

Implementation of EBA Guidelines in Luxembourg

# CSSF CIRCULAR 20/750 ICT & SECURITY RISK MANAGEMENT

Obligation to review key aspects of your IT environment

## Context

On 25 August 2020, the Commission de Surveillance du Secteur Financier (CSSF) published Circular 20/750 on requirements regarding information and communication technology (ICT) and security risk management, implementing in Luxembourg the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04).

Scope of application (as per EBA Guideline):

- ▶ banks
- ▶ investment firms
- ▶ payment and electronic money institutions
- ▶ extended the scope to include both specialised and support PSFs (in Luxembourg).

## MAIN OBJECTS

- ▶ Address the risks and adverse impacts on the supervised entities' operations
- ▶ Establish a consistent approach to the mitigation and management of ICT and security risks
- ▶ Provide a better understanding of CSSF's expectations on the management of ICT & security risks

## MAIN PROVISIONS



## KEY REGULATORY ASPECTS

- ▶ Repeals Circular CSSF 19/713 on security measures for operational and security risks of payment services under PSD2
- ▶ Updates Circular CSSF 12/552 on Central administration, internal governance and risk management, notably the requirements related to the IT function (section 5.2.3) and the role of IT function in the 3 lines of defense model (Part II Chapter 2)
- ▶ Additional CSSF Risk Reporting obligations for payment service providers (PSP):
  - Credit institution:  
As soon as possible after the closure of the financial year and no later than 30 April of each calendar year
  - E-money & payment institutions:  
No later than the last day of the third month after the closure of the financial year

## HOW CAN BDO HELP YOU?

- ▶ **BDO Luxembourg** will help organisations improve their ICT risk management framework which includes:
  - ▶ **ICT and security risk assessment** – gap assessment against the regulatory requirements outlined in the Circular 20/750
  - ▶ **Optimised IT Governance framework** - based on identified gaps from the assessment BDO may help you with a remediation of gaps. Depending on a gap, BDO has a catalogue of services which may help you to stay compliant with the CSSF circular 20/750:
    - IT Strategy & IT Governance
    - Information/Cyber Security Awareness Training
    - Information Security Policy BCP/DRP
    - Security Testing (e.g. Vulnerability & Threat assessment, Penetration testing etc.)
    - Incident Response Simulation
    - IAM/PAM review
    - Social Engineering (e.g. Simulation of a phishing attack or physical security test)
  - ▶ **ICT and security risk re-assessment** – regular re-assessment against the regulatory requirements outlined in the Circular 20/750 after a remediation of gaps
  - ▶ **Control monitoring program** - our monitoring program helps to manage and plan upcoming modifications and new regulations



**FOR FURTHER INFORMATION, FEEL FREE TO CONTACT OUR EXPERTS:**




**Benoît Wtterwulghe**

Partner

+352 45 123 795

[benoit.wtterwulghe@bdo.lu](mailto:benoit.wtterwulghe@bdo.lu)

► Follow us 

► [www.bdo.lu](http://www.bdo.lu)

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad guidance only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication herein without obtaining specific professional advice. Please contact the appropriate BDO Member Firm to discuss these matters in the context of your particular circumstances. No entity of the BDO network, nor the BDO Member Firms or their partners, employees or agents accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it. BDO is an international network of public accounting firms, the BDO Member Firms, which perform professional services under the name of BDO. Each BDO Member Firm is a member of BDO International Limited, a UK company limited by guarantee that is the governing entity of the international BDO network. Service provision within the BDO network is coordinated by Brussels Worldwide Services BVBA, a limited liability company incorporated in Belgium with its statutory seat in Brussels. Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BVBA and the member firms of the BDO network is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BVBA and/or the member firms of the BDO network. BDO is the brand name for the BDO network and for each of the BDO Member Firms. © 2021 BDO Advisory. All rights reserved.