COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

In case of discrepancies between the French and the English text, the French text shall prevail

Luxembourg, 7 January 2013

To all professionals of the financial sector[1]

CIRCULAR CSSF 13/554

Re: **Evolution of the usage and control of the tools for managing information technology resources and the management of access to these resources**

Ladies and Gentlemen,

This circular concerns the tools allowing the management of access rights to IT resources connected to a network and/or the centralised registration and administration of most these resources (user accounts, printers, computers, services, etc.).

Some international groups of financial professionals tend to regroup these tools at group level so as to achieve a uniform and sovereign management of these IT resources.

The CSSF would like to remind you that the professionals of the financial sector[1] must always have full control over the resources under their responsibility and the corresponding access to these resources, primarily for compliance and governance reasons and secondly in order to protect confidential data subject to professional secrecy.

The technical note "Evolution of the usage and control of the resources access tools" annexed hereto provides the technical rules with which the professionals of the financial sector must comply. The CSSF requests all the institutions concerned to ensure their compliance with this note, particularly when faced with demands from their group in this area.

This circular comes into force with immediate effect.

Yours faithfully,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON	Andrée BILLON	Simone DELCOURT	Jean GUILL
Director	Director	Director	Director General

Annexe: Technical note – Evolution of the usage and control of the resources access tools

[1] As defined in the law of 5 April 1993 on the financial sector

Annex: Technical note – Evolution of the usage and control of the resources access tools.

The resources Access Tools[2], hereinafter named AT, allow companies to manage access rights to the IT resources connected to their network and/or to centrally register and administer most of those resources (user accounts, printers, computers, services, etc.).

Financial Institutions in Luxembourg, hereinafter named FI[3], must always have permanent full control over the resources under their responsibility and the corresponding accesses to these resources, primarily for compliance and governance reasons and secondly to protect confidential data subject to professional secrecy.

The CSSF considers that this obligation is fulfilled when a FI has a separate and isolated AT in Luxembourg, either exclusively maintained and controlled by itself, or with the assistance of a Support Professional of the Financial Sector (Support PFS) under a service contract. In this last case, the FI should have adequate outsourcing supervision controls in place.

Some international groups tend to regroup the AT of the FIs belonging to their group into the global AT of the group. The underlying reasons for these requests are:

1. To allow a uniform and simplified management of IT resources via a central administration of the AT at the group level;

2. To facilitate access to resources located within the group (e.g. Luxembourg users can automatically access to applications located and managed abroad via their AT account synchronised with the application user account).

Any FI wishing to use such a configuration is required to introduce a formal and detailed authorization request to the CSSF. The authorization request document needs to demonstrate that the obligation of a permanent full control by the FI over the resources under its responsibility and over the corresponding accesses to these resources is always fulfilled.
This notably implies that:

1. The Luxembourg entity must be isolated as a "segment" of the AT covering the AT resources under its responsibility (for instance in the context of a Microsoft Active Directory usage, preferably a dedicated LU domain or, at a minimum, a dedicated Organisational Unit "OU");

2. A formal AT policy management procedure is in place respecting the following points:
   a) The FI approves and controls the AT policy defined for its AT "segment", hereinafter named the **"approved AT policy"**[4];

   b) The FI is able to ensure the continuous technical implementation of the "approved AT policy" on AT systems, hereinafter named the **"implemented AT policy"**[4]. Both policies must be fully consistent, i.e.:

[2] Such as Microsoft Active Directory, Novell eDirectory, Oracle Access Manager, IBM RACF, etc.

[3] Defined as "professionals of the financial sector" in the Law of 5 April 1993 on the financial sector.

[4] See glossary at the end of the document

i. The "implemented AT policy" is always matching the "approved AT policy" (e.g. an AT policy update "pushed" from the group must always be first communicated in a comprehensive way for prior formal approval by the FI and for update of the "approved AT policy" accordingly. The updated "approved AT policy" can then be technically implemented);
ii. All the approved policies are implemented;
iii. No unauthorized policies are implemented.

Considerations on preventive versus corrective controls/usage of specific tools

To ensure that its "implemented AT policy" is fully and constantly consistent with its "approved AT policy" (as required under point 2.b) above), a FI must control that every AT policy change is authorised before its implementation.

Such a preventive control will allow to prevent the push of a non-approved policy, as opposed to a corrective control that will allow the identification and subsequent correction of a pushed non-approved policy after its implementation.

Specific tools are available today on the market to perform preventive controls. Globally, they function as described below:

- The tool has its own internal AT policy, referred to herein as the **"tool internal policy"**[4]. The "tool internal policy" must be configured as the exact digital transposition of the "approved AT policy";
- The tool locally controls the FI AT "segment" by systematically comparing an AT policy change request (push) to its "tool internal policy";
- In case the push contains a change that is not in line with the "tool internal policy", the update is blocked.

This functionality provides a higher degree of security compared to corrective controls. Indeed, even if a corrective control is performed shortly after an AT policy push, unauthorised access to FI resources will have been possible between the implementation of the AT policy update and the consequent correction.

Consequently, the CSSF requires the implementation of a preventive control as described above. Corrective controls are not considered as sufficient and should be performed as a contingency solution in case of preventive control failover (server failure, agent breakdown, etc.)[5]**.**

[5] Please refer to section "Use of corrective controls as contingency solution".

Conditions for preventive control effectiveness

The usage of tools performing preventive controls implies the respect of the following requirements to ensure the effectiveness of those preventive controls:

1. The tool that will locally control the AT must:

   - Be exclusively operated and controlled by the Luxembourg entity or the Support PFS in case of outsourcing;
   - Be protected against any access from the group;
   - Use internal policies exclusively controlled by the Luxembourg entity.

2. The scope of controls made by the implemented tool must be clearly defined and formalized in a complete documentation and must in any case cover at least the AT policy;

3. The AT policy management procedure has to ensure the continuous alignment of the three policies: “approved AT policy”, “tool internal policy” and “implemented AT policy”;

4. The solution must be yearly audited at a technical and an organizational level including all documentation. Notably, the tool must be periodically controlled to ensure that:

   - The “tool internal policy” is matching with the “approved AT policy” and the “implemented AT policy”;
   - The logs do not show any malfunctioning of or suspect actions to the solution used.

5. Access to the tool and changes to the internal tool policy should be logged. Access to those logs needs to be adequately protected (for instance, no modification or deletion by the tool administrators). The logs must be archived in such a way that their confidentiality, integrity and availability are ensured.

6. The team needs to have the necessary skills to keep control on the policies, the day to day management of the solution and the procedures.

7. The proper functioning of the tool (including any additional product or functionality necessary to run the control, e.g. agents, services, servers, SNMP, etc.) must be constantly monitored. If they are in a fail over mode, a real time alerting functionality should be activated to warn of unexpected shutdown and to allow for immediate reaction (see section “Use of corrective controls as contingency solutions” below).

Use of corrective controls as contingency solutions

It is important to notice that if the tool used to perform preventive controls is down, the preventive controls are not operational anymore and all AT policy changes can be directly pushed and implemented.

Therefore, if the preventive controls are no longer available, corrective controls must be used to identify unauthorised access / AT policy changes which potentially occurred during the shutdown window and perform relevant corrections.

Those corrective controls can be based on AT log reviews and/or audit tools or gap analysis tools. The FI should explain the technical feasibility of the chosen corrective control in its authorisation request, taking into account notably for AT logs analysis that:

1. The availability of appropriate logs is key for a post event diagnostic. Some AT versions cannot provide adequate log functionality (no logs available or no logs of appropriate events such as policy changes); logs must trace all sensitive activities including those of super users, actions performed from outside of Luxembourg and any activities impacting data confidentiality. They must provide the ability to perform forensics if required. The sensitive activities will be explicitly defined by the entity for audit purposes;
2. Access to logs needs to be adequately protected (for instance, no modification or deletion by the administrators);
3. Logs must be archived in such a way that their confidentiality, integrity and availability are ensured.

Particular case of policy import

If a FI has a separate and isolated AT in Luxembourg but imports policy from its group (e.g. by uploading files from USB keys or dedicated hard drives), the FI also will have to ensure its conformity to the rules explained in this technical note. A specific procedure covering this import process will have to be set up to stay compliant with this technical note.

***

Glossary

Approved AT policy: The "approved AT policy" is a text document written in such a way that people who are not AT specialists – as the FI management - are able to understand, discuss and finally approve it. This is not a technical document extracted from the AT.

Implemented AT policy: The "implemented AT policy" is the technical implementation of the "approved AT policy" on AT systems.

Tool internal policy: The "tool internal policy" is the exact digital transposition of the "approved AT policy" in the tool used to perform the preventive controls as described in this document; the "tool internal policy" is the baseline used to compare AT policy change requests to the "approved AT policy" and to authorise or prohibit their implementation on AT systems.