The Systemic Cyber Incident Coordination Framework: EU-SCICF

What is 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, in case of cyber incidents posing a risk to financial stability.

What kind of incidents are covered by the EU-SCICF?

Major cross-border information and communication technologies (ICT) related incidents or related cyber threats potentially having a systemic impact on the Union’s financial sector.

What is the envisioned composition?

- National Authorities
- Supervisory
- Macroprudential
- Resolution

How does the EU-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.

Set-up

<table>
<thead>
<tr>
<th>Non-crisis mode</th>
<th>Crisis mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>Sharing information</td>
</tr>
<tr>
<td>Development</td>
<td>Discussion on impact, response and tools</td>
</tr>
<tr>
<td>Crisis mode testing and maintenance</td>
<td>Identifying areas of alignment</td>
</tr>
</tbody>
</table>

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