SUPERVISION OF INFORMATION SYSTEMS

1. Activities in 2009
2. Supervisory practice
1. ACTIVITIES IN 2009

1.1. Participation in national groups

In 2009, the department “Information systems and supervision of support PFS” represented the CSSF within the following committees, commissions, associations or working groups:

- ABBL - Payments Committee. The Committee in which the CSSF participates as observer deals with topics relating to payment and clearing systems, bank cards and direct debit. In 2009, it especially dealt with the transposition of the Payment Services Directive (PSD) into national law and its operational application.

- CRP Henri Tudor. In 2009, the CRP continued its works on the research programme INNOFinance which identifies projects related to innovation and promotion of financial sector services. The CSSF is involved in the strategic orientation of the INNOFinance projects and it also takes part in the strategic sub-committees in the fields of IT systems security and service quality.

- Luxembourg Institute for Standardisation, Accreditation, Safety and quality of products and services (Institut Luxembourgeois de la Normalisation, de l’Accréditation, de la Sécurité et qualité des produits et services, ILNAS). This authority, under the responsibility of the Minister for Economic Affairs and Foreign Trade, has been created by the law of 20 May 2008 and started its activities on 1 June 2008. ILNAS comprises, among others, the Luxembourg office of Accreditation and Surveillance (Office luxembourgeois d’accréditation et de surveillance, OLAS) and the State energy service (Service de l’Énergie de l’État, SEE) and consolidates the works in standardisation of IT quality and systems security previously initiated by the Association de Normalisation pour la Société de l’Information Luxembourg (ANSIL). In the context of the financial sector, the CSSF participates in the standardisation of IT systems security (ISO/IEC Standards 270xx).

- Operational Crisis Prevention Group for the financial sector (OCPG) under the aegis of the Luxembourg Central Bank. The mission of OCPG consists in identifying the risks supported by the financial sector in relation to critical infrastructures, in order to suggest measures enabling to prevent a possible operational crisis which would disrupt the functioning of the financial professionals and jeopardise the proper settlement of monetary policy operations.

1.2. International cooperation

The department took part in the international conferences of the IT Supervisory Group (ITSG), which gathers the persons responsible for the prudential supervision of the IT systems within the different authorities every year.

The aim of this group is to foster the exchange of information on the current technological challenges. The group also covers aspects such as business continuity plans, electronic banking, countermeasures against the phishing phenomenon and, in general, the specific weaknesses of banking IT, as well as the supervision of cross-border IT outsourcing. Throughout the year, the members of the group exchange information on subjects related to the use of IT and of the Internet by financial sector players, mainly in the banking sector. The information exchanged in 2009 concerned IT system attacks and identity or bank card thefts.

New countries wish to join the ITSG every year, indicating that its popularity is constantly growing. The subjects discussed are carefully prepared and the conferences are very structured in order to cover in the most efficient way the subjects considered to be the most important. The members have taken the necessary measures in order to keep the number of countries represented under control and have also discussed the possibility to introduce a mandatory sponsorship by a member country. In 2009, Mexico and China joined the ITSG. These new members valuably contributed to the discussions and allowed the group to understand the challenges peculiar to the newcomers. As the group is becoming larger and in order to cover the European specificities, an exclusively European ITSG conference has been organised for the second time in 2009.
1.3. Developments in the regulatory framework

The department “Information systems and supervision of support PFS” continued its works aiming at improving the efficiency of supervision for the supervised entities, the réviseurs d’entreprises (statutory auditors) and the CSSF.

The risk-based approach as announced in Circular CSSF 08/350, which will be applicable to support PFS, has been analysed and the results of this study will be submitted for comments in 2010. The publication is planned in 2010 in order to provide a concrete basis for supervision as from 2011. This will give support PFS enough time to adapt their internal governance.

2. SUPERVISORY PRACTICE

Supervision includes the verification that supervised entities comply with the legal and regulatory framework, with the direct or indirect purpose to maintain or improve the professionalism of their activities. It focusses, in particular, on the technologies implemented for the information systems and takes into account the specificities of the outsourcing of these services with support PFS or third parties, outside or within the group.

2.1. Implementation of multi-tenant financial software

The objective of a financial institution offering IT services to other entities within or outside the group is obviously to mutualise some of the IT systems in order to optimise costs. Using equipment mutualising is not a new concept. The CSSF has always put forward the risks of a possible loss of confidentiality or integrity of data if the different functional environments of mutualised IT systems are not correctly segregated. Where a banking institution intends to mutualise its banking software in order to make it also available to its subsidiaries or other companies of the group, the CSSF always recommends to duplicate the applications, in order to preserve in the best possible way the segregation of data and to ensure that an instance user (for example a subsidiary) may not have access to data and processing of other instances (another subsidiary or the bank itself).

The risks mainly depend from the technical soundness of the hardware partitioning to resist a “loss of protection” between systems.

For each instance running on a separate computer, protection is managed at connectivity level between these machines and at the level of the access rights set up on each machine. A vulnerability in the software or in the operating system of a computer does not imply a loss of protection if these computers do not interact or if communications are under control. If each instance runs on the same computer, the protection of the operating system between the logical partitions that have to be managed shall be investigated. The CSSF is not aware of any cases reported which would jeopardize the reliability of operating systems allowing partitioning, whether on virtual machines or proprietary operating systems. Segregation only works if a sound, documented, regularly reviewed implementation, a follow-up of vulnerabilities and regular corrective updates are performed. Partitioning or virtualisation technology is more and more widespread and seems, so far, sufficiently robust to be considered for a professional use for mutualising technical financial platforms and in particular for banking platforms. In a partitioned or virtual environment, several instances of the single-institution software, each instance being affected to an institution, allow the implementation of additional security and environment segregation mechanisms as, for example, cryptography of partitions at operating system level, hindering another instance from reading the data, even in case of protection loss.
If mutualising is done at application level, i.e. if the software has been created to manage different institutions, one shall be prudent to assess the risks based on the activity performed, the qualification of the managed information (confidential or not) and the permanent specific controls that are executed to ensure that errors (or frauds) are detected on time. An investment fund management software should thus allow the management of multiple UCIs, as it has already been developed, from conception, for multiple compartments. Confidentiality is not necessarily a decisive criteria in the calculation of the NAV and the daily accounting and financial controls performed allow detecting a possible bug.

However, banking software with full functionality coverage, which would separate the management of each individual bank only based on a selection at user connection level, represents \textit{a priori} an important risk which would be hard to evaluate if data would be mixed up. The complexity of the software may generate unpredictable bugs, similarly to some operating systems which are now so complex that they create unexpected errors which are difficult to reproduce. Systematic financial controls within a credit institution are also more widespread due to the diversity of available functions and, as a consequence, the probability of an error not being detected on time increases. It is much more difficult to guarantee confidentiality in a multi-institution software than in a single-institution software.

Depending on the application architecture used by the software designer (two-tiers or three-tiers), the implementation of the database system used by the application should also be checked. It is important to have a detailed knowledge of the architecture chosen to mutualise the resources. Even if each institution has a dedicated instance of the software, the supervisor of this mutualisation must ensure that each application instance has its own database instance. If there is a single global database for all mutualised financial institutions, the risk is the same as, or even greater than having a multi-institution software. This type of architecture is generally offered to entities within a group which mutualises its IT infrastructure with a single operator. As each financial institution is responsible for its own controls as a distinct legal entity, mostly located in different jurisdictions, it is more likely that no global mechanism will be considered at group level to ensure that no manipulation is done in the database. A database administrator or an intruder (IT hacker), who has sufficient functional knowledge, may thus manipulate the accounts and transactions between different group subsidiaries, guaranteeing at the same time a balanced accounting for each of them.

As a consequence, a mutualisation of several financial institutions, based on a single database only, even if each institution has an application instance of the financial software, is not acceptable without formal evidence of in-depth controls and of a complete traceability of transactions made on the database, as well as a global governance proving the possibility to detect potential errors or frauds based on a manipulation of data of each mutualised institution at the lowest technical level.

2.2. Cloud computing and virtualization

It is not easy to provide a unique definition for “cloud computing”. This concept has however been used for several years now by different organisations active in the Internet world.

Cloud computing may be considered from two aspects: economic/financial and technical.

From an economic and financial point of view, cloud computing consists in switching from a capital expenditure (CapEx) model to an operating expenses (OpEx) model. Cloud computing is usually used to provide IT resources on demand and at a price which is proportional to the requested resource. Forrester Research defines cloud computing as the ability to provide standardised IT services through Internet technologies (services, software or infrastructure) which are pay-per-use in self-service mode. Switching from a CapEx model to an OpEx model allows the provider to distribute the investment among many users, so that those users only participate in the investment based on their effective needs. Consequently, switching from one model to the other is only feasible for a company if the service is outsourced to a provider having a very large number of clients or if the own IT infrastructure is sufficiently important to provide the service to these multiple clients via, for example, the group. Cloud computing represents in some aspects the ultimate step of equipment and IT services mutualisation.
From a technical point of view, this mutualisation implies a standardisation and, consequently, a homogenisation of technical infrastructures and applications. Cloud computing consists in activating on demand resources, often virtual machines, allowing one or several software to run simultaneously in order to meet users’ requests. The cloud may concern archiving, CPU for the execution of programmes or a more sophisticated service consisting of a complete system. The term “cloud” suggests that the service is offered as a consistent set to the user, without the user knowing the place where and the detailed manner in which this service is offered.

The search engines on the Internet and the major virtual stores use a cloud technology to meet the volume of the end users. A search or purchase will be processed in the cloud according to a complex mechanism which makes the predictability of the location difficult. The first available server, regardless of its location, will provide the service.

In cybercrime, hackers who corrupt private or public PCs to use them without their owners being aware in order to perform a cyberattack create a BotNet, which is merely a cloud executing distinct actions, without the criminal knowing exactly which of the hacked computers is active. The criminal spreads his programme which will operate autonomously on hundreds of thousands of computers.

As a consequence, the concept of cloud computing is based on the ability to duplicate an IT processing, similar to cloning, within a vast and relocated technical resources environment. This environment is often called farming and means that the IT system has many physical machines which make those clones work. This means that the user has a huge virtual computer and a virtual storage space, whose physical component is based on computers and storage equipment which are interconnected and geographically distributed (within a room, country or one or more regions around the world).

Cloud computing is also mainly based on virtualisation, not only of the service, but also of the operating system. A physical computer may encompass several virtual machines. Due to the reduced number of virtual machines, it may not be defined as cloud, but the base principle is the same.

Cloud computing has the advantage of being resilient, as losing one equipment for whatever reason does not imply that the service stops as there is always, a priori, a cloud equipment which remains active to meet users requests.

Questions on the extent to which a financial institution may use cloud computing are more and more frequently asked to the CSSF.

The answer cannot be exhaustive, mainly because the concept is new and requires a more precise definition. Part of the answer may however be given by splitting the specific concepts of cloud computing and confronting them to the prudential and regulatory concepts.

In the concept of cloud, the concepts of replication, distribution and opaqueness can be identified. Indeed, the cloud can only work because the processes are replicated. Distribution is inherent to the cloud, but the term “cloud” also suggests the idea of opaqueness and lack of visibility.

- Replication: Replication of a processing is not a problem as such, except for the reliability of the processing in relation to equipment and operating system. A processing is considered as being “stable” when its performance is known and its results stable in time. Hence, the quality of the processing depends on the quality of the tests performed. In a traditional environment, tests are performed in a well-known environment. The equipment is well defined, the operating system as well and the tests are performed for every update of a component. Despite a series of tests, the processing may generate an error or stop. The more complex the processing, the less predictable the error is. This is due to the interaction of the complex processing with the equipment and operating system, which are both just as complex. This unexpected error risk must be multiplied by the number of instances operating in the cloud, with a multiplier effect if the cloud is not homogeneous, i.e. established on heterogeneous equipment or working with different versions of an operating system. A processing error by only one instance of the cloud may pass unnoticed. If identified, the instance which caused the problem must still be determined. The instance’s specific traceability must hence be considered when the system is developed. The reliability of the processing necessarily implies its integrity. Replication must hence include a verification of the integrity of the processing at each step of
the cloning. This can be done through electronic signature and code hashing mechanisms. The potential actions of a hacker who breaks into the cloud and modifies the processing during its cloning can easily be imagined. From a prudential point of view, replication must occur together with a guarantee of integrity and a traceability of the functioning of each clone. The processing must therefore be specifically realised in a cloning perspective in order to take into account these control mechanisms.

- **Distribution:** This section covers at least two aspects which have to be considered for the financial sector, i.e. the physical location of the processing and of the data, that is to say the geographical distribution, and the timing for the distribution of the updates. The Luxembourg legal and regulatory framework imposes certain restrictions to the distribution of processing and storage abroad, in particular as regards the provisions relating to professional secrecy (law of 5 April 1993 on the financial sector, Circular CSSF 05/178 on the IT support function and its outsourcing with a third party). The distribution timing may also be a problem when an update is required for the fixing of an error or the amendment of a functionality. Indeed, the larger and the more geographically extended a cloud, the longer the distribution time. This is all the more true if the distribution is geographically extended as a poor quality of network communication may slow down this distribution. As a comparison, the update of a domain name in the DNS (Domain Name Server which allows resolving the IP address of a machine through its URL) may take up to 72 hours. During all this time, some DNS still contain the old link leading to an old server. A slower distribution for a programme or financial function would result in certain functionalities running on the old version of the software. Due to this uncertainty, the instance’s version used that realises an operation must be traceable if used in the financial sector, as is the case for replication.

As a conclusion, cloud computing is a concept which is based on complex technical possibilities, which may not be suited for all financial services in the financial sector. The need for controls required by the legal, regulatory and prudential framework is only compatible with cloud computing if these complex mechanisms include a traceability of each transaction and if automatic detection mechanisms are implemented to identify any anomaly. A financial software must be specifically developed to be used in a cloud in order to be considered as potentially compliant with the prudential requirements of the financial sector. The concept of cloud computing is a priori in contradiction with the prudential principle of a financial institution always remaining responsible for its decisions, in particular as regards the choice of technical infrastructures and outsourcing, and hence always required to have control over its functioning. This inconsistency may be lifted if the cloud becomes transparent in its functioning and operation.

### 2.3. Dematerialisation and archiving of documents

In its 2008 Annual Report, the CSSF pointed out the legal uncertainty of a proof if a paper document is dematerialised, in particular if the original paper is destroyed.

Considering the volume of archived documents that must be kept by the supervised entities, the Minister for Economic Affairs and Foreign Trade associated the CSSF with its works aiming at improving this situation by drawing up a more appropriate legal and regulatory framework.

Currently and as long as these works are not accomplished, and considering Article 1333 of the Civil Code on private deeds which provides that: “Where the original deed or a deed valid as an original within the meaning of Article 1322-2 exists, the copies are only valid for the content of the deed, whose presentation may always be required.”, the CSSF maintains its position of last year and recommends institutions under its supervision to be extremely cautious before considering the destruction of original documents in paper form.
2.4. Pandemic

2009 was marked by the fears of a pandemic linked to the new flu virus A H1N1. In its 2006 Annual Report, the CSSF had already discussed the pandemic issue within the financial sector, recommending a sufficient preparation allowing to minimise the consequences of such catastrophe on the Luxembourg and international financial centres.

The CSSF reminds that a pandemic does not modify the legal and regulatory framework and that financial institutions are still required to comply with it.

Telework, often presented as an essential element to ensure business continuity, is only possible if the four-eyes principle remains applicable. A certain number of financial institutions however use IT systems that have not been planned to ensure a four-eyes principle without having to use paper documents. In practice, a document is validated by the initials or handwritten signature of at least two persons. Telework is however mostly based on an exclusive usage of IT and does not involve "paper" flow, which entails that this control principle is departed from. Moreover, telework from abroad is not compliant if the person can visualise information falling under professional secrecy within the meaning of Article 41 of the law of 5 April 1993 on the financial sector.

2.5. State of the vulnerabilities reported in Internet-based financial services

The situation has remained stable since 2008. The attacks registered are always linked to a vulnerability of the client’s computer or to a vulnerability of the provider’s website.

In addition to the remarks and comments made in 2008, the CSSF observes that the vulnerabilities allowing a criminal to enter a banking infrastructure thanks to the weakness of a website indirectly connected to that infrastructure result from a lack of global security governance in the outsourcing.

Indeed, where a financial institution develops and operates itself its IT system, the whole process is often much better controlled by the department in charge of systems security than it would be if it was outsourced. In case of outsourcing, security is mostly considered from a unitary point of view by each party concerned. There is hence no precise global view on security and vulnerabilities appear because each party is only concerned by the domain under its responsibility. As an example, the provider which operates the IT system of its financial sector client will consider that the responsibility of the applications rests with the developer, i.e. the client. There may however be security weaknesses due to the way the development is implemented by the provider. Moreover, the client may have contacted a third party for its developments and the chain of responsibilities for security is again weakened.

A global security governance grouping all the persons responsible for security of the parties concerned, allows reviewing the production chain in more detail and hence highlighting potential vulnerabilities which might come up during the implementation process.