Deloitte.

Regulatory news alert

Regulatory key points for credit institutions and PSFs

5 October 2016

CSSF Annual Report 2015

Dear All,

Following the publication of the CSSF Annual Report 2015, you will find below a summary of key attention points for credit institutions, PSFs and the supervision of information systems.

Credit institutions

Main risks on Luxembourg banking sector remain unchanged, i.e.:

- Sovereign risks
- Risks linked to residential real estate in Luxembourg
- Risks linked to intra-group exposures
- Risks related to the activity of depositary bank
- Profitability risk
- Other risks (financing and asset encumbrance)

The CSSF included opinions and recommendations regarding some of these risks, which are summarized below.

Risks linked to residential real estate in Luxembourg

Pursuant to point 221 of CSSF Circular 12/552. The CSSF reminds that banks are required to apply a reasonable safety margin to absorb an increase in interest rate.

The CSSF considers that capital requirements should not represent less than 1.6% of the total mortgage loan outstanding when they use the internal model-based approach.

The CSSF expects that credit institutions have information systems fulfilling CSSF Circular 12/552 requirements, allowing the monitoring of key prudential ratios including loan-to-value ratio and the borrower's reimbursement capacity.

Deloitte.

Supervision of interest rate risk according to CSSF Circular 08/338

The CSSF reminds that according to Article 30(4) of the CSSF regulation N°15-02, measures should be taken if this ratio fall below -20%.

Supervision of operational risk

Regarding capital requirements allocated to operational risk, the CSSF expects that the capital is consistent with the business and risk profile of the bank. The analyses must be reflected in the ICAAP process as required in Article 18 of CSSF Regulation N° 15-02 on the supervisory review and evaluation process.

Regarding the risks linked to business conduct, the CSSF expects an irreproachable deontological approach from Luxembourg banks with a view to respect and protect the reputation of Luxembourg financial centre.

Intervention in commercial policies

Within the process of prudential supervision laid down in CSSF Circular 07/301, the CSSF reminds that banks shall maintain a sound relation between their risk exposures and their capacity to bear these risks.

Long-form reports

The CSSF reminds that credit institutions supervised on a consolidated basis are required to submit, on a yearly basis, a consolidated long-form report and individual long-form reports for each subsidiary included in the consolidation and carrying out an activity of the financial sector.

Supervision on a consolidated basis

For those entities that remain subject to its consolidated supervision, the CSSF reminds it pays special attention to the “group head” function set up at the Luxembourg institution under its consolidated supervision. It takes a particular interest in the way the Luxembourg parent company communicates its policies and strategies to its subsidiaries as well as in the controls set up at the Luxembourg parent undertaking in order to monitor the organisation and activities of the subsidiaries, and their exposures.

Review of risk management models

For the banks that have opted for the AMA approach, the CSSF reminds it requires an active and reactive management of operational risks in Luxembourg. Beyond the application of a model generally set by the parent undertaking, the CSSF expects that within the Luxembourg entity, the capital allocated to operational risks is duly analysed, argued and justified as to its adequacy for the entity’s operation in Luxembourg. The capital allocated to operational risks through an internal process under an AMA approach should fully and accurately reflect the entity’s specific risk profile.

PSFs

Investment firms

Capital base

The CSSF reminds that subordinated loans or profits for the current financial year shall not be taken into account for the determination of the minimum capital base of a PSF (Pursuant to Article 20(5) of the Law of 5 April 1993 on the financial sector).

Specialised PSF

Capital base

The CSSF reminds that, pursuant to Article 20(4) of the Law of 5 April 1993 on the financial sector, own funds must be permanently available to the PSF and invested in its own interest. Moreover, the legislator indicated in the comment to this Article that "[...] the first requirement aims at ensuring that the capital base is neither invested in participations nor blocked for credits granted. The second requirement aims at ensuring that the capital base is used in the interest of the PSF and of its clients and not in the interest of its shareholders or its group."

In this context, the CSSF points out that the funds invested in a participation shall be deducted from the capital base of the PSF, where applicable.

Furthermore, the CSSF reminds that the payment of interim dividends, in accordance with the provisions of the Law of 10 August 1915 on commercial companies, shall be deducted from equity and must be considered for the determination of the PSF capital to respect the minimal amount required.

Compliance of the day-to-day management

The CSSF would like to reiterate the importance of being in compliance with the legal and regulatory provisions in force with respect to day-to-day management of PSF. Indeed, based on the two-man management principle, the entity's day-to-day management shall be handled by at least two delegates. This principle aims at ensuring involvement and effective presence within the PSF for the purpose of mutual control and collegial decision making. The delegates of the day-to-day management shall justify the same level of accountability and autonomy and are directly and severally liable for the effective, sound and prudent management skills with respect to all the activities pursued and risks related.

Loan-granting activity

The CSSF reminds that, due to prudential considerations, a specialised PSF cannot grant loans to its shareholders, managers, employees or third parties. Indeed, it is essential that, on the one hand, all participations in the authorised capital of a PSF is financed through own funds and not through borrowed funds. The granting of advances and loans to shareholders, however, results in the return of the authorised capital to the shareholders. On the other

hand, the CSSF considers that granting loans does not fall within the context of the usual business of a PSF, except for professionals authorised to grant loans to the public pursuant to Article 28-4 of the Law of 5 April 1993 on the financial sector.

Support PSF

Segregation of PSF and non-PSF activities within the same legal entity

The CSSF has already indicated that such separation is feasible on a condition that non-PSF activities do not impact PSF activities. Financial obligations, anti-money laundering and terrorist financing and client due diligence (KYC) cannot be separated and have to cover all the activities.

Relaxation of geographical constraints

More and more banks and investment firms relocate their IT abroad. Support PSF can use a processing centre abroad or act abroad covered by the support PSF status. The CSSF indicated that the use of a branch is already an option since these branches, without separate legal personality, remain under CSSF's supervision. Discussion is under way on the various cases which could be accepted by the CSSF and on the principles and requirements to be respected by support PSF with regard to the substance, control and central administration in Luxembourg.

Merger of both status of IT systems operators

Having been consulted on the possibility of merger of both status of IT systems operators governed by Articles 29-3 and 29-4 of Law of 5 April 1993 on the financial sector, the CSSF has given a positive opinion and suggest to reduce capital requirement (from EUR 370.000) to EUR 125.000 in order not to penalise the smallest providers.

FATCA and CRS report

The CSSF decided that the compilation and submission of FATCA and CRS reports to tax authorities on behalf of Luxembourg financial services professionals may be deemed administrative services inherent to the activity of these financial professionals, requiring then the status of financial services administration agent as referred to in Article 29-2 of the Law of 5 April 1993 on the financial sector.

Reminder to support-PSFs: cloud services' presentation to the CSSF

The CSSF reminds that support-PSF who put in place a cloud offer (even outside the financial sector) are supposed to present it to the CSSF both on a commercial and technical perspective.

Support PSFs which have not yet presented their cloud solution to the CSSF are therefore invited to present it without delay.

Deloitte.

SUPERVISION OF INFORMATION SYSTEMS – PRACTICAL CONSIDERATIONS

Usage of tracking tools and traffic analysis of internet sites of entities

In conformity with CSSF Circular 12/552, all information which is transmitted to a third party other than a support-PSF or a Luxembourg credit institution and which could be linked to private users in order to track their behaviour shall first be anonymized.

The CSSF reminds that information such as IP address should not be logged by the host website if it is not a support-PSF.

CSSF Circular 15/611: externalization of systems that allow the compilation, distribution and consultation of documents of the management board/strategic council

The CSSF calls attention of the entities to the potentially sensitive data stored in a system hosted and managed by an external service provider. The CSSF stresses that it is the responsibility of the entities not to disclose information deemed confidential in the meaning of Article 41 of the Law of 5 April 1993 on the financial sector to any third party such as a service provider, unless it falls within the scope of Article 41(5) of the aforementioned law.

The CSSF considers that the entities are required to perform their own due diligence, covering a detailed assessment of the security level of the service provider. Indeed, these service providers are likely to store information presenting high value by the nature of information (sensitive data) or their volume (concentration of data within the same system) could represent a strategic target for hackers and fraudsters.

Outsourced data-extraction in the event of bankruptcy of a subcontractor

The CSSF calls attention of supervised entities on the fact that local regulation applied in other countries may not provide the same protection as in Luxembourg. Hence, in case of outsourcing to a company outside Luxembourg, the entity who outsources must ensure that the local legal framework will allow it to retrieve data in the event of bankruptcy of the subcontractor.

Cloud outsourcing: reminder of current requirements

The CSSF points out that the regulatory requirements in case of IT outsourcing (cloud or not) under CSSF Circular 12/552 and 05/178 are still in force. Likewise, the prudential principles regarding the use of cloud computing, as detailed in CSSF annual report of 2011 remain valid. It is also stressed that a supervised entity who wishes to use a cloud run by a non-support PSF must first submit an application to the CSSF.

Data protection: privacy by design and need-to-know principles

The CSSF points out to supervised entities that the data protection including protection of personal data for which they are responsible is an objective to be taken into account as from the conception of the IT design developed in-house (privacy by design) or in the assessment

of the software to be acquired. Institutions must also ensure that access to data is only on a need-to-know basis.

Cybercrime

The CSSF calls attention of financial institutions on the importance of patch management in the fight against cybercrime. Several concordant sources (regulator, solution provider, penetration tests) reveal the existence of known security flaws for which patches have been available since a long time. These flaws represent an entrance door for hackers who can sometimes stay months in the systems undetected. Although this is the responsibility of financial institutions to perform risk analysis, such situation is unacceptable. The CSSF strongly recommends institutions to patch existing flaws that are still active.

In general, institutions have to establish a monitoring to be quickly informed of new security flaws and a patch management procedure allowing their correction within a short notice when they are likely to have a significant impact on IT systems. The CSSF considers that internal audit must incorporate the monitoring process review and the patch management in the multi-annual audit plan.

Should you have any question, please contact **LU, Regulatory Watch**.

Best regards,

Your contacts

Martin Flaunet
Partner | Banking Leader
Tel: +352 451 452 334
mflaunet@deloitte.lu

Stéphane Césari
Partner | PSF Leader
Tel +352 451 454 487
scesari@deloitte.lu

Anne-Françoise Liégeois
Director – Regulatory watch
Tel: +352 451 452 536
afliegeois@deloitte.lu

Deloitte Luxembourg
560, rue de Neudorf
L-2220 Luxembourg

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

Designed and produced by MarCom at Deloitte Luxembourg