

April 2005

IT outsourcing : new CSSF requirements for Luxembourg banks and other Professionals of the Financial Sector

The Commission de Surveillance du Secteur Financier (CSSF) released on April 11, 2005 Circular 05/178 on the IT function of Luxembourg banks and other Professionals of the Financial Sector (PFS). This new circular abrogates and replaces the part of Circular 96/126 that was dealing with the IT function, and that needed to be updated following the emergence of new IT regulated service providers created by the law of August 2, 2003 amending the law of April 5, 1993 on the financial sector.

In accordance with the recommendations of the Joint Forum paper on “Outsourcing in financial services” dated February 2005, the Luxembourg banks and PFS which are willing to outsource (part of) their IT function now need to comply with the following key principles:

- The Board of Directors must document and validate the outsourcing policy that should notably include a deep analysis of the financial, operational, legal and reputation risks incurred by the outsourcing.
- Any outsourcing must be formalised into a Service Level Agreement describing both parties’ responsibilities, more specifically the acceptable conditions under which the IT service provider intends to outsource again to another party.
- The bank/PFS must ensure if it needs to inform, or not, its third parties and more importantly its customers, with regards to contractual clauses, or legal provisions such as data privacy.
- For each delegated activity, the bank/PFS shall designate an employee responsible for the relationship with the IT service provider.
- The bank/PFS shall be able to operate in case of exceptional events such as the break of the communication line with the IT service provider.
- The bank/PFS shall be able to transfer the outsourced services to another party or to take them back internally, should the quality of the services rendered by the IT service provider be unsatisfactory.

The main changes or details compared to previous circular are as follows:

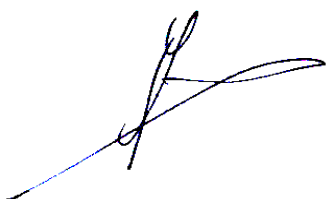
- Luxembourg banks and PFS that wish to outsource certain IT services to regulated Luxembourg “IT systems and communication networks operators of the financial sector” as defined by Article 29-3 of the amended law of April 5, 1993 on the financial sector (referred to as “PFS IT”) must notify the CSSF and confirm that the various conditions listed in the Circular are respected. The IT PFS, as they are entitled to the Luxembourg professional secrecy, are authorised to have access to customers’ confidential data, if those data are necessary for the execution of the service agreement.
- Luxembourg banks and PFS that wish to outsource certain IT services to other parties, even within their own group, are required to ask the prior approval from the CSSF and, again, confirm that the various conditions listed in the Circular are respected. The third party or the group entity, which provides outsourcing services, is not authorised to have access to the Luxembourg bank/PFS customers’ confidential data.

Any existing outsourcing arrangement should be adapted to the conditions of Circular 05/178 by December 31, 2005 or, at least, at the next renewal date of the contract.

The main conditions applicable to banks/PFS willing to outsource IT services are summarised in Appendix.

For further information or discussion on this circular, please refer to the following contact persons:

Philippe Sergiel	Partner, Audit	philippe.sergiel@lu.pwc.com	+ 352 49 48 48 2531
Emmanuelle Henniaux	Director, Regulatory Compliance Advisory Services	emmanuelle.henniaux@lu.pwc.com	+ 352 49 48 48 2549
Yves Decoster	Director, Systems and Process Assurance	yves.decoster@lu.pwc.com	+352 49 48 48 6112



Philippe Sergiel
Partner



Emmanuelle Henniaux
Director

Reference in Circular 05/178	Summarized conditions	Maintenance of IT systems (including advice and programming services)		Operation of IT systems		
		Provided by a non-regulated IT service provider	Provided by a Luxembourg PFS IT (Art 29-3 of the Law of April 5, 1993)	Provided by the parent company or another group entity		Provided by a Luxembourg PFS IT (Art 29-3 of the Law of April 5, 1993)
				Located in Luxembourg	Located abroad	
4.5.2.1		Advice, programming, maintenance services				
	- The bank/PFS must be able to function normally in case of IT breakdown and must thus have back up solutions <i>which are consistent with its business continuity plan</i>	✓	✓	✓	✓	✓
	a A Service Level Agreement including conditions below must be formalised	✓	✓	✓	✓	✓
	b The accounting function, <i>including data input</i> , must not be transferred to the service provider	✓	✓	✓	✓	✓
	c (i) Service provider's interventions and modifications must be pre-approved by the bank/PFS	✓	N/A – PFS IT can have access without prior approval from the bank/PFS	✓	✓	N/A – PFS IT can have access without prior approval from the bank/PFS
	c (ii) One bank / PFS's employee must have sufficient IT knowledge to understand the effects on the programmes on the accounting system and <i>the actions made by the service provider</i>	✓	✓	✓	✓	✓
	c (iii) The bank / PFS must have, in its premises, adequate documentation of the programmes	✓	✓	✓	✓	✓
	d The bank/PFS must ensure that there is no legal obstacle which would prevent it having access to the operating programmes. <i>The bank / PFS must anticipate actions to guarantee continuity of services in case of service provider's default</i>	✓	✓	✓	✓	✓
	e Service provider may not have access to confidential data	✓	N/A – PFS IT may have access to confidential data	✓	✓	N/A – PFS IT may have access to confidential data
	f In case of breakdown and if access to confidential data cannot be avoided, the service provider must be accompanied throughout his intervention by an IT employee of the bank / PFS	✓	N/A – PFS IT may have access to confidential data	✓	✓	N/A – PFS IT may have access to confidential data

Legend:

- ✓ : conditions to be respected
- in italic bold* : main changes compared to Circular 96/126

Reference in Circular 05/178	Summarized conditions	Maintenance of IT systems (including advice and programming services)		Operation of IT systems		
		Provided by a non-regulated IT service provider	Provided by a Luxembourg PFS IT (Art 29-3 of the Law of April 5, 1993)	Provided by the parent company or another group entity		Provided by a Luxembourg PFS IT (Art 29-3 of the Law of April 5, 1993)
				Located in Luxembourg	Located abroad	
g	The bank / PFS must designate an employee responsible for managing the access to confidential data	✓	✓	✓	✓	✓
h	The service provider can work only in a test environment and must obtain the express agreement of the bank / PFS for each intervention	✓	N/A – PFS IT may work in production environment without prior agreement from the bank/PFS	✓	✓	N/A – PFS IT may work in production environment without prior agreement from the bank/PFS
i	Telecommunications must be encrypted or protected by other valid technical means. Means must be in place to continue to function normally in case of breakdown in the link	✓	✓	✓	✓	✓
4.5.2.2	Systems management services					
-	If the service provider is located abroad, the outsourcing must be delegated <i>contractually</i> to the parent company or to another group entity which is included in the scope of the supervision on a consolidated basis by a financial supervisory authority <i>The processing centre can be located with an entity which is not the entity contractually responsible</i>		N/A	N/A	✓	N/A
-	<i>When the processing centre is physically located by an entity which is not the one that is contractually responsible, the bank/PFS must ensure that conditions listed under paragraph 4.5.2.1 are respected by the entity which is contractually responsible</i>		N/A	N/A	✓	N/A
-	<i>The bank/PFS must provide the CSSF with a document justifying that the outsourcing “in cascade” is monitored, showing that the other supervisory authorities are aware of this outsourcing</i>		N/A	N/A	✓	N/A
-	<i>No confidential data can be stored with a service provider, unless this data is encrypted and can only be decrypted by the bank/PFS</i>		N/A	✓	✓	N/A – PFS IT may have access to confidential data
-	The bank/PFS must require the prior authorisation from the CSSF and must prove that the conditions listed in the Circular are respected		N/A	✓	✓	N/A
a	The bank/PFS must have rapid and unlimited access to the information stored by the service provider		N/A	✓	✓	✓

Legend:

- ✓ : conditions to be respected
- in italic bold* : main changes compared to Circular 96/126

Reference in Circular 05/178	Summarized conditions	Maintenance of IT systems (including advice and programming services)		Operation of IT systems		
		Provided by a non-regulated IT service provider	Provided by a Luxembourg PFS IT (Art 29-3 of the Law of April 5, 1993)	Provided by the parent company or another group entity		Provided by a Luxembourg PFS IT (Art 29-3 of the Law of April 5, 1993)
				Located in Luxembourg	Located abroad	
	a	Data input and printing must be performed in the bank/PFS's premises	N/A	✓	✓	N/A – PFS IT may have access to confidential data
	a	The bank/PFS must have a trial balance and a journal of all accounting entries on a daily basis	N/A	✓	✓	✓
	b	The system must permit the maintenance of accounting records in accordance with the Luxembourg accounting principles	N/A	✓	✓	✓
	c	Communications must be encrypted or protected by other valid technical means	N/A	✓	✓	✓
	c	No customer name must be input or stored in the system to which the service provider has access	N/A	✓	✓	N/A – PFS IT may have access to confidential data
	d	The external auditor and the internal auditor must be able to perform the necessary tests at the service provider to allow them to issue an opinion on the adequacy of the IT link	N/A	✓	✓	✓
	e	The IT link must be formalised in a Service Level Agreement	N/A	✓	✓	✓
4.5.2.3	-	If the bank/PFS operates abroad with recourse to the services of professional intermediaries (<i>even</i> if these are part of the group to which the bank/PSF belongs) or if it operates through representative offices abroad, these intermediaries on representative offices cannot have access to the bank/PFS's IT system in Luxembourg	✓	✓	✓	✓
4.5.2.4	-	<i>When outsourcing to a PFS IT, the bank/PFS's organization and procedures manual must be adapted. The bank/PFS's business continuity plan must be consistent with the PFS IT's business continuity plan. The IT infrastructure can belong to the bank/PFS that outsources or to the PFS IT. The PFS IT staff can work either in its premises or in the bank/PFS's premises</i>	N/A	N/A	N/A	✓

Legend:

✓ : conditions to be respected

in italic bold : main changes compared to Circular 96/126

Reference in Circular 05/178	Summarized conditions	Maintenance of IT systems (including advice and programming services)		Operation of IT systems		
		Provided by a non-regulated IT service provider	Provided by a Luxembourg PFS IT (Art 29-3 of the Law of April 5, 1993)	Provided by the parent company or another group entity		Provided by a Luxembourg PFS IT (Art 29-3 of the Law of April 5, 1993)
				Located in Luxembourg	Located abroad	
a	<i>There is no professional secrecy between the bank/PFS and the PFS IT as soon as (i) information is transmitted in accordance with a Service Level Agreement relative to the regulated activity and (ii) information is necessary for the execution of the service</i>	N/A	N/A	N/A	N/A	✓
b	The Bank/PFS's external auditors and internal auditors must be able to perform the necessary tests at the PFS IT in order to allow them to issue an opinion on the adequacy of the IT link. <i>They can use the PFS IT's external auditors reports if necessary</i>	N/A	N/A	N/A	N/A	✓
c	The bank/PFS that uses a PFS IT must notify it to the CSSF in justifying that above conditions are respected	N/A	N/A	N/A	N/A	✓

Legend:

- ✓ : conditions to be respected
- in italic bold* : main changes compared to Circular 96/126