

MEMO# 33454

April 20, 2021

Luxembourg CSSF Issues Teleworking Circular

[33454]

April 13, 2021 TO: Global Operations Advisory Committee
ICI Global Information Security Officer Committee - London
ICI Global Investing Subcommittee
ICI Global Regulated Funds Committee
International Compliance Advisory Committee RE: Luxembourg CSSF Issues Teleworking Circular

On April 9, Luxembourg's Commission de Surveillance du Secteur Financier (CSSF) issued a circular detailing the governance and security requirements for entities under the supervision of the CSSF to perform tasks or activities through telework (Circular).[\[1\]](#) The Circular enters into force on September 30, 2021, and applies only under normal general working conditions. It does not apply under pandemic situations (such as COVID-19) or in case of other exceptional circumstances having a comparable impact on the general working conditions. The CSSF will review the Circular within 12 months after its entry into force and update it as needed.

The key provisions of the Circular are briefly described below.

Scope

The Circular applies to all entities supervised by the CSSF (supervised entities), including their branches in Luxembourg or abroad. It also applies to Luxembourg branches of entities originating from outside the European Economic Area (EEA).

Telework

The Circular specifies criteria that must be met in order for a work relationship to qualify as telework:

- work must be delivered by means of information and communication technologies based on a previous approval by the employer; and
- work must be performed on a regular or occasional and voluntary basis and within the defined working hours at a predetermined place that is different from the employer's premises.

Supervised entities must have rules in place to define from where telework is allowed, and such rules must be documented and followed.

General Principles

The Circular lays out a handful of general principles that broadly govern the ability of a supervised entity to offer telework.

- A supervised entity is required to maintain at all times a robust central administration (described below) in Luxembourg and to maintain sufficient substance at its premises, also in order to allow it to deal with emergencies and other time-critical issues in due time.
- A supervised entity is required to assess to what extent it allows its staff members to work remotely.
- Telework shall, in no case, jeopardize the regular operational functioning of a supervised entity.
- Telework is organized under the ultimate responsibility of the supervised entity's Board of Directors.
- Approval by the CSSF is not required to implement telework.

Baseline Requirements

To supplement the general principles, the CSSF has specified certain baseline requirements for the use of telework arrangements.

- A “robust central administration” (which is required to be maintained at all times) consists of a “decision-making center” and an “administrative center.” These must include sufficient staff with the necessary skills, knowledge, and expertise as well as the technical and administrative infrastructure to exercise its function or activity.
- Staff members must be able to return to the supervised entity's premises on short notice in case of need.
- These specific criteria must be followed when using telework:
 - The number of staff of a supervised entity that may telework at the same time must comply with the central administration requirements.
 - The amount of their normal working time individual staff members are allowed to telework should be limited.
 - At least one authorized manager must be on-site at the head office at all times and key functions must be sufficiently represented every day in the premises and permanently guarantee the adequate functioning of the activities and controls as well as proper decision-taking.
 - The supervised entity must be able to demonstrate that the head office remains at all time the “decision-making center.”
 - The requirement to guarantee the ongoing performance of critical activities must be adequately considered in the implementation of the telework policy.

Internal Organization and Internal Control Framework

The Circular imposes certain additional obligations with respect to the internal control framework for telework.

- The supervised entity must conduct a risk analysis to identify the inherent risks in implementing teleworking, in particular the operational risks, including legal, information and communication technology (ICT), compliance and reputational risks.
- Risk identification and mitigation measures must be adequately formalized.
- The Board of Directors is required to define the supervised entity's telework policy and the limits under which telework will be allowed; it must review the policy annually.
- The existing management information system and control environment of a supervised entity cannot be altered while allowing tasks to be performed via telework.

- The supervised entity must maintain evidence enabling the CSSF to monitor the supervised entity's compliance with the Circular.

Requirements Related to ICT and Security Risks

The Circular also contains a number of requirements related to ICT and security risks. The CSSF notes that although all of the requirements apply in principle to all supervised entities, in implementing the requirements, supervised entities should take into consideration the principle of proportionality by considering the nature, scale, and complexity of their activities.

The Circular provides that a supervised entity's security policy must define the high-level principles and rules applicable in the context of telework, to protect the confidentiality, integrity, and availability of the entity's data and information and ICT systems. The telework security policy must be complemented at an operational level by adapting existing user procedures as needed.

The Circular then addresses the CSSF's expectations regarding various aspects of ICT and security, including:

- staff member risk awareness;
- access rights management procedures;
- remote access devices and the use of private owned devices;
- telework infrastructure;
- security of connections;
- review of communication chain security;
- technology monitoring; and
- logging process.

Eva M. Mykolenko
Associate Chief Counsel - Securities Regulation

endnotes

[1] The Telework Circular is *available at* https://www.cssf.lu/wp-content/uploads/cssf21_769eng.pdf?utm_campaign=email-210409-59e30.