FIN-FSA
FINANCIAL SUPERVISORY AUTHORITY

Publications and press releases

Press release 4 March 2022

Enhanced monitoring of situation in financial sector, sanctions enforcement and cyber risk preparedness

The Financial Supervisory Authority has enhanced its monitoring of the situation in the financial sector in an operating environment where Russia's invasion of Ukraine and the sanctions imposed on Russia are creating uncertainty.

The Finnish financial sector is stable and therefore faces the changed situation from a good foundation. There are no indications to date that the events have adversely impacted to a significant degree financial sector activities and companies' access to financing in Finland. At this stage, the Financial Supervisory Authority (FIN-FSA) is drawing its supervised entities' attention particularly to enforcement of sanctions and preparedness for cyber risks.

Compliance with sanctions as part of supervised entities' activities

The European Union and the G7 countries have imposed sanctions on Russia affecting, amongst others, Russian banks as well as Russian companies and private individuals. As part of the sanctions, Russian banks are excluded from the international SWIFT payment system. In addition, the sanctions more widely restrict transactions with the Central Bank of Russia and the export of certain products and technologies to Russia.

EU sanctions are directly binding on all supervised entities of the FIN-FSA, and compliance with them is important from the standpoint of supervised entities' risk management. The FIN-FSA urges supervised entities to ensure that their systems and instructions for complying with sanctions are up to date. Cooperation with customers to ascertain the basis for payments and the parties involved is particularly important.

Identifying and responding to cyber attacks

The escalation of the international security situation also increases the possibility of cyber attacks against financial sector actors and service providers. The FIN-FSA urges supervised entities to ensure that their protective measures against various cyber threats are up to date.

It is important for supervised entities to be able to detect security breaches in ICT environments and to react immediately to cyber incidents and disruptions. ICT environment risk assessments, risk management measures and technical protections must be kept up to date. In addition, business- and system-specific continuity plans and cyber-threat protection must be kept up to date also in outsourced services and throughout the supply chain.

The FIN-FSA also encourages supervised entities to monitor National Cyber Security Centre situation reports and information, and reminds supervised entities that they must immediately notify the FIN-FSA of significant disruptions and faults in services as well as security breaches and cyber attacks.

The FIN-FSA will report in more detail on its situation assessment of the financial sector and actions taken at a press conference to be held on Tuesday, 15 March at 10 a.m. The invitation to the event will be published later. An open link enabling the public to follow the event will also be published later on the FIN-FSA website.

See also

- Supervision release on sanctions enforcement
- Supervision release on cyber risk preparedness