Deloitte.

Regulatory News Alert

CSSF sets telework requirements for financial sector

14 April 2021

Scope

On 9 April 2021, the Commission de Surveillance du Secteur Financier (CSSF) published Circular 21/769 regarding governance and security requirements for supervised entities to perform tasks or activities through telework (the "Circular").

This Circular applies to all CSSF supervised entities, including their branches in Luxembourg or abroad, as well as Luxembourg branches of entities originating from another Member State or outside the European Economic Area. No approval is required from the CSSF to implement telework solutions.

Objectives

The Circular sets out the requirements of CSSF supervised entities using teleworking solutions in a non-pandemic situation. These requirements provide additional guidance on the governance and security areas that must be followed when implementing teleworking solutions for employees.

The Circular highlights what is required of the supervised entities' central administration and the responsibility of the board of directors. It also reminds these entities that they must guarantee the ongoing performance of critical activities at all times.

The internal organization and the internal control framework shall ensure the following:

- Risk analysis is performed to identify the inherent risks in implementing teleworking, mitigating controls are implemented, and the analysis and appropriateness of controls are reviewed regularly;
- The board of directors (or the body that represents the supervised entity) defines a telework policy that determines:
    - The business units that are allowed to use telework;
    - The activities to be performed onsite;
    - The minimum number of staff required at the premises;
    - The working hours allowed for telework;
    - The monitoring controls;
    - The physical meetings to be held at the premises; and
    - The measures with regards to compliance with confidentiality and data protection regulations;

- The supervised entity maintains evidence related to the compliance monitoring of the telework policy; and
- Internal control functions (e.g., compliance, risk and internal audit) include a teleworking review in their pluri-annual work program and, in their annual summary report, include any significant operational incidents regarding telework, as well as a short statistic on the use of telework during the year.

For the purpose of the Circular, persons put at the supervised entity's disposal through a third-party employer contract are also considered staff members.

Supervised entities' requirements related to information and communications technology (ICT) and security risks

1. Policies and procedures: define the high-level principles that apply to protect the confidentiality, integrity and availability of the entities' data and ICT systems.
2. Risk awareness: ensure all staff members are aware of teleworking risks and best practices, including organizational and technical risks.
3. Access rights: review and adapt access rights management procedures and the accesses granted for telework in line with the entity's risk assessment and telework security policy.
4. Remote access devices: ensure that the security of devices used to connect remotely to the supervised entity's ICT systems is controlled. ICT teams shall not be able to access and administer ICT systems using private devices.
5. Telework infrastructure: ensure that a high level of security and availability of the telework infrastructure is maintained over time and the various components are properly functioning, secured and closely monitored.
6. Security of connections: ensure that data in transit is secured and implement two-factor authentication (2-FA) when connecting remotely to systems (a strong 2-FA procedure must be implemented for critical activities).
7. Review of the communication chain security: an independent security control function shall review, before the go-live and then regularly, the proper functioning of the communication chain from the remote device to the corporate infrastructure, as well as the effectiveness of the implemented security measures.
8. Technology watch: implement a solid monitoring process to be quickly informed of new security vulnerabilities and apply the necessary corrections promptly.
9. Logging: implement a sound logging process to ensure all teleworking connections and relevant technical information are logged and protected from unauthorized modification or deletion.

What is next?

The Circular does not apply during pandemics (for example, COVID-19) or other exceptional circumstances that have a similar impact on general working conditions. It enters into force on 30 September 2021. The CSSF will review its application within 12 months after it enters into force to address potential abuses or any other shortcomings.

Deloitte.

How can Deloitte help?

Deloitte can help organizations improve their ICT security and risk management practices' maturity by assessing, designing, and implementing:

- Cyber risk services—assistance for the design, selection, implementation and assessment of security controls pertaining to your teleworking environment, including services like penetration tests of remote access infrastructure, information security awareness training, and vulnerability watch.

- ICT regulatory compliance assessment—gap assessment against the regulatory requirements.

- ICT and security risk assessment—ICT and security risk assessment in the context of digital initiatives or major ICT changes, tailored to the organizations' risk profile and integrated into the organizations' risk management framework.

- ICT internal audit—outsourcing or co-sourcing assistance to support the internal audit functions of your institution with the execution of ICT internal audit missions.

Deloitte's RegWatch service helps you stay ahead of the regulatory curve to better manage and plan for upcoming regulations.

Your Contacts

Subject matter specialists

Irina Hedea
Partner – Risk Advisory
Tel: +352 45145 2944
ighedea@deloitte.lu

Laureline Senequier
Director – Risk Advisory
Tel: +352 45145 4422
lsenequier@deloitte.lu

Stephane Hurtaud
Partner – Risk Advisory
Tel: +352 45145 4434
shurtaud@deloitte.lu

Maxime Verac
Director – Risk Advisory
Tel: +352 45145 4258
mverac@deloitte.lu

Regulatory Watch Kaleidoscope service

Simon Ramos
Partner – IM Advisory & Consulting Leader
Tel: +352 45145 2702
siramos@deloitte.lu

Benoit Sauvage
Director – Risk Advisory
Tel: +352 45145 4220
bsauvage@deloitte.lu

Jean-Philippe Peters
Partner – Risk Advisory
Tel: +352 45145 2276
jppeters@deloitte.lu

Marijana Vuksic
Senior Manager – Risk Advisory
Tel: +352 45145 2311
mvuksic@deloitte.lu

Deloitte Luxembourg
20 Boulevard de Kockelscheuer
L-1821 Luxembourg
Grand Duchy of Luxembourg

Tel: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu

Designed and produced by MarCom at Deloitte Luxembourg