Problem tree

Drivers

Problems

Consequences

Regulatory and supervisory divergent approaches and gaps

Increased reliance on ICT TPPs

Highly digitalised and interconnected financial sector

1. Fragmentation in managing ICT risks

Lack of specific requirements on ICT risks

Disparity of ICT risk requirements across financial sectors

2. Ineffective reporting of and limited awareness about threats and incidents

Lack of incident reporting requirements for some financial institutions

Multiple incident reporting requirements for some financial institutions

Insufficient trust to share threat intelligence and uncertainty over legal compliance when sharing

3. Limited and uncoordinated testing

Overlapping testing for some financial institutions

Lack of testing for some financial institutions

4. ICT third party risk

Contractual limitations / gaps in written agreements with ICT TPPs

No coherent oversight framework for ICT TPPs

Insufficient regulatory response to increased levels of ICT risks

Incomplete view over the frequency and significance of incidents

Complex, inconsistent and overlapping reporting obligations

Insufficient information sharing and cooperation on threat intelligence

Fragmentation due to multiple testing and no cross-border recognition of results

Insufficient assessment of preventive and resilience capabilities

Challenges for financial institutions to assure compliance with the regulatory framework

Unmonitored ICT TPPs risks

Incomplete Single Rulebook on digital dimension

Financial sector stability and integrity at risk

Insufficient/unequal protection of consumers and investors

Excessive administrative burden and limited supervisory effectiveness

Out of scope:
Data breach notifications under GDPR

22