



EU-SCICF

#CYBERSECURITY #ICT #COORDINATION #EUFINANCE

# THE SYSTEMIC CYBER INCIDENT COORDINATION FRAMEWORK: EU-SCICF

The Systemic Cyber Incident Coordination Framework, also known as EU-SCICF, is set up to facilitate communication and coordination among EU authorities and to liaise with other key stakeholders at international level. The framework will focus on cyber incidents posing a risk to financial stability.

## WHAT KIND OF INCIDENTS ARE COVERED BY THE EU-SCICF?

The EU-SCICF will cover major cross-border information and communication technologies (ICT) related incidents or related cyber threats having a systemic impact on the Union’s financial sector.

## WHAT IS THE ENVISIONED STRUCTURE?



## HOW DOES THE EC-SCICF WORK?

The participating members will be alerted and will share information on potential systemic cyber incidents or threats. When a systemic risk materialises, the EU-SCICF will serve as forum for relevant authorities to communicate and coordinate on any needed action and on the use of tools to counter the crisis from a macroprudential perspective.

## HOW WILL IT BE SET UP?

### ORGANISATION



- EU-SCICF Secretariat
- Supportive tools
- Governance and arrangements

### NON-CRISIS MODE



- Awareness
- Development
- Crisis mode testing and maintenance

### CRISIS MODE



- Sharing information
- Discussion on impact, response and tools
- Identifying areas of alignment

The set-up is subject to the outcome of the Report to be drafted by the European Commission based on the Recommendation.