



REPUBLIC OF SLOVENIA  
COURT OF AUDIT

# AUDIT REPORT

## Efficiency of ensuring cybersecurity in the Republic of Slovenia

**Performance audit**

Audit period: 1 January 2016 to 30 September 2019



# Cybersecurity

is the ability to protect, secure and defend cyberspace from cyber threats, incidents and attacks.

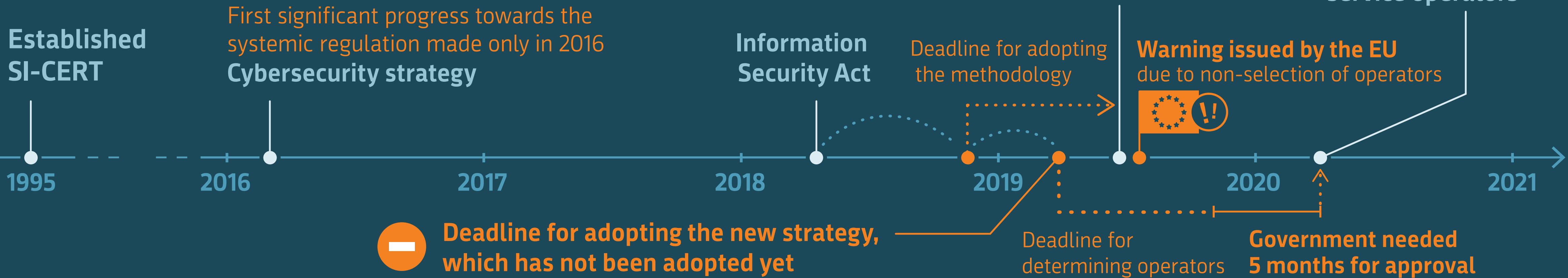
## Cybercrime causes considerable damage in various fields



How does the Republic of Slovenia ensure cybersecurity?

Audited was efficiency of the Government, the Government Office for the Protection of Classified Information and the Ministry of Public Administration in ensuring cybersecurity



# Activities for regulating the field



## Achieving objectives set in the cybersecurity strategy adopted in 2016




 **Safety of citizens in cyberspace**

-  The State failed to carry out awareness-raising programmes for citizens despite warnings of the EU
-  New strategy was not adopted

 **Public safety's cybersecurity and fighting cybercrime**

-  Understaffing
-  Resources not provided
-  New strategy not adopted

 **Ensuring safe operation and availability of key information and communication technology systems in the event of major natural disasters and accidents**

-  Understaffing
-  Lack of instructions and methodologies

 **Cybersecurity in the economy**

-  Cybersecurity Section at the Chamber of Commerce and Industry of Slovenia
-  Conferences organized
-  Security operations centres (SOC) established

 **Strengthening national cybersecurity by international cooperation**

-  Participating in international exercises, committees, working bodies and associations

# OPINION OF THE COURT OF AUDIT



**Ensuring cybersecurity** in the period from 1 January 2016 to 30 September 2019 **was not efficient** despite intensified activities in 2019.

## Demands

## Recommendations

GOVERNMENT



plan of activities for **adopting new strategy**



plan of activities for **awareness-raising programmes**



plan of activities for **introducing cybersecurity in education system**



**should define, harmonise and consistently apply terminology** (cyber/information security), thereby following the EU trends



**should unify/streamline parameters for each disruption and incident** when providing essential service

MINISTRY OF PUBLIC ADMINISTRATION



**to reinforce staffing and financing** in the field of cybersecurity



**to start carrying out risk assessment** pertaining to critical infrastructure operations in public administration



**should make the services of CSIRT of public administration bodies available also to other national authorities**



should provide institutions with **instructions for reporting the occurrence of incidents**