	<ul style="list-style-type: none"> - Energy sector Electricity Oil Gas - Transport sector Road transport Rail transport Air transport Inland waterway transport Short-haul transport and short sea shipping and ports 	<p><i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Annex I</i></p>
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	An interdepartmental coordination group is appointed by the Government of the Republic of Slovenia. It is composed by representatives from the ministries responsible for the economy, transport, agriculture, forestry and food, environment and space, health, internal affairs and defence, and government services, but also economic interest groups. The Interdepartmental coordination group is headed by a representative from the Ministry of Defence. Administrative and technical tasks for the interdepartmental coordination group are carried out by the Ministry of Defence.	<p><i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 8</i></p>
Application of the procedure for the identification of ECI (as per Annex III)	The Interdepartmental Coordination Group, at the proposal of the ministries responsible for energy or transport, or other ministries, identifies a potential ECI that meets the cross-cutting and sectoral criteria established by the Regulation and meets the ECI definition	<p><i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 3</i></p>
<i>Step1 – Application of sectoral criteria</i>	Step 1 - This step identifies the potential ECI in the Republic of Slovenia in accordance with the definition of ECI (see above). For the first selection of critical infrastructure in the Republic of Slovenia sectoral criteria are used.	<p><i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Annex II</i></p>
<i>Step 2 – Application of the definition of critical infrastructure</i>	<p>Step 2 - With regard to the potential ECI set out in step 1, the critical infrastructure definition (see list of definitions) shall be taken into account. The basis for the identification of a potential ECI is the sectoral criteria for the transport and energy sectors, which form part of the Commission's non-binding guidelines for the implementation of Directive 2008/114 / EC and are applied directly.</p> <p>The criteria are of a secret nature and are drawn up in a separate document. The severity of the consequences shall be determined using national methods for determining critical infrastructure or in terms of cross-cutting criteria. The infrastructure providing the basic service also takes into account the</p>	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	availability of alternatives and the duration of the failure or recovery, in the event of damage to the infrastructure.	
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	<p>Step 3 - For the potential ECI that has undergone the first two steps of this procedure, an element of transboundary implications is assessed.</p> <p>A bilateral or multilateral dialogue with Member States is established, which could be affected by the failure or destruction of a critical infrastructure. Together with such a Member State or Member States, the severity of the impact and consequences resulting from the failure of the critical infrastructure shall be checked. For the infrastructure providing the basic service, the availability of alternatives and the duration of the failure or restoration are also considered. The potential ECI, which corresponds to these estimates, is dealt with in the next step of the procedure.</p>	
<i>Step 4 – Application of the cross-cutting criteria</i>	<p>Step 4 - For the remaining potential ECI, the cross-cutting criteria are applied. The cross-cutting criteria include effects in terms of the number of victims, economic and other losses, and public consequences or effects, and also take into account the severity of the impact, the availability of alternative options for infrastructure, which provides the basic service and the duration of the failure or recovery. The cross-cutting criteria and approximate thresholds form part of the Commission's non-binding guidelines for the implementation of Directive 2008/114 / EC and are applied directly. The criteria are of a secret nature and are set out in a separate document. A potential ECI that does not meet cross-cutting criteria is not considered as an ECI and the evaluation process is completed. A potential ECI that has been the subject of the Critical Infrastructure Determination procedure shall be notified only to Member States for which this ECI could have serious consequences.</p>	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	The thresholds for cross-cutting criteria are formed on the basis of the severity of the consequences of the failure or destruction of each infrastructure. Powers for cross-cutting criteria are determined by the Government of the Republic of Slovenia at the proposal of the inter-ministerial coordination group on a case-by-case basis, at the initiative of the ministries responsible for energy and transport, or other ministries, in co-operation with the owners and managers of the ECI.	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 3</i>
Identification of potential ECI on an ongoing basis (Art 3.1)	The process of identifying a potential European critical infrastructure (ECI) is carried out as a continuous process, but at least once a year or whenever the cross-cutting or sectoral criteria are changed.	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 3.3</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	ECI shall be designated by the Government of the Republic of Slovenia on the proposal of the Interdepartmental coordination group. The interdepartmental coordination group formulates proposals in agreement with the ministries responsible for energy or transport, or other ministries.	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 4</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	If there is a potential ECI in the Republic of Slovenia, a bilateral or multilateral dialogue with other Member States for which a potential ECI could have serious consequences is established. A bilateral or multilateral dialogue with other Member States is maintained by the contact point for the protection of ECI in co-operation with the interdepartmental coordination group.	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 4</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	Introductory discussions in the form of talks at bilateral meetings were held between the contact points of the neighbouring Member States and representatives from the competent ministries as holders of the critical infrastructure sectors. Bilateral meetings were held with each Member State once. In the continuation of the process of identifying a potentially ECI regarding the identification the ECI the official letters were exchanged between the neighbouring Member States.	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	The Ministry of Defence is responsible for communication, whose representative is appointed by the Government of the Republic of Slovenia as a contact point for the protection of European Critical infrastructure. So far, there has been no need for the European Commission to participate in a dialogue with neighbouring Member States. In case of need, they would use e-mail and/or the CIWIN application.	
Agreement for the designation of the ECI (Art. 4.3)	In the territory of the Republic of Slovenia, the ECI shall be determined on the basis of an agreement concluded between the Republic of Slovenia and those Member States that could suffer serious consequences from the disruption of this ECI. The agreement with other Member States, concluded in accordance with the law governing foreign affairs, shall also regulate the manner of exchanging classified information and other sensitive information concerning ECI and other issues.	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 4</i>
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The ECI Protection Contact Point shall inform the Commission annually of the number of designated ECI in each sector and the number of Member States affected by a particular ECI.	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 9</i>
Informing the owner/operator of the designated ECI (Art. 4.5)	The owner or operator of the ECI shall be informed by a decision of the Government of the Republic of Slovenia	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 4</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The supervision of the preparation, acceptance and updating of OSP and the implementation of measures from security plans or equivalent measures for the protection of ECI shall be carried out in accordance with their respective competences by the Inspectorate of the Republic of Slovenia for Energy, the Inspectorate of the Republic of Slovenia for the Interior, the Inspectorate of the Republic of Slovenia for natural and other disasters, the Inspectorate of the Republic of Slovenia for Defence and the Ministry of Transport. During the preparation of the OSP, assets of the ECI shall be identified and the safety measures that exist or are implemented to protect these assets and which ensure the smooth functioning of the ECI are determined.	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 5</i>
Verification that the OSP or equivalent is in place		<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 5</i>
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The competent ministries work with a contact person for co-operation in the area of critical infrastructure, which the Critical Infrastructure Operators are obliged to determine.	<i>Act on Critical Infrastructure, Official Gazette of the Republic of Slovenia, no.75/2017; Publication date: 22/12/2017 (Zakon o kritični infrastrukturi; Uradni list RS; 75/2017); Article 18 and Article 19/2</i>
Function of the SLO (Art. 6.1)	Similar tasks as the Security Liaison Officer in accordance with Directive 2008/114 has a contact person for co-operation with Critical Infrastructure Operators, other holders of Critical Infrastructure sectors and the Ministry of Defence as stated in the Act on Critical Infrastructure.	<i>Uredba o evropski kritični infrastrukturi; Uradni list RS; 35/2011; Article 6</i> <i>Zakon o kritični infrastrukturi, Uradni list RS; 75/2017; Article 2/1, 18/1 and Article 15</i>
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	The responsibility of competent ministries as holders of critical infrastructure sectors that direct and offer expert assistance to critical infrastructure operators in their planning of critical infrastructure protection.	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	In addition to CIWIN, a network of the National Crisis Management Centre has been set up in Slovenia for national CI, which includes ministries and certain critical infrastructure operators. Activities are currently underway to include the remaining Critical Infrastructure operators in the network. The network also allows the exchange of classified information and sensitive information.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	Persons working in the field of critical infrastructure and its protection in ministries and in critical infrastructure operators have access to the network.	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	The Ministry of Defence is responsible for reporting to the European Commission as a contact point for the protection of European critical infrastructure in the Republic of Slovenia. The reports are always coordinated with the competent ministries in advance.	
Performance of threat assessments within ECI subsector within one year following the designation of ECI	Within one year of determining the critical infrastructure in the Republic of Slovenia for the ECI Ministry responsible for energy and transport, it shall carry out a risk analysis in accordance with this Regulation unless the risk analysis is carried out already under the sectoral regulations governing a particular type of ECI.	<i>Uredba o evropski kritični infrastrukturi;Uradni list RS; 35/2011; Article 4</i>
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The ECI Protection Contact Point shall send the Commission every two years a summary of general information on the types of risks, threats and vulnerabilities identified for ECI in the Republic of Slovenia. The summary shall be sent on a single form to be determined by the Commission.	<i>Uredba o evropski kritični infrastrukturi;Uradni list RS; 35/2011; Article 9</i>
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The tasks of the contact point for the protection of ECI in the Republic of Slovenia are performed by the Ministry of Defence or another body appointed by the Government of the Republic of Slovenia. The Point of Contact for the Protection of European Critical Infrastructure in the Republic of Slovenia was appointed by the Government of the Republic of Slovenia with the Decision on the appointment of the Interdepartmental Coordination Group for the Protection of Critical Infrastructure (Government of the Republic of Slovenia, no. 01203-17/2012/3 dated 27.9.2012, 01203-6/2014/3 dated 24.7.2014, 01203-10 / 2015/3 dated 29. 4. 2015 and 01203-10/2015/7 dated 9.6. 2016.	<i>Uredba o evropski kritični infrastrukturi;Uradni list RS; 35/2011; Article 7</i>
MS body(-ies) serving as ECIP contact point	The Ministry of Defence/ Defence affairs Directorate	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<i>Zakon o kritični infrastrukturi (ZKI), stran 11338</i>	<i>Act on Critical Infrastructure; Official Gazette of the Republic of</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<i>Act on Critical Infrastructure</i>	<i>Slovenia, no.75/2017 of 22December2017; Article 13</i>
Scope of national CIP policy		
Sectors of critical importance	<p>The critical infrastructure sectors are:</p> <ul style="list-style-type: none"> • the energy sector; • the transport sector; • the food sector • the water supply sector; • the health sector; • the finance sector; • the environmental protection sector; and • the information and communications networks and systems sector 	<i>Act on Critical Infrastructure; Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 4(1)</i>
Number of national CI	A Critical Infrastructure of national importance in the Republic of Slovenia was determined by the Government of the Republic of Slovenia with a decision in 2014, The number of national critical infrastructure is 63. Currently, the new Decision on the designation of national critical infrastructure, which will be determined on the basis of the Critical Infrastructure Act, is in the process of adoption. The number of designated critical infrastructures and its operators will not significantly deviate from the existing one.	
Number of national CI operators	The number of a national critical infrastructure operators of is 50.	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	The critical infrastructure of the Republic of Slovenia includes those facilities that are of key importance for the country and would have a significant impact on the disruption or destruction of their operation and would have serious consequences for national security, the economy and other key social functions and health, safety, security and human well-being. The protection of critical infrastructure is an activity undertaken to ensure the continuity of critical infrastructure operations.	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 3</i>
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	The design of critical infrastructure protection involves assessing the risks to the operation of critical infrastructure and the design of measures to protect critical infrastructure. The assessment of the risks to the operation of critical infrastructure is the result of a comprehensive process of identifying, analysing and evaluating the various sources of risk for the operation of critical	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 3</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	infrastructure, which is carried out to provide a basis for the design of measures for the protection of critical infrastructure.	
Coordination of ministries, bodies and offices concerned	In accordance with Article 20 of the Critical Infrastructure Act, expert guidance and coordination in the area of critical infrastructure is carried out by the Ministry of Defence.	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 20</i>
Communication with owners/operators	The Ministry of Defence is a contact body for co-operation between holders of critical infrastructure sectors and participating state authorities and critical infrastructure operators. Holders of Critical Infrastructure Sectors and Critical Infrastructure operators have identified contact persons for mutual co-operation in the field of critical infrastructure.	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 18/2 and 19/2</i>
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	The inspectorate responsible for defence shall oversee the implementation of the provisions of the Act on Critical Infrastructure.	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 28</i>
Other relevant aspects of national authorities involved in CIP protection	In addition to the other tasks defined in the Critical Infrastructure Act, the Government, defines policy in this area and, if necessary, from holders of Critical Infrastructure sectors, Critical Infrastructure operators, Ministry of Defence and Defence Inspectors, requires additional reports on the implementation of tasks from their jurisdiction, which are not covered by Chapter 5 of the Act on Critical Infrastructure. National Crisis Management Centre collects information on contact persons and provides support for decision-making on the field of critical infrastructure.	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 17, 21 and 25</i>
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Critical Infrastructure Managers shall designate a contact person or more of such for co-operation with other holders of Critical Infrastructure sectors, Critical Infrastructure operators and the Ministry of Defence.	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 19/2</i>
- Preparation of a security plan	Critical Infrastructure operators shall develop and maintain Critical Infrastructure Protection Planning Documents. Critical Infrastructure Protection Planning Criteria include risk assessment and measures to protect critical infrastructure. On the proposal of the holders of Critical Infrastructure Sectors, Critical Infrastructure operators have, in accordance with the regulations governing private security, be designated as obligatory entities for the organisation of	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 11/1 in 2 in 13/6</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	security, which must implement critical infrastructure protection in accordance with these regulations. In this connection, they need to develop a security plan.	
- Review of the plan (timing)	Critical Infrastructure operators need to update their planning documents on a regular basis and at least once a year. When new circumstances arise which may have a significant impact on the operation of critical infrastructure, planning documents should be amended no later than a month. Such revised planning documents require the consent of the competent holder of the Critical Infrastructure Sector.	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 14</i>
- Reporting incidents	The Critical Infrastructure operator shall, as soon as possible, inform the holders of Critical Infrastructure Sector and the National centre for crisis management of the Critical Infrastructure Cause Suspension, which it deems to have potential material and other consequences for the Critical Infrastructure Sector, and the Critical Infrastructure Protection Measures already undertaken. Holders of Critical Infrastructure Sector, based on the Annual Reports of Critical Infrastructure operators to ensure the continuity of Critical Infrastructure Performance for the previous year, which they draw up by the end of February, have to prepare an annual report on ensuring the critical operation of the critical infrastructure for the Critical Infrastructure sector under its jurisdiction and by the end of April shall submit to the Ministry of Defence, which have to prepare a joint annual report on the provision of continuous operation of the critical infrastructure of the Republic of Slovenia and submit it to the Government by the end of May for the previous year.	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 23 and 24</i>
- Exchange of information	CIWIN (Critical infrastructure warning information network) is a protected internet portal designed for publication of research works, analyses and studies, and for facilitating exchange of information and views of the expert public about critical infrastructure in the EU Slovenia has established a network of the National Crisis Management Centre to support decision-making in the area of national critical infrastructure, but not all Critical Infrastructure operators are included yet.	<i>Official Gazette of the Republic of Slovenia, no.75/2017 of 22December2017; Article 21</i>
Other distinctive features of the national CIP framework		
- Approach (sectoral, all-hazards) - Review of the strategy (timing)	Cybersecurity measures: Slovenia adopted a Cybersecurity strategy in February 2016. It was established that critical infrastructure of ICT support	Zakon o informacijski varnosti (Act on information security)

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
<ul style="list-style-type: none"> - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>sector should be designed and managed to provide systemic ICT support at various levels. Rapid and efficient mechanisms for responding to threats and debugging, i.e. resolving damage resulting from security incidents, and preventive mechanisms that as far as possible prevent such threats and errors, was established.</p> <p>Slovenia has adopted the Act on Information Security, which is published in the Official Gazette of the Republic of Slovenia, no. 30/2018, which transposed the Directive (EU) 2016/1148 / EC into the Slovenian legal order. The law in the third paragraph of Article 6 stipulates that critical infrastructure operators shall also be designated as performers of essential services, determined on the basis of the Critical Infrastructure Act. At the moment, the Decree on the Determination of Essential Services and a more detailed methodology for determining the providers of essential services, in accordance with the Law on Information Security, is in preparation.</p>	<p><i>Official Gazette of the Republic of Slovenia, no.30/2018 of 26 April 2018; Article 6 and 7/4</i></p>

Spain

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<ul style="list-style-type: none"> Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. <p>(GENERAL PROVISIONS: With regard to horizontal regulations, the links established with Laws 8/2011, of 28 April, establishing measures for the protection of critical infrastructures, and 36/2015, of 28 September, on National Security, and with Royal Decree 3/2010, of 8 January, regulating the National Security Scheme in the field of Electronic Administration, as special regulations on the security of public sector information systems).</p>	Transposition into Spanish law of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of networks and information systems in the Union .
Definitions (Art 2)		
'critical infrastructure'	"Critical Infrastructure" : strategic infrastructures whose operation is essential and does not allow alternative solutions, so that their disruption or destruction would have a serious impact on essential services.	<ul style="list-style-type: none"> Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información.(Art 3)
'European critical infrastructure'	"European Critical Infrastructures" : those critical infrastructures located in a Member State of the European Union, whose disruption or destruction would seriously affect at least two Member States, all in accordance with Directive 2008/114, of the Council, of 8 December 2008, on the identification and designation of European Critical Infrastructures and the evaluation of the need to improve their protection.	
'risk analysis'	<p>"Risk Analysis": the study of possible threat scenarios necessary to determine and evaluate the existing vulnerabilities in the different strategic sectors and the possible repercussions of the disruption or destruction of the infrastructures that support it.</p> <p>"Risk" (scope Real Decreto-ley 12/2018): any reasonably identifiable circumstance or fact that has a possible adverse effect on the security of networks and information systems. It can be quantified as the probability of materialisation of a threat that produces an impact in terms of operability, physical integrity of people or material or image.</p>	
'sensitive critical infrastructure protection related information'	"Sensitive critical infrastructure protection related information" : the specific data on strategic infrastructures that, if disclosed, could be used to plan and carry out actions whose objective is to cause the disturbance or destruction of these.	
'protection'	"Protection of critical infrastructures" : the set of activities designed to ensure the functionality, continuity and integrity of critical infrastructures in order to prevent, mitigate and neutralise the damage caused by a deliberate attack against such	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>infrastructures and to guarantee the integration of these actions with others that come from other Plan for the Protection of Critical Infrastructures, in accordance with the general assessment of the threat and with the specific assessment that is made in each case on each infrastructure, in virtue of which it will correspond to declare a concrete degree of intervention of the different organisms responsible in matter of security.</p> <p>Security of networks and information systems (scope Real Decreto-ley 12/2018): the ability of networks and information systems to withstand, with a given level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or the corresponding services offered by or accessible through such networks and information systems.</p>	
'owners/operators of ECI'	<p>"owners/operators of ECI": the entities or bodies responsible for the investments or the daily operation of an installation, network, system, or physical or information technology equipment designated as critical infrastructure in accordance with this Law.</p> <p>Critical operator: the entities or bodies responsible for the investments or for the daily functioning of an installation, network, system, or physical or IT equipment classified as critical infrastructure pursuant to this Law.</p> <p>Operator of essential services (scope Real Decreto-ley 12/2018): a public or private entity that is identified considering the factors established in article 6 of this royal decree law, which provides such services in one of the strategic sectors defined in the annex to Law 8/2011, of 28 April.</p>	
Other relevant national definitions	<ul style="list-style-type: none"> - "Essential service": a service necessary for the maintenance of basic social functions, health, safety, social and economic welfare of citizens, or the effective functioning of State Institutions and Public Administrations. - "Essential service" (scope Real Decreto-ley 12/2018): service necessary for the maintenance of basic social functions, health, safety, social and economic welfare of citizens, or the effective functioning of State Institutions and Public Administrations, which depends for its provision of networks and information systems. - Digital service (scope Real Decreto-ley 12/2018): information society service within the meaning of letter a) of the annex to Law 34/2002, of 11 July, on information society services and electronic commerce - Digital service provider (scope Real Decreto-ley 12/2018): a legal person providing a digital service. - "Strategic sector": each one of the areas within the labour, economic and productive activities which provides an essential service or that guarantees the exercise of the authority of the State or of the security of the country. - "Strategic sub-sector": each one of the areas in which the different strategic sectors are divided, at the proposal of the affected Ministries and agencies, and 	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>the technical document that is approved by the National Centre for the Protection of Critical Infrastructures.</p> <ul style="list-style-type: none"> - "Strategic infrastructures": facilities, networks, systems and physical equipment and information technology on which the operation of essential services rests. - "Critical zone": the continuous geographical area where several critical infrastructures are established by different and interdependent operators, which is declared as such by the competent Authority. The declaration of a critical zone will aim to facilitate better protection and greater coordination between the different operators of critical infrastructures or ECI located in a small geographical area. - "Criticality criteria": the parameters according to which the criticality, severity and consequences of the disturbance or destruction of a critical infrastructure are determined will be evaluated according to: <ul style="list-style-type: none"> o The number of people affected, valued according to the potential number of fatalities or injuries with serious injuries and the consequences for public health o The economic impact in terms of the magnitude of economic losses and the deterioration of products and services. o The environmental impact, degradation in the place and its surroundings. o Public and social impact, due to the impact on the confidence of the population in the capacity of Public Administrations, physical suffering and the alteration of daily life, including the loss and serious deterioration of essential services. - "Interdependencies": the effects that a disturbance in the operation of the installation or service would produce in other facilities or services, distinguishing the repercussions in the sector itself and in other sectors, and the repercussions of local, regional, national or international scope. - "Level of Security": the level whose activation by the Ministry of the Interior is foreseen in the National Plan for the Protection of Critical Infrastructures, in accordance with the general assessment of the threat and with the specific assessment that is made in each case on each infrastructure. - <i>Incident (scope Real Decreto-ley 12/2018): unexpected or unwanted event with consequences detrimental to the security of networks and information systems.</i> - <i>Incident management (scope Real Decreto-ley 12/2018): procedures followed to detect, analyse, limit and respond to an incident.</i> - "National Catalog of Strategic Infrastructures": the complete information, updated, comparable and systematically computerised relative to the specific characteristics of each one of the strategic infrastructures existing in Spain. 	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Scope (Art 3.3)		
<p>Sectors and sub-sectors in scope:</p> <ul style="list-style-type: none"> - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports) 	<p>Sectors of critical importance</p> <p>Energy Sector: Electric, hydrocarbons, gas.</p> <p>Technology Sector Information: Telephony, radio, television.</p> <p>Transport Sector: Airports, ports, railways and roads.</p> <p>Water Sector: Deposits, reservoirs, treatment, and distribution.</p> <p>Health Sector: Biological, hospital assistance, vaccines and laboratories.</p> <p>Food Sector: Storage and distribution centres.</p> <p>Finance Sector: Regulated markets, payment and compensation.</p> <p>Nuclear Sector: Production and radiological storage.</p> <p>Chemical Sector: Chemical substances, weapons and explosives.</p> <p>Research Sector: Laboratories and storage.</p> <p>Space Sector: Control and telecommunications centres.</p> <p>Administration Sector: High State Institutions, Defence, Interior, Political Parties, Emergency Services.</p> <p><i>(Scope Real Decreto-ley 12/2018) This Royal Decree-Law shall apply to the provision of:</i></p> <p><i>a) Essential services dependent on the networks and information systems included in the strategic sectors defined in the annex to Law 8/2011, of 28 April, establishing measures for the protection of critical infrastructures.</i></p> <p><i>(b) Digital services, as defined in Article 3(e), which are online markets, online search engines and cloud computing services.</i></p> <p><i>They shall be subject to this royal decree-law:</i></p> <p><i>Operators of essential services established in Spain. It shall be understood that an essential services operator is established in Spain when its residence or registered office is in Spanish territory, provided that these coincide with the place where the administrative management and management of its business or activities are effectively centralised.</i></p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Annex)</i></p> <p><i>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Article 2. Scope of application.)</i></p>
Identification of the ECI (Art. 3)		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<p>MS body(-ies) responsible for the identification of potential ECI</p> <p><i>Identification of essential services and operators of essential services.</i></p>	<p>Ministry of Interior, through the Secretary of State for Security, as well as CNPIC. In particular, the process of identifying an infrastructure as critical is carried out by the CNPIC.</p> <p>(Scope Real Decreto-ley 12/2018) 1. The identification of essential services and the operators that provide them shall be carried out by the bodies and procedures provided for by Law 8/2011, of 28 April, and its implementing regulations.</p> <p>(Scope Real Decreto-ley 12/2018) The list of essential services and the operators of these services shall be updated, for each sector, on a biennial basis, in conjunction with the review of the sectorial strategic plans provided for in Law 8/2011 of 28 April.</p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 5)</i></p> <p><i>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 6).</i></p>
<p>Application of the procedure for the identification of ECI (as per Annex III)</p>	<p>The Ministry of the Interior, is responsible for the National Catalog of Strategic Infrastructures, an instrument that which contains all the information and assessment of the country's strategic infrastructures, including those that will be included those classified as ECI.</p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 5)</i></p>
<p><i>Step1 – Application of sectoral criteria</i></p>	<p>For each strategic sector, at least one ministry, organism, entity or organ of the General State Administration is designated. The appointment, registration or resignation of a ministry or organisation with responsibility for a strategic sector shall be carried out through the modification of the annex to this Law. The ministries and agencies of the System will be responsible for promoting, within their scope of competence, the Government's security policies on the different national strategic sectors and for ensuring their application, acting also as specialised contact points in the matter. For this, they will collaborate with the Ministry of the Interior through the Secretary of State for Security.</p> <p>Based on the information described above, the process of identifying an infrastructure as critical will be carried out by the CNPIC, which will be able to request the participation and advice of the interested party, as well as of the competent System agents, who will subsequently report on the outcome of such process.</p> <p>(Scope Real Decreto-ley 12/2018) An operator shall be identified as an operator of essential services if an incident suffered by the operator is likely to have significant disruptive effects on the provision of the service, taking into account at least the following factors:</p> <p>a) In relation to the importance of the service provided:</p> <p>The availability of alternatives to maintain a sufficient level of provision of the essential service;</p> <p>The assessment of the impact of an incident on the provision of the service, evaluating the extent or geographical areas that could be affected by the incident; the dependence of other strategic sectors on the essential service offered by the entity and the impact, in</p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 5)</i></p> <p><i>Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (Article 8).</i></p> <p><i>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 6).</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p><i>terms of degree and duration, of the incident on economic and social activities or on public safety.</i></p> <p><i>b) In relation to the clients of the entity evaluated:</i></p> <ol style="list-style-type: none"> <i>1. The number of users who place their trust in the services provided by the entity;</i> <i>2. ° Its market share.</i> <p><i>Sector-specific factors may be added by regulation to determine whether an incident could have significant disruptive effects.</i></p>	
Step 2 – Application of the definition of critical infrastructure	<p>The competence to classify an infrastructure as strategic, and where appropriate, as critical infrastructure or critical European infrastructure, as well as to include it in the National Catalog of Strategic Infrastructures, will correspond to the Ministry of the Interior, through the State Secretariat of Security, including proposals, where appropriate, from the competent body of the Autonomous Communities and Cities.</p> <p>(Scope Real Decreto-ley 12/2018) <i>In the case of a critical operator designated in compliance with Law 8/2011 of 28 April, it will suffice to establish its dependence on networks and information systems for the provision of the essential service in question.</i></p> <p><i>3. In identifying essential services and essential service operators, the relevant recommendations adopted by the co-operation group shall be taken into account to the greatest extent possible.</i></p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 5)</i></p> <p><i>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 6).</i></p>
Step 3 – Application of the transboundary element of the definition of ECI	<p>The classification of an infrastructure as a potential ECI will entail the additional obligation to communicate its identity to other Member States that may be significantly affected by it, in accordance with the provisions of Directive 2008/114 / EC. In this case, the notifications, in reciprocity with other Member States, will be made by the CNPIC, in accordance with the security classification that corresponds according to the current regulations.</p> <p>(Scope Real Decreto-ley 12/2018) <i>When an operator of essential services offers services in other Member States of the European Union, the single contact points in those States shall be informed of the intention to identify it as an operator of essential services.</i></p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 5)</i></p> <p><i>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 6).</i></p>
Step 4 – Application of the cross-cutting criteria	<p>The Ministry of the Interior, through the Secretariat of State for Security, is responsible for classifying an infrastructure as strategic and, where appropriate, as a critical infrastructure or European critical infrastructure, as well as including it for the first time</p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	in the Catalog, prior verification that it meets one or more of the horizontal criticality (see section on definitions). Moreover, CNPIC is tasked with analysing the effects of sectoral interdependencies based on the information provided by the operators.	<i>infraestructuras críticas (Articles 5, 7)</i>
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	<p><i>The process of identifying potential Critical Infrastructures is a Cross-Cutting Criteria and takes into account the IMPACT on the population (casualties and injured), economic effects, environmental effects, and service disruption (recovery time in number of days, geographical extension, size of population affected, cascading effects on other assets...).</i></p> <p><i>To assess the Impact they use a Criticality Scale: A range from 0 to 5. In which 4 and 5 are considered Critical and 3, 2 and 1 Essential.</i></p> <p><i>VERY SERIOUS: The loss of this infrastructure would have a catastrophic impact on Spain.</i></p> <p><i>SERIOUS: The impact of loss of these assets on essential services would be severe.</i></p> <p><i>-An asset is mapped against the consequences of a potential service failure. The criticality levels (from 0 to 5) are mapped against the cross-cutting criteria (casualties, economic impact...). This segmentation is done jointly with sector-specific criteria, which are unique to each of the 12 critical sectors.</i></p> <p><i>Only assets at category 4 and above are considered truly critical.</i></p> <p><i>The combination of the category level and the likelihood of the attack (threats and vulnerabilities) identify the asset priority.</i></p>	
Identification of potential ECI on an ongoing basis (Art 3.1)	In the cases in which there is a relevant modification that affects the infrastructures, the operators responsible for them will provide, through the means made available to them by the Ministry of the Interior, new data to the CNPIC, which must validate it prior to its incorporation into the Catalog. In any case, the update of the available data should be done on an annual basis. In particular, CNPIC is tasked with maintaining and updating the Catalog, establishing the procedures for registration, deregistration and modification of infrastructures, both national and European, that are included in it under the horizontal criteria and on basis of sectoral interdependencies.	<i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Articles 5, 7)</i>
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	Identification by CNPIC, designation by Ministry of the Interior through the National Commission for the Protection of Critical Infrastructures (See table below). The negotiation process is performed on the basis of the stipulations of the Directive. In particular, the Decree states that CNPIC is responsible to execute the actions derived from compliance with Directive 2008/114/EC on behalf of the Secretary of State for Security (Article 7) and the Secretary of State for Security must ensure compliance with the obligations and commitments assumed by Spain within the framework of Directive 2008/114/EC, without prejudice to the competences that correspond to the Ministry of Foreign Affairs and Co-operation.	<i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Articles 6, 7)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>Competent authorities.</p> <p>(Scope Real Decreto-ley 12/2018) 1. The following are competent authorities for the security of networks and information systems:</p> <p>(a) For operators of essential services:</p> <p>In the event that these are also designated as critical operators in accordance with Law 8/2011, of 28 April, and its implementing regulations, regardless of the strategic sector in which such designation is made: the Secretary of State for Security, Ministry of the Interior, through the National Centre for Infrastructure Protection and Cybersecurity (CNPIC).</p>	<p>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 9).</p>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	The classification of an infrastructure as an ECI entails the obligation to communicate its identity to other Member States that may be significantly affected by it, in accordance with the provisions of Directive 2008/114/EC. In this case, the notifications, in reciprocity with other Member States, are made by the CNPIC, in accordance with the security classification that corresponds according to the current regulations.	Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 5)
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	<p><i>The specific steps followed for the consultation process are four:</i></p> <p><i>1st step: In order to assess those critical infrastructures with a cross-border dimension, the Spanish Government set up a technical working group which involved the competent ministries together with the main operators. This WG provided valuable and essential information to start talks with neighbouring countries.</i></p> <p><i>2nd step: An Invitation Letter was sent, to encourage bilateral engagement, work together, and try to reach an agreement on the identification of European Critical Infrastructures.</i></p> <p><i>3rd step: Formal meeting took place</i></p> <p><i>4th step: Final decision taken.</i></p>	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	<p>CNPIC</p> <p><i>The State Secretariat for Security (Ministry of Interior) informed the European Commission, through the Permanent Representation of the country to the European Union, of the outcome of the process initiated.</i></p>	Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 7)
Agreement for the designation of the ECI (Art. 4.3)	<i>When both MS take a final decision and mutually agree on implementing security measures on the designated ECI.</i>	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	CNPIC is the National Contact Point with other MS and with the European Commission, and is tasked with providing, after consulting the National Counter-Terrorism Coordination Centre, reports on threat assessment and types of vulnerabilities and risks found in each of the sectors in which European critical infrastructures have been designated, according to the provisions and parameters set by the Directive	<i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 7)</i>
Informing the owner/operator of the designated ECI (Art. 4.5)	<p>CNPIC informs the operator before proceeding to its final classification.</p> <p>For the designation of a CI/ECI operator, it shall suffice that at least one of the infrastructures managed by it meets the consideration of critical infrastructure, in application of the criticality criteria (see above). In such case, the CNPIC shall prepare a resolution proposal and notify the holder or administrator thereof. The aforementioned proposal shall contain the intention to designate the owner or administrator of the facility or facilities as a CI operator. The interested party shall have a period of fifteen days from the day following receipt of the notification to send to the CNPIC the considerations it deems appropriate, after which the Commission, at the proposal of the Working Group (see table below), shall issue the designated. This resolution may be appealed before the Secretary of State for Security, and, subsequently, before the -administrative jurisdiction. Communications with the interested party will take into account, in any case, the security classification that corresponds according to the current regulations.</p> <p>The CNPIC will be responsible for managing the information and communication management systems that are designed in the field of the protection of critical infrastructures, which must have the support and collaboration of the System's agents and all of them those other organisms or entities affected. The Presidency of the Government will facilitate the use of Malla B, a system for secure strategic communications of the National Crisis Management System and the Government Presidency, through which authorised stakeholders will be able to access the information available in the Catalog.</p>	<p><i>Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. (Article 13)</i></p> <p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 14)</i></p> <p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 33)</i></p>
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or	OSPs are the strategic documents that define the general policies of CI operators to guarantee the security of the set of facilities or systems of their ownership or management. Within six months of the notification of its designation, each CI operator	<i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
equivalent is in place and is reviewed regularly	<p>must have prepared an Operator Security Plan and submit it to the CNPIC, which will evaluate it and report it for approval, if applicable, by the Secretary of State for Security. The OSP must establish a risk analysis methodology that guarantees the continuity of the services provided by said operator and in which the application criteria of the different security measures that are implemented to deal with the physical and logical threats identified on each of the types of their assets.</p> <p>The Secretary of State for Security, following a report from CNPIC, will approve the OSP or proposals for improvement thereof, notifying the interested party within a maximum period of two months. CNPIC will manage and safeguard a central registry of all existing OSPs, once these are approved by the Secretary of State for Security. Moreover, within four months of the approval of the OSP, each CI operator must have prepared a Specific Protection Plan for each of CI.</p> <p>The OSP must be reviewed every two years by the critical operators approved by the CNPIC. This may require at any time specific information on the status of implementation of the Operator Security Plan. The same procedure and deadlines apply when a new critical infrastructure is identified. The modification of any of the data included in the Operator's Security Plans will require the automatic updating of these, which will be carried out by the critical operators responsible and will require the express approval of the CNPIC.</p> <p>The Specific Protection Plans of the different CI will include all those measures that the respective operators consider necessary based on the risk analysis carried out regarding the threats, in particular, those of terrorist origin, on their assets, including the IT systems. Each Specific Protection Plan must contemplate the adoption of permanent protection measures, based on the provisions of the previous paragraph, as well as temporary and graduated security measures, which will come, as the case may be, determined by the activation of the National Plan of Protection of Critical Infrastructures, or as a consequence of the communications that the competent authorities can make to the critical operator in relation to a specific threat on one or several infrastructures managed by it.</p> <p>Together with the approval or request for modification, CNPIC, on the basis of the actions of the competent regulatory body and by virtue of the applicable sectoral regulations, will can make recommendations it deems pertinent, proposing in any case a calendar of gradual implementation with a the prioritisation of the measures and the procedures to be adopted.</p>	<i>infraestructuras críticas (Articles 22-29)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>(Scope Real Decreto-ley 12/2018) Security obligations on essential service operators and digital service providers.</p> <p>1. Operators of essential services and digital service providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the networks and information systems used in the provision of services subject to this Royal Decree-Law.</p> <p>Without prejudice to their duty to report incidents under Title V, they shall take appropriate measures to prevent and minimise the impact of incidents affecting them.</p> <p>2. The regulatory implementation of this Royal Decree-Law shall provide for the necessary measures for essential service operators to comply with the provisions of the preceding paragraph.</p> <p>3. Operators of essential services shall designate and communicate to the competent authority, within the period established by regulation, the person, unit or collegiate body responsible for information security, as the point of contact and technical coordination with the public administration.</p>	<p>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 16).</p>
Verification that the OSP or equivalent is in place	<p>The Government Delegations to the Autonomous Communities the authority to ensure the correct execution of the different Specific Protection Plans and shall have powers of inspection in the field of the protection of critical infrastructures. Said powers are developed, where appropriate, in a coordinated manner with the inspection authorities of the competent body or body to grant the operators the corresponding authorisations according to current sectorial legislation.</p> <p>In the exercise of this monitoring, the competent bodies may at any time request from the person responsible for the CI or ECI the updated status of the implementation of the measures proposed in the resolutions approving or modifying the Specific Protection Plans prepared in case of variation of the circumstances that determined their adoption, or to adapt them to the current regulations that affect them, reporting the result of this to the Secretary of State for Security, through the CNPIC.</p> <p>(Scope Real Decreto-ley 12/2018) The competent authorities may, by ministerial order, establish specific obligations to ensure the security of the networks and information systems used by operators of essential services. They may also issue technical instructions and guidance to detail the content of such orders.</p> <p>When drawing up regulations, instructions and guides, they shall take into account the sectoral obligations, the relevant guidelines adopted in the co-operation group and the information security requirements to which the operator is subject by virtue of other rules, such as Law 8/2011 of 28 April and the National Security Scheme approved by Royal Decree 3/2010 of 8 January.</p> <p>The competent authorities shall coordinate among themselves and with the various sectoral bodies competent in the matter, as regards the content and application of orders, technical instructions and guidance issued by them in their respective areas of</p>	<p>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 28)</p>
Verification that the OSP or equivalent is appropriately and regularly reviewed		<p>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 16).</p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>competence, in order to avoid duplication of obligations and to facilitate compliance by essential service operators.</p> <p>Digital service providers shall determine the security measures they will implement, taking into account, as a minimum, technical progress and the following aspects:</p> <p>(a) The security of systems and facilities; (b) Incident management; (c) Business continuity management; (d) Supervision, audits and testing; (e) Compliance with international standards.</p> <p>Digital service providers will also be responsible for the implementing acts by which the European Commission details the above aspects.</p>	
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	<p>CI operators shall appoint and communicate to the Ministry of the Interior a SLO within the period established by regulation.</p> <p>In particular, within three months of their designation as CI operators, these shall name and communicate to the Secretary of State for Security, through the CNPIC, the name of the SLO.</p>	<p>Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. (Article 16)</p> <p>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 34)</p>
Function of the SLO (Art. 6.1)	The SLO will represent the critical operator before the Secretary of State for Security in all matters related to the security of their infrastructures and the different plans specified in this regulation, channelling, where appropriate, operational and information needs that arise in this regard.	Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 34)
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	Inspection delegated to Government Delegations within the Autonomous communities	Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 28)

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	<p>The CNPIC will be responsible for managing the information and communication management systems that are designed in the field of the protection of critical infrastructures, which must have the support and collaboration of the System's agents and all of them those other organisms or entities affected. The Presidency of the Government will facilitate the use of Malla B, a system for secure strategic communications of the National Crisis Management System and the Government Presidency, through which authorised stakeholders will be able to access the information available in the Catalog.</p> <p>(Scope Real Decreto-ley 12/2018) Obligation to notify:</p> <p>1. Operators of essential services shall notify the competent authority, through the CSIRT of reference, of incidents that may have significant disruptive effects on those services. Notifications may also refer, as determined by regulation, to events or occurrences that may affect the networks and information systems used for the provision of essential services, but which have not yet had a real adverse effect on those services.</p> <p>2. Likewise, digital service providers shall notify the competent authority, through the reference CSIRT, of incidents that have significant disruptive effects on these services. The obligation to report the incident shall only apply where the digital service provider has access to the information necessary to assess the impact of an incident.</p> <p>3. Notifications from both essential service operators and digital service providers shall refer to incidents affecting the networks and information systems used to provide the services indicated, whether they are their own networks and services or those of external providers, even if these are digital service providers subject to this Royal Decree-Law.</p> <p>4. Competent authorities and reference CSIRTs shall use a common platform to facilitate and automate incident reporting, communication and information processes.</p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 33)</i></p> <p><i>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 19).</i></p>
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	CNPIC	<i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 7)</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	<p>CNPIC develops reports on threat assessment and types of vulnerabilities and risks found in each of the sectors in which European critical infrastructures have been designated, in the terms and conditions set by the Directive.</p> <p>National Plan for protection of CI</p> <p>Moreover, the National Plan for the Protection of CI is the State's programming instrument prepared by the Secretary of State for Security and aimed at keeping the Spanish infrastructures that provide essential services to society safe. The National Plan for the</p>	<i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 7)</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>Protection of Critical Infrastructures establishes the criteria and precise guidelines to mobilise the operational capacities of public administrations in coordination with operators, articulating the necessary preventive measures to ensure the permanent, updated and homogeneous protection of the system of strategic infrastructures vis-à-vis the threats coming from deliberate attacks against them. In addition, the Plan provides for different levels of security and police intervention, which will be activated, in each case, based on the results of the threat assessment and in coordination with the existing Plan for Prevention and Protection against Terrorism. The Plan is updated every 5 years.</p> <p>Sectoral Strategic Plans</p> <p>The Sectoral Strategic Plans are the planning instruments with scope throughout the national territory that will allow knowing, in each of the sectors contemplated in the annex of Law 8/2011, what are the services considered as essential, the general functioning of these, the vulnerabilities of the system, the potential consequences of their inactivity and the strategic measures necessary for their maintenance. The Working Group, coordinated by CNPIC, will elaborate with the participation and technical advice of the affected operators, where appropriate, a Strategic Plan for each one of the sectors or sub-sectors of activity. The Sectoral Strategic Plans will be based on a general risk analysis that considers the potential vulnerabilities and threats, both physical and logical, that affect the sector or sub-sector in question in the field of the protection of strategic infrastructures. Each Sectoral Strategic Plan shall contain, as a minimum, the following data:</p> <ul style="list-style-type: none"> - Analysis of risks, vulnerabilities and consequences at the global level. - Proposals for the implementation of organisational and technical measures necessary to prevent, react and, where appropriate, alleviate the possible consequences of the different scenarios that are foreseen. - Proposals for the implementation of other preventive and maintenance measures (for example, exercises and drills, preparation and instruction of personnel, articulation of the precise communication channels, evacuation plans or operational plans to address possible adverse scenarios). - Coordination measures with the National Plan for the Protection of Critical Infrastructures. <p>(scope Real Decreto-ley 12/2018) Incidents affecting digital services.</p> <p>Operators of essential services and digital service providers subject to this Royal Decree-Law, as well as any other interested party, who become aware of incidents that significantly affect digital services offered in Spain by providers established in other Member States of the European Union, may notify the competent authority providing</p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Articles 16-18)</i></p> <p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Articles 19-21)</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p><i>the relevant information in order to facilitate co-operation with the Member State in which the said provider is established.</i></p> <p><i>Similarly, if they become aware that such providers have failed to comply with the applicable security or incident reporting requirements in Spain, they may notify the competent authority providing the relevant information.</i></p>	<p><i>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 24).</i></p>
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	<p>CNPIC</p> <p>(scope Real Decreto-ley 12/2018) Handling of incidents with cross-border impact.</p> <p><i>When competent authorities or reference CSIRTs become aware of incidents that may affect other Member States of the European Union, they shall inform the Member States concerned via the single contact point, specifying whether the incident is likely to have significant disruptive effects on the essential services provided in those States.</i></p> <p><i>2. When information is received through this contact point on incidents notified in other countries of the European Union that may have significant disruptive effects on the essential services provided in Spain, the relevant information shall be forwarded to the competent authority and to the reference CSIRT, so that they may take the appropriate measures in the exercise of their respective functions.</i></p> <p><i>3. The actions considered in the previous sections are understood to be without prejudice to the exchange of information that the competent authorities or the reference CSIRTs may carry out directly with their counterparts in other Member States of the European Union in relation to incidents that may be of mutual interest.</i></p>	<p><i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 7)</i></p> <p><i>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 25).</i></p>
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	<p><i>The appointment as ECIP Contact Point is made formally by delegation of The Ministry of Interior, through the Secretariat of State for Security, the competent body for the protection of critical infrastructures in Spain.</i></p>	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
MS body(-ies) serving as ECIP contact point	CNPIC	<i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Article 7)</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	See table above.	
Scope of national CIP policy		
Sectors of critical importance	See table above.	
Number of national CI	N.A.	
Number of national CI operators	N.A.	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	<ul style="list-style-type: none"> - The transposition of Directive 114/08 was an occasion to develop a comprehensive law on CI protection in Spain - Critical infrastructures are defined in the Spanish national security strategy as installations, networks, physical and information technology systems and equipment whose functioning is indispensable and for which there are no alternative solutions. The disturbance or destruction of any of these assets may have a direct impact on National Security and affect, for example, financial stability, public health or a combination of these security dimensions. The considerable complexity of the systems which underpin public services and the interrelations between these systems explain why the failure of a critical infrastructure can trigger a cascade of negative effects by causing a chain of failures in other systems or installations, with harmful consequences on basic services for the population and the functioning of the State. 	<i>THE NATIONAL SECURITY STRATEGY: Sharing a Common Project, Government of Spain, 2013</i>
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	<ul style="list-style-type: none"> - One of the strategic lines of actions of the Spanish national security strategy is Balance and efficiency. The Government applies a homogeneous 	<i>THE NATIONAL SECURITY STRATEGY: Sharing a Common</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	methodology that allows efforts to be concentrated on the most vital areas, with an identification and classification of infrastructures according to priority	<i>Project, Government of Spain, 2013</i>
Coordination of ministries, bodies and offices concerned	<ul style="list-style-type: none"> - The <i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas</i>, in Article 5 states that The Critical Infrastructure Protection System is made up of a series of institutions, bodies and companies, coming from both the public and private sectors, with responsibilities for the proper functioning of essential services or in the security of citizens. These are: <ul style="list-style-type: none"> o The Secretary of State for Security of the Ministry of the Interior. o CNPIC. o The Ministries and organisms of competence for each CI sectors o The Autonomous Communities and the Cities with the Statute of Autonomy. o The Government Delegations in the Autonomous Communities and in the Cities with the Statute of Autonomy. o The National Commission for the Protection of Critical Infrastructures, which is an interministerial body chaired by the Ministry of Interior o The Interdepartmental Working Group for the Protection of Critical Infrastructures, which is chaired by CNPIC. o Critical operators in the public and private sectors. 	<i>Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (Title 2 – Articles 6-15)</i>
Communication owners/operators with	The Spanish national security strategy establishes shared responsibility and public-private co-operation. Both Public Administrations and private operators must assume the corresponding responsibility and work in a coordinated manner in the protection of critical infrastructures at all times. The Government promotes the creation of a system that includes all the responsible agents and will facilitate the secure communication channels and procedures that make possible the mutual co-operation and the exchange of information of interest for all parties.	
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	See table above.	
Other relevant aspects of national authorities involved in CIP protection	See table above.	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	See table above.	
- Preparation of a security plan	See table above.	
- Review of the plan (timing)	See table above.	
- Reporting incidents	See table above.	
- Exchange of information	See table above.	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>(scope Real Decreto-ley 12/2018) Strategic framework for the security of networks and information systems.</p> <p><i>The National Cybersecurity Strategy, under the umbrella of and aligned with the National Security Strategy, frames the objectives and measures to achieve and maintain a high level of security of networks and information systems.</i></p> <p><i>The National Cybersecurity Strategy will address, among other issues, those set out in Article 7 of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.</i></p> <p><i>To this end, the National Security Council will promote the revision of the National Cybersecurity Strategy, in accordance with the provisions of Article 21.1 e) of Law 36/2015 of 28 September on National Security.</i></p>	<p><i>Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. (Art 8)</i></p>

Sweden

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Ordinance N. 611-2009 amending the Ordinance 1002-08 "Swedish Civil Contingencies", Ordinance N. 513-2012 amending the Ordinance 1119-2007 "instruction to Swedish enterprises in the energy sector", Ordinance N. 793-2012 amending the Ordinance 185-2010 "instruction for the transport administration", Ordinance N. 512-2012 amending the Ordinance 1153-2007 "instruction for the Swedish Energy Agency"</i>	
Definitions (Art 2)		
'critical infrastructure'	The directive has not been implemented in national law	
'European critical infrastructure'	The directive has not been implemented in national law	
'risk analysis'	The directive has not been implemented in national law	
'sensitive critical infrastructure protection related information'	The directive has not been implemented in national law	
'protection'	The directive has not been implemented in national law	
'owners/operators of ECI'	The directive has not been implemented in national law	
Other relevant national definitions	The directive has not been implemented in national law	
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	<p>Transport sector The Swedish Transport Administration shall carry out every two years an identification work of potential European critical infrastructure in the transport sector according to Council Directive 2008/114/EC and submit it to the Swedish Civil Contingencies Agency</p> <p>Energy sector (electricity): The Swedish Transmission System operator, shall carry out every two years, after consulting the Swedish energy agency, the identification of potential European Critical Infrastructures in the energy Sub-sector pursuant to Council Directive 2008/114 / EC and submit it to the Swedish Civil Contingencies Agency</p> <p>Energy sector (oil and gas):</p>	<p><i>Ordinance N. 793-2012 amending the Ordinance 185-2010 "instruction for the transport administration" (section 4)</i></p> <p><i>Ordinance N. 513-2012 amending the Ordinance 1119-2007 "instruction to Swedish enterprises in the energy sector"</i></p> <p><i>Ordinance N. 512-2012 amending the Ordinance 1153-2007</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	The Swedish energy agency, shall carry out every two years, after consulting the Swedish Transmission System operator, the identification of potential European Critical Infrastructures in the energy Sub-sector pursuant to Council Directive 2008/114 / EC and submit it to the Swedish Civil Contingencies Agency	"instruction for the Swedish Energy Agency"(Section 2)
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The Swedish Transport Administration, The Swedish energy agency and The Swedish Transmission System operator	
Application of the procedure for the identification of ECI (as per Annex III)	Common analysis made for each sector in 2009, updated every second year from the responsible bodies.	
Step1 – Application of sectoral criteria	According to sector specific criterion in directive	
Step 2 – Application of the definition of critical infrastructure	According to the cross-cutting criteria in directive	
Step 3 – Application of the transboundary element of the definition of ECI	According to transboundary element of definition in 2b	
Step 4 – Application of the cross-cutting criteria	According to the cross-cutting criteria in directive	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	The criterion of Economic effect, significant economic loss and degradation of products and services (art 3, 2b) disruption of daily life/loss of essential services (art 3, 2c) were mainly focus for definitions.	
Identification of potential ECI on an ongoing basis (Art 3.1)	Every second year	
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	Government offices: Ministry of Justice in consultation with Ministry of enterprise and innovation	
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	If needed, Ministry of Justice through The Swedish Contingencies Agency	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	If needed, The Swedish Contingencies Agency in co-operation with other relevant bodies mentioned above. Discussion and tools on an ad hoc basis.	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	If needed, The Swedish Contingencies Agency	
Agreement for the designation of the ECI (Art. 4.3)	Collective governmental decision (channelled through Ministry of Justice)	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The Swedish Contingencies Agency	
Informing the owner/operator of the designated ECI (Art. 4.5)	If needed, The Swedish Contingencies Agency	
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly		
Verification that the OSP or equivalent is in place		
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place		
Function of the SLO (Art. 6.1)		
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)		
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)		
Reporting (Art. 7)		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
MS body(-ies) responsible for fulfilling reporting obligations	The Swedish Transport Administration, The Swedish energy agency and The Swedish Transmission System operator are responsible for fulfilling reporting obligations to the Swedish Contingencies Agency every second year. The Swedish Contingencies Agency then reports to the Commission. The Swedish Contingencies Agency is not formally designated to report but has taken this role according to PoC-responsibility. (<i>Ordinance N. 611-2009 amending the Ordinance 1002-08 "Swedish Civil Contingencies"</i>)	<i>Ordinance N. 611-2009 amending the Ordinance 1002-08 "Swedish Civil Contingencies",</i> <i>Ordinance N. 793-2012 amending the Ordinance 185-2010 "instruction for the transport administration" (section 4)</i> <i>Ordinance N. 513-2012 amending the Ordinance 1119-2007 "instruction to Swedish enterprises in the energy sector"</i> <i>Ordinance N. 512-2012 amending the Ordinance 1153-2007 "instruction for the Swedish Energy Agency"(Section 2)</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	<i>The Swedish Civil Contingencies Agency, in co-operation with authorities, municipalities, county councils, organisations and companies, shall identify and analyse vulnerabilities, threats and risks in society which may be considered to be particularly serious. The Authority shall, together with the responsible authorities, carry out an overall planning of measures to be taken. The Authority shall evaluate, compile and report the results of the work to the Government.</i> <i>The aim of the Act on Municipal and County Council Measures prior to and during Extraordinary Events in Peacetime and during Periods of Heightened Alert (2006:544) is to reduce vulnerabilities in local level governmental operations and to maintain a good capacity for handling crises in peacetime, and thereby also attaining a fundamental capacity for civil defence during periods of heightened alert.</i>	The Act on Municipal and County Council Measures prior to and during Extraordinary Events in Peacetime and during Periods of Heightened Alert (2006:544)
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	<i>Annual reporting of the National Risk and Vulnerability Assessment to the Commission.</i>	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	Swedish Civil Contingencies Agency is the Swedish point of contact in accordance with the directive that the EU decided on in this field and which covers the energy and transport sectors.	<i>Ordinance N. 611-2009 amending the Ordinance 1002-08 "Swedish Civil Contingencies"(section 17.a)</i>
MS body(-ies) serving as ECIP contact point		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	<p><i>Ordinance N. 1002-08 "Swedish Civil Contingencies"(section 17.a)</i></p> <p>A functioning society in a changing world - The MSB's report on a unified national strategy for the protection of vital societal functions</p> <p><i>Swedish Civil Contingencies Agency, Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure</i></p>	
Scope of national CIP policy		
Sectors of critical importance	<p>11 sectors have been identified (<i>not formally regulated</i>)</p> <ul style="list-style-type: none"> • Energy supply (Production & distribution of: electricity, local heating, fuel); • Financial services (Payments, access to cash, central payment system, securities trading); • Trade & industry (Construction, retail, manufacturing) • Health, medical and care services (Emergency medical services, pharmaceutical and equipment supply, childcare, disabled and elderly care, primary health care, psychiatry, social services, disease control for animals and people); • Information and communication (Telephony (mobile & fixed), internet, radio communications, distribution of mail, production & distribution of daily papers, web site information, social media); • Municipal technical services (Drinking water supply, sewage treatment, sanitation, road maintenance); • Foodstuffs (Distribution, primary production, inspections and manufacture of foodstuffs); 	<i>Swedish Civil Contingencies Agency, Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, MSB, July 2014</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> Public administration– Management functions and Support functions (Local, regional, national management, funeral services, diplomatic and consular services); Protection, safety and security (The judiciary, prosecution service, military defence, prison service, coastguard, police, fire & rescue service, PSAP, customs & excise, border protection, immigration control, guarding and security activities); Social security (Public pension system, sickness and unemployment insurance); Transport (Air, rail, maritime, road 	
Number of national CI	No NCI formally designated	
Number of national CI operators	No CI operators formally designated	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	In 2014 Sweden developed the Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, developed by MSB – the Civil Protection and Emergency Agency. The objective for the action plan is to create the prerequisites for vital societal functions and critical infrastructure to implement a systematic work on risk management, business continuity management and response to incidents/crisis by 2020.	<i>Swedish Civil Contingencies Agency, Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, MSB, July 2014</i>
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	The Swedish CIP strategy adopts an all-hazards approach. Vital Societal Functions (VSF) & CI can be affected by various threats and risks, when many risks are difficult to predict. It is therefore crucial that work on societal functionality of society is based on a wide threat and risk profile.	<i>Swedish Civil Contingencies Agency, Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, MSB, July 2014</i>
Coordination of ministries, bodies and offices concerned	Municipalities, county councils, county administrative boards and national authorities are represented in the identification and management of CI. Private sector entities have roles as owners and operators. The MSB's task is to support and to coordinate the measures and activities of the action plan	<i>Swedish Civil Contingencies Agency, Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, MSB, July 2014</i>
Communication with owners/operators	Each societal level contains public and private owners and operators. This means that the public sector entities that have a responsibility to identify VSF & CI also have a responsibility to coordinate, i.e. to inform and interact with owners and operators of VSF & CI. This places great demands on both public-public co-operation and private-public co-operation; owners and operators	<i>Swedish Civil Contingencies Agency, Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, MSB, July 2014</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	alike must be invited to take part in the development work and to be made aware of knowledge enhancement measures.	
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	The county administrative boards have an overarching responsibility over the municipalities for implementing relevant measures from the risk and vulnerability analysis (including threat analysis). In these CI and VSF are to be identified but not formally designated, therefor are there no mandatory obligations in place. MSB has a coordinating role, on a national level. <i>No background checks nor CI Inspections are imposed from the national level, though it may be conducted on a voluntary basis at a local level.</i>	<i>Swedish Civil Contingencies Agency, Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, MSB, July 2014</i>
Other relevant aspects of national authorities involved in CIP protection		
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	N/A There are no formally designated NCI in Sweden.	
- Preparation of a security plan	<i>There is a range of laws and regulations at national level and for different subsectors that aims to strengthen national security with different measures, also including important infrastructures. However, these laws and regulations are dispersed and not connected to a national CI-system. Some infrastructures which can be considered as critical might therefor have security plans but not due to a national system for CI.</i>	
- Review of the plan (timing)	N/A	
- Reporting incidents	There are no formal requirements for operators of CI to report incidents (except mandatory requirements stipulated according to the NIS-directive.)	
- Exchange of information	Exchange of information is well established according to some specific regulations (i.e. electricity) but not implemented on a NCI-system basis. Other areas also have established exchange of information but not at the same operational level.	
Other distinctive features of the national CIP framework		
- Approach (sectoral, all-hazards) - Review of the strategy (timing)	Approach: All hazards	<i>Swedish Civil Contingencies Agency, Action Plan for the Protection of Vital Societal</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
<ul style="list-style-type: none"> - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Risk management, Business continuity management and response to incidents/crisis: In order to meet changes in, for example, risks and dependencies there is a need for work on the protection of VSF & CI to be performed in a continuous process that is developed and updated in line with alterations to society and its challenges. A systematic work on security at all levels is fundamental for the protection of VSF & CI. Within the framework of this work on risk management, business continuity management and response to incidents/crisis are included as important pillars.</p> <p>These are all connected to and supplement each other.</p> <p>Risk management includes identifying, processing, evaluating, managing and controlling risks, for example, in the context of RVA (and preferably in accordance with the Risk Management Standard ISO 31000).</p> <p>Business continuity management (with methods from, for example, the Business Continuity Management Standard, ISO 22301) focuses on planning to be able to maintain VSF & CI and the processes needed to create the necessary capability for functionality, regardless of type of incident or crisis.</p> <p>Planning for the response to incident & crisis, ranging from incident management to crisis management, creates the conditions for the effective management of an event and so that VSF & CI can be maintained.</p> <p>Review: Action plan with target to implement systematic work on security at all stakeholder levels supposed to be reached in 2020, with continuous improvement envisioned</p> <p>Workflow: The various entities are responsible for identifying VSF & CI as follows:</p> <ul style="list-style-type: none"> - Municipalities identify VSF & CI in their own geographical areas - County administrative boards will identify VSF & CI in their own geographical areas and will have an overarching role for the group of municipalities under their jurisdiction. - County councils (mainly health) will identify VSF & CI within their own fields of responsibility. 	<p><i>Functions & Critical Infrastructure, MSB, July 2014</i></p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<ul style="list-style-type: none"> - National authorities will identify VSF & CI within their own fields of responsibility. <p>Measures: Measures for VSF & CI are planned through the mandatory risk- & vulnerability assessments made at all levels described above.</p> <p>At national level the Swedish Civil Contingencies Agency are i.e. pursuing Regulation on Risk & Vulnerability assessment, Regulation on information security & assurance for governmental agencies and Regulation on mandatory IT-incident reporting. The agency are also supporting stakeholders at all levels through advice and guidance i.e. Guidance on Continuity management, Guidance on protection of vital societal functions, Guidance to increased security in industrial control systems, Guidance on robust tendering for vital societal functions, Guidance on information security & assurance for municipalities, Guidance on robust tendering for IT-systems, Guidance on mitigation of reserve power production systems processes, Guidance on Risk & Vulnerability assessment for antagonistic electromagnetic threats against critical infrastructures and more.</p>	

IMPLEMENTATION TABLES NOT VALIDATED BY PoCs

Cyprus

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011</i>	<i>Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011»</i>
Definitions (Art 2)		
'critical infrastructure'	N/A	
'European critical infrastructure'	N/A	
'risk analysis'	N/A	
'sensitive critical infrastructure protection related information'	N/A	
'protection'	N/A	
'owners/operators of ECI'	N/A	
Other relevant national definitions	N/A	
Scope (Art 3.3)		
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Energy and Transport sector	
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The coordinating authority (Civilian Administrator), in co-operation with the competent authorities, on a case-by-case basis, identifies the possible	<i>Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	ECI located on the territory of the Republic and informs the competent authority (Minister of Interior).	κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011
Application of the procedure for the identification of ECI (as per Annex III)	The Coordinating authority (Civilian Administrator) informs the competent authority and designates an infrastructure as an ECI, following an agreement with the competent authorities of the Member States that may be significantly affected by this infrastructure.	Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011
Step 1 – Application of sectoral criteria	N/A	
Step 2 – Application of the definition of critical infrastructure	N/A	
Step 3 – Application of the transboundary element of the definition of ECI	N/A	
Step 4 – Application of the cross-cutting criteria	N/A	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	N/A	
Identification of potential ECI on an ongoing basis (Art 3.1)	N/A	
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	The Council of Ministers and designates an infrastructure as an ECI, following an agreement with the competent authorities of the Member States that may be significantly affected by this infrastructure.	Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		Βελτίωσης της Προστασίας τους Κανονισμοί του 2011
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	N/A	
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	N/A	
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	N/A	
Agreement for the designation of the ECI (Art. 4.3)	N/A	
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	N/A	
Informing the owner/operator of the designated ECI (Art. 4.5)	N/A	
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The plans are prepared by the infrastructure managers and submitted by the coordinating authority to the competent services on a case-by-case basis The coordinating authority checks whether the designated ECI have a SLO and a OSP that have to be implemented and regularly reviewed	Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011
Verification that the OSP or equivalent is in place	N/A	
Verification that the OSP or equivalent is appropriately and regularly reviewed		
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The coordinating authority checks whether the designated ECI have a SLO and a OSP that have to be implemented and regularly reviewed	Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011
Function of the SLO (Art. 6.1)	N/A	
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	N/A	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	N/A	
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	N/A	
Performance of threat assessments within ECI subsector within one year following the designation of ECI	N/A	
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	N/A-	
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The Co-ordinating authority is the national contact point for the protection of ECI that coordinates the consideration of ECI protection issues within the Republic with the competent authorities of other Member States.	Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011»
MS body(-ies) serving as ECIP contact point		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011»	Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011»
Scope of national CIP policy		
Sectors of critical importance	Sectors of critical importance: <ul style="list-style-type: none"> • Energy • Nuclear Industry • ICT • Water • Food • Health • Financial • Transport • Chemical Industry 	<ul style="list-style-type: none"> • Booz & Company (2009), Study: stock-taking of existing critical infrastructure protection activities
Number of national CI	It is not specified the number of CI. However, it is specified that there are no ECI in Cyprus	Έκθεση της Κοινοβουλευτικής Επιτροπής Εσωτερικών για τους κανονισμούς «Οι περί Προσδιορισμού και Χαρακτηρισμού των Ευρωπαϊκών Υποδομών Ζωτικής Σημασίας και Αξιολόγησης της Ανάγκης Βελτίωσης της Προστασίας τους Κανονισμοί του 2011»
Number of national CI operators	N/A	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	Cyprus does not have a critical infrastructure protection strategy or plan in place. The critical infrastructure protection in general is under the responsibility of the Ministry of Interior and Civil Defence.	Link

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	N/A	
Coordination of ministries, bodies and offices concerned	N/A	
Communication with owners/operators	N/A	
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	N/A	
Other relevant aspects of national authorities involved in CIP protection	N/A	
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	See the table above	
- Preparation of a security plan	See the table above	
- Review of the plan (timing)	See the table above	
- Reporting incidents	N/A	
- Exchange of information	N/A	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	Cybersecurity Cyprus has recently approved the "Cybersecurity Strategy of the Republic of Cyprus" (2017) with a view to implement the NIS Directive	<i>Presentation: Cybersecurity Strategy of the Republic of Cyprus, George Michaelides Commissioner Office of the Commissioner of Electronic Communications & Postal Regulation, 26/04/2017</i>

Lithuania

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo</i>	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo</i>
Definitions (Art 2)		
'critical infrastructure'	Critical Infrastructure means an institution or its structural unit, enterprise, installation or part of the installation, regardless of whether its manager is a private or public administration, providing critical services that if impaired or destroyed could adversely affect national security, the economy of the country, the interests of the state or society.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Article 1)</i> <i>NUTARIMAS DĖL YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS IDENTIFIKAVIMO METODIKOS PATVIRTINIMO (Art. 2.3) for Critical Infrastructure definition</i>
'European critical infrastructure'	European Critical Infrastructure is a CI of national significance in the Member States of the European Union, the destruction or disruption of which would have a significant impact on at least two Member States. The magnitude of the impact is assessed on the basis of the general criteria for assessing the impact of other types of infrastructure.	
'risk analysis'	n.a.	
'sensitive critical infrastructure protection related information'	Classified information are information concerning the existence or content of documents, works, products or other objects recognised by the state secret or secret service, as well as the documents, works, products or other objects that if disclosed could be used to plan / execute attacks to ECI/CI	
'protection'	Protection is an activity aimed at ensuring the functionality, continuity and integrity of CI/ECI, preventing, reducing or neutralising threats, risks or vulnerabilities.	
'owners/operators of ECI'	Owners/operators of ECI are owners/operators of sites of national significance that are designated as ECI, responsible for the daily operations of these infrastructures.	
Other relevant national definitions		
Scope (Art 3.3)		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Sectors and sub-sectors in scope: - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports)	Same as Directive: - Energy a. Electricity b. Oil c. Gas - Transport a. Road transport b. Air transport c. Air transport d. Inland waterways transport e. Ocean and short-sea shipping and ports	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Annex 1)</i>
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	The Prime Minister's Office, following proposals from the competent Ministries of Energy and Transport	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Section II)</i>
Application of the procedure for the identification of ECI (as per Annex III)	The sequence of actions for identifying European Critical Infrastructure in Lithuania is described in Annex 3 of the Procedure	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Annex 3; Art. 12)</i>
<i>Step1 – Application of sectoral criteria</i>	The first step is to assess whether potential European Critical Infrastructures meet the sector criteria. The national transposition documents do not describe how this is performed in practice.	
<i>Step 2 – Application of the definition of critical infrastructure</i>	The second step - the potential ECI must comply with the definition of the object of "state importance" and, in accordance with the Description of the Procedure for the Recognition of infrastructures as State-owned infrastructures, approved by the Government of the Republic of Lithuania in 2010, June 7 Resolution No. 717 (Official Gazette, 2010, No. 69-3442), to be attributed to infrastructures of state importance;	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	The third step is to assess whether disruption or destruction of a potential ECI would affect other Member States. If the infrastructure is used to provide a necessary service, the alternatives must be taken into account and the duration of the disruption and/or restoration of the operation.	
<i>Step 4 – Application of the cross-cutting criteria</i>	The fourth step - the cross-cutting criteria are applied to infrastructures that fulfil the conditions of the first, second and third steps. The general criteria include: 1. the victims (taking into account the number of potential deaths or injuries); 2. the economic impact criterion (taking into account the extent of the economic loss and / or the deterioration of products or services, including the potential environmental impact); 3. public exposure criteria (taking into account the impact on public confidence, physical suffering and disturbance of daily life, including the loss of essential services).	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	The precise threshold values applicable to the cross-cutting criteria for a specific object of state importance are established on a case-by-case basis.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Section II, Art. 13)</i>
Identification of potential ECI on an ongoing basis (Art 3.1)	Each year, the Ministries of Energy and Transport regularly perform, not less than once a year, a review of the compliance of state-owned objects with the criteria of the energy/transport sector and identifies objects of state importance that could be classified as ECI.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Section II, Art. 5)</i>
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	The Government of the Republic of Lithuania approves the designation of a critical infrastructure as ECI by means of a resolution.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
		<i>ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 21)</i>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	The Prime Minister's Office informs other Member States that may be significantly impacted by a particular CI, the name of this infrastructure and the reasons why it may be classified as ECI. The notification is addressed to contact points designated by the Member States.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Section III, Art. 16)</i>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	The Prime Minister's Office organises bilateral and/or multilateral discussions with other Member States, which could be affected by potential ECI in Lithuania. Representatives from the European Commission may be invited to participate in these discussions, but they are not entitled to access detailed information that would allow the identification of the object or objects of national significance that are being debated	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Section III, Art. 17, 18)</i>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	The Prime Minister's Office may contact the European Commission and inform it of the wish to participate in bilateral and / or multilateral discussions on this matter. Specific channels are not mentioned in transposition act	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 8, Art. 19)</i>
Agreement for the designation of the ECI (Art. 4.3)	The transposition act does not mention when a bilateral / multilateral agreement can be considered achieved.	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	The Prime Minister's Office prepares an annual report for the European Commission with information on the number of sites of national significance classified as ECI by sector and by the number of MS dependent on each ECI.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 33)</i>
Informing the owner/operator of the designated ECI (Art. 4.5)	The Prime Minister's Office informs the owner/operator of a potential ECI concerning the designation as European Critical Infrastructure within 5 working days after the decision of the Government of the Republic of Lithuania.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 22)</i>
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	The owners/operators of ECI shall prepare an OSP within one year from the receipt of the information concerning the designation, and submit a copy to the Prime Minister's Office.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 24)</i>
Verification that the OSP or equivalent is in place	OSP must be reviewed regularly, at least once a year. Revised plans are submitted to the Prime Minister's Office. The Prime Minister's Office controls the preparation of European Critical Infrastructure OSP and whether they meet the requirements.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 27, 29)</i>
Verification that the OSP or equivalent is appropriately and regularly reviewed		

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	The owner/manager of a ECI, after receiving information from the Prime Minister's Office on the designation, shall, within 30 days, nominate an SLO and submit to the Prime Minister's Office the name of the person, his duties, telephone number and e-mail address.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 30)</i>
Function of the SLO (Art. 6.1)	The main responsibilities of the designated SLO is maintaining a security relationship between the owner/operator of the European Critical Infrastructure and the Office of the Prime Minister.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 2)</i>
Verification that the SLO or equivalent is in place (Art, 6.2 and 6.3)	Not specified	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	The Prime Minister's Office shall provide the designated SLO with a telephone number and e-mail address, by which he must immediately inform the Prime Minister's Office of events, incidents, identified risks and threats that could lead to the security of the European Critical Infrastructure and disrupt the operation of this facility.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 31)</i>
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	Prime Minister's Office, competent Ministries, ECI owners/operators	
Performance of threat assessments within ECI subsector within one year following the designation of ECI	ECI owners/operators assess the threats of these infrastructures and report the threats to the relevant Ministry of Energy (if it is classified as a European Critical Infrastructure for the Energy Sector) and the Ministry of Transport (if it is a European Critical Infrastructure for the transport sector). The Ministry	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	of Energy and the Ministry of Transport summarise information on threats in the relevant sectors and submit it to the Prime Minister's Office.	<i>šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 34)</i>
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	The Prime Minister's Office every two years provide the European Commission the information concerning the type of risks, threats and vulnerabilities for each sector whose subject matter has been classified as European Critical Infrastructure (see list of sectors, above)	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 35)</i>
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	The contact point for the protection of European Critical Infrastructure is assigned to the Prime Minister's Office in Lithuania. The Prime Minister's Office is responsible for coordinating with other Member States and the European Commission issues relating to European Critical Infrastructure. Other state institutions participate in solving issues of protection of these objects according to their competence.	<i>Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 "Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo"(Art. 37)</i>
MS body(-ies) serving as ECIP contact point		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	„LIETUVOS RESPUBLIKOS - NACIONALINIAM SAUGUMUI UŽTIKRINTI SVARBIŲ OBJEKTŲ APSAUGOS – ĮSTATYMAS“ "NUTARIMAS DĖL YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS IDENTIFIKAVIMO METODIKOS PATVIRTINIMO"	<i>Document No.: XIII-992, Published: TAR, 23-21-2018, No. 1004</i>
Scope of national CIP policy		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Sectors of critical importance	<p>The following sectors of the economy are strategically important for national security:</p> <ol style="list-style-type: none"> 1) Energy <ol style="list-style-type: none"> a. Electricity b. Oil and oil products c. Natural gas d. District Heating 2) Transportation <ol style="list-style-type: none"> a. Air transport b. Road transport c. Railway transport d. Maritime transport e. Postal 3) Information technology and telecommunications, other high-tech <ol style="list-style-type: none"> a. Information technology b. Electronic communications 4) Finance and credit <ol style="list-style-type: none"> a. Banking services; b. Payment transfer service c. Stock exchange service. 5) Water Supply Sector <ol style="list-style-type: none"> a. Drinking water b. Sewage 6) Food Sector: <ol style="list-style-type: none"> a. Agricultural/food production service; b. Provision of food (public storage) service; c. Food quality and safety assurance. 7) Health sector: <ol style="list-style-type: none"> a. Emergency Medical Assistance Service; b. In-patient and outpatient care; c. Supply of medicines, vaccines, blood and medical supplies; d. Infectious Diseases/Epidemic Control Service. 8) Public security and legal order sector: <ol style="list-style-type: none"> a. Public safety assurance service; b. Judicial and penal system. 9) Industry Sector: <ol style="list-style-type: none"> a. Chemical and Nuclear Industry; 10) Government management sector: 	<p>"NUTARIMAS DĖL YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS IDENTIFIKAVIMO METODIKOS PATVIRTINIMO" Chapter II, Art. 4</p>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>a. Functioning of the main institution in Lithuania (i.e. the President of the Republic, the Government, and the management of critical information resources of the state).</p> <p>11) Civil Protection:</p> <p>a. General emergency telephone service;</p> <p>b. alert for extreme events and situations and their services, liquidation, removal, rescue and coordination of the population and property.</p> <p>12) Environment:</p> <p>a. Air Pollution Observation and Early Warning Service;</p> <p>b. Meteorological observation and early warning service;</p> <p>c. Surveillance (River, Lakes) Surveillance and Early Warning Service;</p> <p>d. Marine Pollution Observation and Control Service.</p> <p>13) Foreign and Security Policy:</p> <p>a. Foreign and Security Policy Implementation Service.</p>	
Number of national CI	n.a	
Number of national CI operators	n.a	
Responsibilities allocated to Ministries, bodies, and offices		
Definition of scope and objectives of the national CIP strategy	The Critical infrastructure protection strategy in Lithuania is heavily based on cybersecurity measures as established by the Resolution for the approval of the identification of information infrastructure method, adopted in 2016	"NUTARIMAS DĖL YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS IDENTIFIKAVIMO METODIKOS PATVIRTINIMO"
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	The competent authorities are asked to fill a questionnaire on order to assess the risk and vulnerabilities of potential critical infrastructures.	
Coordination of ministries, bodies and offices concerned	Same as table above	
Communication with owners/operators	Same as table above	
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)		
Other relevant aspects of national authorities involved in CIP protection		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	Same as table above	
- Preparation of a security plan	Same as table above	
- Review of the plan (timing)	Same as table above	
- Reporting incidents		
- Exchange of information	Same as table above	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 		

United Kingdom

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
List of national measures transposing and implementing Directive 2008/114 into the national legal system	<p>For Gibraltar: <i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011</i></p> <p>For mainland UK: <i>Administrative Arrangements for amending the CPNI procedures in view to including those related to the assessment of the identification and designation of ECI</i></p>	
Definitions (Art 2)		
'critical infrastructure'	"critical infrastructure" means an asset, system or part thereof located in Gibraltar which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in Gibraltar as a result of the failure to maintain those functions;	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011;</i> Section 21</p>
'European critical infrastructure'	"European critical infrastructure" or "ECI" means critical infrastructure located in Gibraltar the disruption or destruction of which would have a significant impact in at least Gibraltar and a Member State and the significance of the impact shall be assessed in terms of cross-cutting criteria which must include effects resulting from cross-sector dependencies on other types of infrastructure;	
'risk analysis'	"risk analysis" means consideration of relevant threat scenarios in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure;	
'sensitive critical infrastructure protection related information'	"sensitive critical infrastructure protection related information" means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations;	
'protection'	"protection" means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability	
'owners/operators of ECI'	"owners or operators of ECI" means those entities responsible for investments in, or day-to-day operation of, a particular asset, system or part thereof designated as an ECI	
Other relevant national definitions	n/a	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Scope (Art 3.3)		
<p>Sectors and sub-sectors in scope:</p> <ul style="list-style-type: none"> - Energy sector (Sub-sectors: Electricity, Oil, Gas) - Transport sector (Sub-sectors: Road, Rail, Air, Inland waterways, Ocean and short-sea shipping and ports) 	<p>Note that the UK did not limit their analysis to the sectoral boundaries of the Directive.</p> <p>FOR GIBRALTAR:</p> <p>Energy sector</p> <ul style="list-style-type: none"> (i) electricity, comprising infrastructures and facilities for generation and transmission of electricity in respect of supply of electricity, (ii) oil, comprising oil production, refining, treatment, storage and transmission by pipelines, (iii) gas, comprising gas production, refining, treatment, storage and transmission by pipelines, and LNG terminals; and <p>Transport sector</p> <ul style="list-style-type: none"> (i) road transport, (ii) air transport, (iii) ocean and short-sea shipping, and (iv) ports <p>FOR MAINLAND UK:</p> <p>Note that the UK did not limit their analysis to the sectoral boundaries of the Directive. The sectoral actors considered all the elements of a sector, which would also include ICT components if required. As mentioned above, the sectors are:</p> <ul style="list-style-type: none"> • Chemicals • Civil Nuclear • Communications (Broadcast, telecommunications, civil, postal) • Defence • Emergency services (Ambulance, coast guard, Fire & rescue, Police) • Energy (Electricity, Gas, Oil) • Finance • Food 	<ul style="list-style-type: none"> • <i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report.</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<ul style="list-style-type: none"> • Government • Health • Space • Transport (Aviation, Ports, Rail, Road) • Water <p>Each sector has one or more Lead Government Department(s) (LGD) responsible for the sector, and ensuring protective security is in place for critical assets. The UK government's official definition of CNI is: 'those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:</p> <ul style="list-style-type: none"> - Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or - Significant impact on national security, national defence, or the functioning of the state.' 	
Identification of the ECI (Art. 3)		
MS body(-ies) responsible for the identification of potential ECI	<p>FOR GIBRALTAR: Government of Gibraltar</p> <p>FOR MAINLAND UK: Working, where appropriate, with infrastructure owners and regulators, the Government departments responsible for the 13 Critical Sectors mentioned above are required to produce Sector Resilience Plans on an annual basis. The process is coordinated by the Civil Contingencies Secretariat (based in the Cabinet Office).</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 22</i></p> <p><i>Summary of the 2015-16 Sector Resilience Plans, UK Cabinet Office</i></p>
Application of the procedure for the identification of ECI (as per Annex III)	<p>FOR GIBRALTAR: When identifying the critical infrastructures which may be designated as an ECI (the "potential ECI"), the Government of Gibraltar must follow the procedure set out in schedule 2 of the Act (see below)</p> <p>FOR MAINLAND UK:</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011)</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	Sector resilience plans are written in relation to the risks identified in current National Risk Assessments. Although individual plans are confidential, the unclassified summary of sector resilience plans is released annually. The summary provides overall information about the resilience of each critical infrastructure sector separately, identifies the risks and vulnerabilities, the desirable level of resilience, a programme of actions for achieving the desired level, and methods of reporting on progress toward achieving it. Working, where appropriate, with infrastructure owners and regulators, the Government departments responsible for the 13 Critical Sectors are required to produce Sector Resilience Plans on an annual basis.	<i>Best Practices for Critical Information Infrastructure Protection (CIIP), 2016, Inter-American Development Bank. Summary of the 2015-16 Sector Resilience Plans, UK Cabinet Office</i>
<i>Step1 – Application of sectoral criteria</i>	<p>FOR GIBRALTAR: In Step 1, the Gibraltar Government applies the sectoral criteria in order to make a first selection of critical infrastructures within a sector.</p> <p>FOR MAINLAND UK: Sector resilience plans are prepared in close co-operation with relevant regulatory agencies and private sector actors, identifying key risks and threats for each sector.</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011); Schedule 2; (1)</i></p> <p><i>Best Practices for Critical Information Infrastructure Protection (CIIP), 2016, Inter-American Development Bank</i></p>
<i>Step 2 – Application of the definition of critical infrastructure</i>	<p>FOR GIBRALTAR: In Step 2, the Government applies the definition of the term critical infrastructure (see list of definitions) to the potential ECI identified under Step 1. The significance of the impact must be determined either by using Gibraltar's own methods for identifying critical infrastructures or with reference to the cross-cutting criteria, at an appropriate Gibraltar level. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption or recovery must be taken into account.</p> <p>FOR MAINLAND UK: Since the resources needed to protect infrastructure assets are limited, and vulnerabilities at every facility are unequal, the United Kingdom uses a risk-</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011); Schedule 2; (2)</i></p> <p>Cabinet Office, Strategic Framework and Policy Statement</p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	based system for prioritising infrastructure. When assessing risks to CI, the United Kingdom evaluates the likelihood of something happening in the next five years, and the consequences or impacts that people will feel if it does occur.	on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards (United Kingdom: Cabinet Office, 2010)
<i>Step 3 – Application of the transboundary element of the definition of ECI</i>	<p>FOR GIBRALTAR:</p> <p>In Step 3, the Government of Gibraltar applies the transboundary element of the definition of ECI (see list of definitions, above) to the potential ECI that has passed the first two steps of the procedure of identification. A potential ECI which does satisfy the definition must follow the next step of the procedure. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption or recovery must be taken into account.</p> <p>FOR MAINLAND UK</p> <p>The specificity of the UK model is that the well-defined procedures for securing national critical infrastructures (CI) easily incorporated the “European requirements” and did not add further regulatory pressure on operators. Collaboration is enacted through the constant exchange of relevant information, also in the form of security advice that not only increases the awareness of the infrastructures’ operators, but also help them set priorities in the implementation process. It is worth mentioning that the implementation of the pieces of governmental security advice is not mandatory for operators, but it strongly felt as being considered and implemented.</p> <p>NB: SPECIFICS ON HOW TRANSBOUNDARY ELEMENT FOR ECI IDENTIFICATION IS APPLIED IN PRACTICE ARE NOT PROVIDED</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i></p> <p><i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011); Schedule 2; (3)</i></p> <p><i>Critical Infrastructure Protection beyond Compliance. An Analysis of National Variations in the Implementation of Directive 114/08/EC. Global Jurist, Volume 16, Issue 3, Pages 267–289, ISSN (Online) 1934-2640</i></p>
<i>Step 4 – Application of the cross-cutting criteria</i>	<p>FOR GIBRALTAR:</p> <p>The Government of Gibraltar applies the cross-cutting criteria to the remaining potential ECI; the cross-cutting criteria must take into account:</p> <ul style="list-style-type: none"> (a) the severity of impact; (b) for infrastructure providing an essential service, the availability of alternatives; and (c) the duration of disruption or recovery or both. <p>A potential ECI which does not satisfy the cross-cutting criteria must not be considered to be an ECI.</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i></p> <p><i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011); Schedule 2; (4)</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	<p>FOR MAINLAND UK</p> <p>NB: SPECIFICS ON HOW CROSS-CUTTING CRITERIA FOR ECI IDENTIFICATION IS APPLIED IN PRACTICE ARE NOT PROVIDED</p>	
Definition of the thresholds for the cross-cutting criteria (Art. 3.2)	<p>FOR GIBRALTAR:</p> <p>The cross-cutting criteria thresholds must be based on the severity of the impact of the disruption or destruction of a particular infrastructure and the precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Government of Gibraltar.</p> <p>FOR MAINLAND UK</p> <p>Government criteria concerning infrastructure resilience are based on four principles</p> <ul style="list-style-type: none"> • Resistance: Concerns direct physical protection, e.g. the erection of flood defences; • Reliability: The capability of infrastructure to maintain operations under a range of conditions, e.g. electrical cabling is able to operate in extremes of heat and cold; • Redundancy: The adaptability of an asset or network, e.g. the installation of back-up data centres; and • Response and Recovery: An organisation's ability to respond to and recover from disruption. <p>The appropriateness and cost-effectiveness of each component varies across the sectors owing to, for example, the different types of infrastructure, technical opportunities and business models. Infrastructure owners work with government and regulators to select the blend of these components which will produce the most cost effective and proportionate strategy. The sector resilience planning process provides the opportunity for government, regulators and infrastructure owners to work together to produce a mix of resilience components that are:</p> <ul style="list-style-type: none"> • proportionate to the risks identified in National Risk Assessment products; • enabled by improved sharing of information; and • in keeping with legal and regulatory frameworks, industry standards, licence agreements and business models. 	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i></p> <p><i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 22.3</i></p> <p><i>Summary of the 2016 Sector Security and Resilience Plans, Cabinet Office</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Identification of potential ECI on an ongoing basis (Art 3.1)	NO FORMALISED TIMING PROVIDED. SECTOR RESILIENCE PLANS ARE CONDUCTED ON YEARLY BASIS	
Designation of the ECI (Art. 4)		
MS body(-ies) responsible for the designation of ECI (discussions and agreement)	<p>FOR GIBRALTAR: Government of Gibraltar</p> <p>FOR MAINLAND UK Government departments supported by CPNI (UK): There are 13 UK Critical Sectors: Chemicals; Civil Nuclear; Communications; Defence; Emergency Services; Energy; Finance; Food; Government; Health; Space; Transport; and Water. Working, where appropriate, with infrastructure owners and regulators, the Government Departments responsible for the 13 Critical Sectors are required to produce Sector Security and Resilience Plans on an annual basis. Key departments include: Office for Security and Counter Terrorism, Department of Energy and Climate Change, GCHQ. Home Office and the Department for Transport</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 24</i></p> <p><i>Summary of the 2016 Sector Security and Resilience Plans, UK Cabinet Office</i></p>
Informing other MS which may be significantly affected of the identity and reasons for designating a potential ECI (Art. 4.1)	<p>FOR GIBRALTAR: The Government of Gibraltar must inform a Member State which may be significantly affected by a potential ECI about its identity and the reasons for its designation as a potential ECI.</p> <p>FOR MAINLAND UK NO FORMALISED PROCEDURE FOUND</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 24(1)</i></p>
Engaging in bilateral/multilateral discussions with other MS (Art. 4.2)	<p>FOR GIBRALTAR: Where a potential ECI is located in Gibraltar, the Government must engage in discussions with any Member State which may be significantly affected by the potential ECI</p> <p>FOR MAINLAND UK NO FORMALISED PROCEDURE FOUND</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 24(2)</i></p>
Informing the EC about the wish to engage in bilateral/multilateral discussions with MS on whose territory a potential ECI is located (Art. 4.2)	NO FORMALISED PROCEDURE FOUND	

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Agreement for the designation of the ECI (Art. 4.3)	<p>FOR GIBRALTAR: Where a potential ECI is located in Gibraltar, the Government must designate it as an ECI following an agreement between the Government and the Member States which may be significantly affected.</p> <p>FOR MAINLAND UK NO FORMALISED PROCEDURE FOUND</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 24(2))</i></p>
Communicating to the EC the number of designated ECI per sector and the number of MS dependent on each designation (Art 4.4)	<p>FOR GIBRALTAR: Where a designated ECI is located in Gibraltar, the Government shall ensure that the European Commission is informed on an annual basis of the number of designated ECI per sector and of the number of Member States dependent on each designated ECI and only the Member State which may be significantly affected by an ECI shall know its identity.</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 24(3))</i></p>
Informing the owner/operator of the designated ECI (Art. 4.5)	<p>FOR GIBRALTAR: Gibraltar: Where an ECI is located in Gibraltar, the Government shall inform the owner or operator of the infrastructure that the infrastructure has been designated as an ECI and such information shall be classified at an appropriate level.</p> <p>FOR MAINLAND UK NOTE: in mainland UK there is reliance of PPP initiatives and private sector buy-in in CIP. UK representatives have highlighted that pre-existing high levels of co-operation on CIP matters between the main actors has meant that there has been little room for additional improvement in relation between these actors as a direct result of the Directive. CPNI has a key role as coordinating body. NO FORMALISED PROCEDURE FOUND TO INFORM OPERATORS OF ECI STATUS DESIGNATION</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 24(3))</i></p> <ul style="list-style-type: none"> • <i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report.</i>
Operator Security Plan (Art. 5)		
MS authority responsible for ensuring that the OSP or equivalent is in place and is reviewed regularly	<p>FOR GIBRALTAR: Gibraltar: Government of Gibraltar</p> <p>FOR MAINLAND UK CPNI: Even prior to the Directive, the UK already had OSP equivalent requirements, and this was especially effective given the presence of a</p>	<p><i>Legal Notice No. 64 Of 2011. Interpretation And General Clauses Act</i> <i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011</i></p>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	specific CIP forum. CPNI has published guidelines concerning operational requirements, focusing on: <ul style="list-style-type: none">Identifying and prioritising assets that are criticalIdentifying threats and vulnerabilitiesAssess the risksIdentify risk mitigation options and develop a strategic security plan (which is A statement of how an organisation's security needs will be met)Review organisational readiness to deliver the strategic security plan	<i>(Gibraltar Gazette No. 3849 of May 12, 2011; Section 25</i> <i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report.</i> <i>CPNI (2018), Operational Requirements Process</i> https://www.cpni.gov.uk/system/files/documents/e7/2e/CPNI-operational-requirements-level-1-process-infographic.pdf
Verification that the OSP or equivalent is in place	FOR GIBRALTAR: The Government must assess whether each designated ECI located in Gibraltar possesses an OSP or has in place equivalent measures.	<i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 25(2)</i>
Verification that the OSP or equivalent is appropriately and regularly reviewed	FOR MAINLAND UK: While governmental security advice is not mandatory for operators , but it strongly felt as being considered and implemented.	<i>Critical Infrastructure Protection beyond Compliance. An Analysis of National Variations in the Implementation of Directive 114/08/EC. Global Jurist, Volume 16, Issue 3, Pages 267–289, ISSN (Online) 1934-2640</i>
Security Liaison Officer (Art. 6)		
MS authority responsible for ensuring that the SLO or equivalent is in place	FOR GIBRALTAR: The Government of Gibraltar must assess whether each designated ECI located in Gibraltar possesses a Security Liaison Officer or equivalent. If the Government finds that a Security Liaison Officer is in place or an equivalent exists, no further implementation action shall be necessary. If the Government finds that a Security Liaison Officer or equivalent does not exist in relation to a designated ECI, it shall ensure, by any measures it deems appropriate, that such a Security Liaison Officer or equivalent is designated. FOR MAINLAND UK:	<i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 27</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
	SLO equivalent requirements in place prior to the Directive	
Function of the SLO (Art. 6.1)	<p>FOR GIBRALTAR: The SLO shall act as the point of contact for security related issues between the owner or operator of the ECI and the Government.</p> <p>FOR MAINLAND UK: N/A</p>	<i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 27(1))</i>
Verification that the SLO or equivalent is in place (Art. 6.2 and 6.3)	N/A	
Establishment of an appropriate communication mechanism between the relevant Member State authority and the SLO (Art. 6.4)	<p>FOR GIBRALTAR: The Government of Gibraltar must implement an appropriate communication mechanism between the Government and the Security Liaison Officer or equivalent with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned and this communication mechanism shall be without prejudice to the requirements concerning access to sensitive and classified information.</p> <p>FOR MAINLAND UK: Presence of CIP Forum / CPNI ensures presence of adequate two-way communication</p>	<i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 27(5))</i>
Reporting (Art. 7)		
MS body(-ies) responsible for fulfilling reporting obligations	<p>FOR GIBRALTAR: Government of Gibraltar</p> <p>FOR MAINLAND UK: Cabinet Office / CPNI</p>	<i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 28)</i>
Performance of threat assessments within ECI subsector within one year following the designation of ECI	<p>FOR GIBRALTAR: The Government must conduct a threat assessment in relation to ECI subsectors within one year following the designation of critical infrastructure in Gibraltar as an ECI within those subsectors.</p> <p>No further specifications are described in the Act.</p> <p>FOR MAINLAND UK: Sector resilience plans are prepared in close co-operation with relevant regulatory agencies and private sector actors, identifying key risks and threats for each sector (see sections above).</p>	<i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 28(1))</i>

IMPLEMENTATION OF COUNCIL DIRECTIVE 2008/114		
Provision	Content	Source
Reporting of generic data on summary basis on the types of risks, threats and vulnerabilities to the Commission per ECI subsector	FOR GIBRALTAR: The Government shall ensure that every two years a classified report is sent to the European Commission containing generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated.	<i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 28(2))</i>
European critical infrastructure protection contact points (Art. 10)		
Appointment of a ECIP contact point	FOR GIBRALTAR: (1) The Government shall appoint a European critical infrastructure protection contact point ('ECIP contact point'). (2) The ECIP contact point shall coordinate European critical infrastructure protection issues within Gibraltar and shall have such other functions as the Government may prescribe. (3) The appointment of an ECIP contact point does not preclude other relevant authorities in Gibraltar from being involved in European critical infrastructure protection issues.	<i>Civil Contingencies Act 2007 (Amendment) - Regulations 2011 (Gibraltar Gazette No. 3849 of May 12, 2011; Section 30)</i>
MS body(-ies) serving as ECIP contact point	Government (Gibraltar); note that in mainland UK the role is fulfilled de facto by the Cabinet Office	<i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report.</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
List of key measures on the protection of national Critical Infrastructures	No overarching CIP legislation, based on good faith co-operation with private sectors	
Scope of national CIP policy		
Sectors of critical importance	13 Sectors (see table above)	
Number of national CI	N.A.	
Number of national CI operators	N.A.	
Responsibilities allocated to Ministries, bodies, and offices		

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Definition of scope and objectives of the national CIP strategy	<p>CNI includes all the essential mechanisms which keep the country functioning, ranging from the core functions of government, through to ensuring the availability of food and water, fuel and reliable communications. Large parts of CNI are in the private sector. The Government works with infrastructure owners and operators to mitigate risks to CNI from malicious attack and from natural hazards. The UK will make sure that the Government has the right regulatory framework to ensure that CNI is resilient to future threats. This will be done by working with owners and operators to strengthen the cyber security of the infrastructure. Responsibilities for infrastructure policing are shared across a number of organisations with different levels of capability and capacity, and different arrangements for funding, oversight, regulation and legislation. In the future, the UK intends to integrate infrastructure policing.</p> <p>Not everything within a national infrastructure sector is judged to be 'critical'. The UK government's official definition of CNI is:</p> <p>'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:</p> <p>a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or</p> <p>b) Significant impact on national security, national defence, or the functioning of the state.</p>	<i>National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom</i>
Identification of challenges, threats and vulnerabilities in each sector covered by the CIP policy	See sector resilience plans (table above)	
Coordination of ministries, bodies and offices concerned	Civil Contingencies Secretariat (Based in the Cabinet Office)	<i>Booz & Company (2012), 'Study to support the preparation of the review of the Council Directive 2008/114/EC', Final Report.</i>
Communication with owners/operators	See table above	

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
Coordination and implementation of the CIP system at territorial level (e.g. background checks, CI inspections)	Depends on sector. CPNI publishes best practice guidelines (for instance on background checks)	https://www.cpni.gov.uk/pre-employment-screening
Other relevant aspects of national authorities involved in CIP protection	The offices involved in the national forum for CIP, include (particularly important roles) the Centre for the Protection of National Infrastructures (CPNI), the National Infrastructure Security Coordination Centre (NISCC), the National Technical Authority for Information Assurance (CESG), and the National Counter Terrorism Security Office (NaCTSO) and the Counter Terrorism Security Advisor (CTSA) network.	<i>European Critical Infrastructure Protection, Alessandro Lazari, 2014</i>
Responsibilities allocated to operators of national CI		
- Appointment of a security officer	National oversight of activities relating to the protection of critical national infrastructure are provided by a governmental forum representing all relevant departments and security agencies.	<i>European Critical Infrastructure Protection, Alessandro Lazari, 2014</i>
- Preparation of a security plan	See table above	
- Review of the plan (timing)	See table above	
- Reporting incidents	CPNI publishes incident management and reporting guidelines	https://www.cpni.gov.uk/content/incident-management
- Exchange of information	See table above	
Other distinctive features of the national CIP framework		
<ul style="list-style-type: none"> - Approach (sectoral, all-hazards) - Review of the strategy (timing) - Measures for business security (including standards) - Cybersecurity measures - Channels used for information exchange 	<p>Approach</p> <p>In the case of the UK, the matter of CIP had been already dealt with a high degree of co-operation through Private–Public partnership (PPP) combined with a consultative approach to National CIP activities. In fact, the UK does not have national CIP laws in place (with the exception of the amended Civil Contingencies Act for Gibraltar), even though it is often internationally recognised as one of the leading CIP programmes. In fact, national oversight of activities relating to the protection of critical national infrastructure is provided by a governmental forum, representing all relevant departments and security agencies. CIP related processes in the UK, even before the promulgation of the Directive, involved close co-operation between</p>	<i>European Critical Infrastructure Protection, Alessandro Lazari, 2014</i>

NATIONAL CIP FRAMEWORK		
Key dimension	Content	Source
	<p>government departments, security agencies, and infrastructure owners/operators. This collaboration is enacted through the exchange of relevant information, in the form of security advice, which not only increases the awareness of the Infrastructure Operators, but also helps them in prioritising the measures that need to be implemented. Security advices are not mandatory for the Operators, but strongly felt as “to be implemented”, thanks to the proactive culture of security and commitment that characterises the UK stakeholders involved in the Protection of national CI</p> <p>Cybersecurity</p> <p>The UK does not limit its CIP activity to the sectoral boundaries of the Directive. Indeed, sectoral actors consider all the elements of a sector, which also include ICT components. Responsibility for the protection of the CNI IT networks, data and systems from cyber-attack sits with the UK’s new National Cyber Security Centre (NCSC).</p>	<p>NCSC website: https://www.ncsc.gov.uk/information/we-work-government-and-critical-national-infrastructure</p>