

## 11. GOVERNANCE OF INFRASTRUCTURE

### Governance of critical infrastructure resilience

Natural hazards and malicious attacks against critical infrastructure systems pose grave risks to societies and economies. Recent shock events – such as the COVID-19 pandemic, Ukraine power grid cyberattack or volcanic ash cloud over Europe – illustrate how disruptions to critical infrastructure can result in cascade effects that cause substantial economic damage as well as loss of life. As the interconnectedness of supply chains and technological systems in the global economy increases, so does the vulnerability of critical infrastructure systems (e.g. those that produce and deliver electricity, gas, water and telecommunications) to shock events (OECD, 2019).

A multitude of diverse stakeholders are involved in the investment, ownership, operation and regulation of infrastructure. National strategies for critical infrastructure protection or resilience are a useful tool for governments to improve co-ordination, situation awareness and preparedness for risks across different sectors. In 2019, out of 27 OECD countries for which information is available, 24 had established such a strategy (89%). In addition, 25 out of the 27 (93%) had designated a lead institution to co-ordinate its implementation. Whether or not they had a strategy, 27 out of 30 OECD countries (90%) had established a definition of critical infrastructure in 2019, and all 32 OECD countries with available data had identified critical infrastructure sectors. Moreover, 19 out of 24 countries (79%) reported they had established national inventories of critical infrastructure assets, systems or functions (Table 11.8). These inventories confirm that a large proportion of critical infrastructure is owned or operated by the private sector (EPRS, 2021).

The design and governance of resilience measures for critical infrastructure systems is highly complex due to functional interdependencies across sectors. Resilience measures range from system redundancies and diversification of key suppliers, to asset hardening, back-up productive capacity, rapid recovery and adaptability. Among the 24 OECD countries with available data, only 12 (50%) have put in place positive or negative incentives of any kind for operators to invest in resilience; only 6 (25%) issue financial penalties in the case of prolonged service disruption. Only the United States has established government grant programmes for investments in infrastructure resilience (Figure 11.9).

#### Methodology and definitions

Data are drawn from the 2016 OECD Survey on the Governance of Critical Risks and the 2018 and 2019-20 Survey on Critical Infrastructure Resilience.

The Survey on Critical Infrastructure Resilience covered 25 OECD countries in 2019-20, and an additional 6 OECD countries in 2016. Respondents for the 2018 and 2019-20 surveys were government officials with responsibility for critical infrastructure resilience or protection at the central government level. Responses to the 2016 survey were co-ordinated by senior government officials with responsibility for disaster risk or crisis management, and included experts in critical infrastructure.

Critical infrastructure is defined in the surveys as systems, assets, facilities or networks that provide essential services for the functioning of the economy and the wellbeing of the population.

Resilience is defined as the capacity of systems to absorb a disturbance, recover from disruptions and adapt to changing conditions while retaining essentially the same function as before the disruptive shock (OECD, 2014). This definition includes the ability to withstand shocks, sustain required operations, limit the duration of service interruption, minimise recovery time, adapt to new conditions and improve systems' functionality.

#### Further reading

OECD (2019), "Policy toolkit on governance of critical infrastructure resilience", in *Good Governance for Critical Infrastructure Resilience*, OECD Publishing, Paris, <https://doi.org/10.1787/fc4124df-en>.

OECD (2014), *Recommendation of the Council on the Governance of Critical Risks*, OECD, [www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf](http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf).

EPRS (2021), *European Critical Infrastructure: Revision of Directive 2008/114/EC*, European Parliamentary Research Service, [www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS\\_BRI\(2021\)662604\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf).

#### Figure notes

Data for Colombia, Denmark, Lithuania and Slovenia are not available.

11.8. Data for Hungary are not available. Data for Belgium, the Czech Republic, Iceland, Italy, Mexico, New Zealand (only for sectors identified), the Slovak Republic and Turkey (only definition of critical infrastructure) are for 2018 instead of 2019.

11.9. Data for Belgium, the Czech Republic, Iceland, Italy, Latvia, Mexico and the Netherlands are not available.

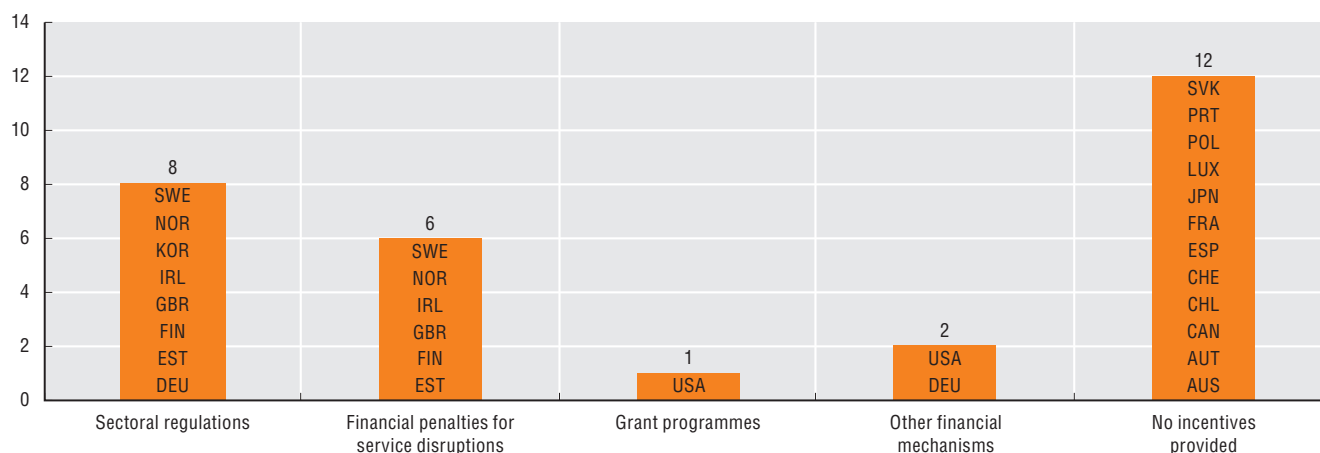
### 11.8. Critical infrastructure strategy, definition and national inventories, 2016 and 2019

	Critical infrastructure protection strategy		Definition of critical infrastructure	Sectors identified	Lead institution identified	National inventory of critical infrastructure assets, systems, functions or operators
	2016	2019	2019	2019	2019	2019
Australia	●	●	●	●	●	●
Austria	●	●	●	●	●	●
Belgium	...	...	●	●	●	...
Canada	●	●	●	●	●	●
Chile	...	●	○	●	●	●
Czech Republic	...	●	●	●	●	...
Estonia	●	●	●	●	●	●
Finland	●	●	●	●	●	○
France	●	●	●	●	●	●
Germany	●	●	●	●	●	●
Greece	...	○	○	●	●	○
Iceland	...	●	...	●	...	...
Ireland	●	●	●	●	●	○
Israel	●	●	●	●	●	●
Italy	...	○	○	●	○	...
Japan	●	●	●	●	●	○
Korea	●	●	●	●	●	●
Latvia	○	●	●	●	●	●
Luxembourg	●	●	●	●	●	●
Mexico	...	...	●	●	...	...
Netherlands	●	●	●	●	●	●
New Zealand	...	...	●	●	...	...
Norway	○	●	●	●	●	●
Poland	●	●	●	●	●	●
Portugal	○	○	●	●	○	●
Slovak Republic	...	...	...	●	...	...
Spain	●	●	●	●	●	●
Sweden	●	●	●	●	●	○
Switzerland	●	●	●	●	●	●
Turkey	...	...	●	●	...	...
United Kingdom	●	●	●	●	●	●
United States	●	●	●	●	●	●
<b>OECD Total</b>						
● Yes	19	24	27	32	25	19
○ No	3	3	3	0	2	5
... Missing	10	5	2	0	5	8

Source: OECD (2016) Survey on the Governance of Critical Risks; OECD (2018 and 2019-20) Survey on Critical Infrastructure Resilience.

StatLink <https://doi.org/10.1787/888934258990>

### 11.9. Incentives for critical infrastructure operators to invest in critical infrastructure resilience, 2019



Source: OECD (2019-20) Survey on Critical Infrastructure Resilience.

StatLink <https://doi.org/10.1787/888934259009>



**From:**  
**Government at a Glance 2021**

**Access the complete publication at:**  
<https://doi.org/10.1787/1c258f55-en>

**Please cite this chapter as:**

OECD (2021), "Governance of critical infrastructure resilience", in *Government at a Glance 2021*, OECD Publishing, Paris.

DOI: <https://doi.org/10.1787/ee7bc35f-en>

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at <http://www.oecd.org/termsandconditions>.