Deloitte.

Regulatory News Alert

CSSF Circulars 17/655, 17/656 and 17/657 on IT outsourcing

29 May 2017

On 17 May 2017, the CSSF published four circulars on IT outsourcing.

The first circular published, Circular 17/654 on cloud computing, was much expected and we presented it in one of our earlier alerts.

The three other circulars contained updates to the existing circulars on more traditional forms of IT outsourcing (i.e. circulars 05/178, 06/240 and 12/552) aiming to:

- Reflect the introduction of a circular specific to IT outsourcing arrangements based on a cloud computing infrastructure
- Harmonize the requirements on outsourcing across the financial sector
- Prepare for bill of law 7024, which is expected to frame communication of confidential data under outsourcing arrangements via the modernization of the professional secrecy requirements set forth in the laws on the financial sector, payment services, and insurance sector

Circular 17/655 updating Circular 12/552

The second circular published, Circular 17/655, updates Circular 12/552 on the central administration, internal governance and risk management. The circular applies immediately to all credit institutions, investment firms and professionals performing lending operations.

As noted above, Circular 17/655 integrates the introduction of Circular 17/654 on cloud computing and paves the way for bill of law 7024. In particular, the circular:

- Reaffirms that the board of directors' **guiding principles** shall address outsourcing, including **IT outsourcing** arrangements which may or may not be based on cloud computing
- Requires institutions to implement (i) a **security monitoring process** allowing to be informed promptly of new vulnerabilities and (ii) a **patch management procedure** allowing timely correction of significant vulnerabilities (the internal audit function will assess these as part of its multi-year audit plan)
- Allows to outsource IT systems management/operations to **any IT provider abroad** (whereas past circulars required to source these services from a parent group entity) provided the IT systems do not include any readable confidential data on customers; otherwise, the circular refers to the institution's legal obligations concerning customers consent and

notification (i.e. paving the way for changes foreseen in bill of law 7024) and emphasizes the need to comply with personal data protection regulations

- Increases requirements on confidentiality and integrity of data and systems; in the frame of outsourcing arrangements, accesses to data and systems shall be managed according to the **"need to know"** and **"least privilege"** principle

Circular 17/656 replacing Circular 05/178

The third circular published, Circular 17/656, replaces Circular 05/178 on IT outsourcing. By doing so, the circular harmonizes the requirements for outsourcing across the financial sector, as well as clarifies IT outsourcing requirements for Support PSFs. The circular applies immediately to all electronic money institutions, payment institutions, as well as professionals of the financial sector other than investment firms.

The first chapter of Circular 17/656 aligns in style and contents on sub-chapter 7.4 "outsourcing" of Circular 12/552 which applies to credit institutions and investment firms, except for certain parts on outsourcing of IT management/operations and hosting, which shall not apply to Support PSFs covered by art. 29-3, 29-4, 29-5 and 29-6 of the Law of 5 April 1993 on the financial sector, as amended.

The second chapter clarifies IT outsourcing requirements for Support PSFs in the following circumstances:

- Support PSFs and their branches covered by art. 29-3 and 29-4 which recourse to IT outsourcing to their parent group
- Support PSFs and their branches which have recourse to IT outsourcing of their IT for internal usage to a third party
- Branches of Support PSFs which offer services to clients of their host countries based on IT infrastructure which is installed in the host countries and which could be outsourced to a third party
- Branches of Support PSFs which offer IT management/operations services to their head office

Circular 17/657 updating Circular 06/240

The fourth and last circular published, Circular 17/657, updates Circular 06/240 and mainly focuses on administrative and accounting organization, IT outsourcing and details regarding services provided under the status of support PSF. The circular applies immediately to all credit institutions and other professionals of the financial sector.

Circular 17/657 reflects the multiple legal and regulatory changes which occurred since the last update to Circular 06/240 in 2013, and in particular, the changes introduced by Circular 17/654, 17/655 and 17/656. One footnote clarifies that only production systems are supposed to contain confidential data and that development and testing systems should not contain these.

Deloitte.

How can Deloitte help?

Deloitte helps our clients comply & remediate through:

- **Compliance Assessment** – gap analysis of our client's IT projects compliance against laws and regulations and pragmatic recommendations for improvement
- **Assisting in Communications with the Regulator** – preparation (or quality assurance) of application files and participation in meetings with the regulator
- **Information Security Officer (ISO) on demand** – Design the security function and provide resources with security and technical expertise to support the function

Your contacts

Roland Bastin
Partner | Information & Technology Risk
Tel: +352 45145 2213
rbastin@deloitte.lu

Martin Flaunet
Partner | Banking & Securities Leader
Tel: +352 45145 2334
mflaunet@deloitte.lu

Stéphane Césari
Partner | PSF Industry Leader
Tel: +352 45145 2487
scesari@deloitte.lu

Laurent de la Vaissière
Director | Information & Technology Risk
Tel : +352 45145 2010
ldelavaissiere@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