ACP
Autorité de Contrôle Prudentiel
Banque de France

Analyses et Syntheses

The risks associated with cloud computing

No. 16 – July 2013

Table of contents

Abstract:

Information systems are of strategic importance in both the banking and insurance sectors. The development of cloud computing is a recent advance that has become a subject of attention.

Cloud computing is defined[1] as a "method of processing a client's data, which are exploited via the Internet in the form of services provided by a service provider. Cloud computing is a special form of information technology (IT) outsourcing, in which end users are not informed of the location or internal structure of the cloud."

This topic is particularly current for a number of regulatory bodies. In France, the *Agence Nationale de Sécurité des Systèmes d'Information* (ANSSI – French Network and Information Security Agency) is working on regulation via a certification mechanism. In 2012 the *Commission Nationale de l'Informatique et des Libertés* (CNIL – French Data Protection Authority) issued recommendations for companies considering subscribing to cloud computing services. Abroad, many supervisory authorities have issued statements (the United States of America, Singapore, the Netherlands), or imposed a system of prior authorisation (Spain) for the use of this technology.

In this context, the *Secrétariat général de l'Autorité de contrôle prudentiel* (SGACP – General Secretariat of the Prudential Supervisory Authority) conducted a short survey to engage in a dialogue with companies in the banking and insurance sectors on the scope, use and risks of cloud computing. A total of 14 companies from the insurance sector and 12 from the banking sector responded to a questionnaire at the beginning of this year, providing a representative view on these topics.

The first idea that emerged from this dialogue was a need to clarify the concept of cloud computing by offering a multi-criteria definition, inspired by that given by the American National Institute of Standards and Technology (NIST). The SGACP therefore proposes to describe these services as follows: cloud computing consists in using remote servers to store and process data traditionally located on local servers or on the user's terminal; it enables on-demand and self-service network access to virtualised and pooled computing resources typically charged for on a pay-per-use model; three types of services are offered (IaaS – Infrastructure as a Service, PaaS – Platform as a Service, SaaS – Software as a Service), deployed according to four models (internal private cloud, external private cloud or community cloud, public cloud, hybrid cloud).

The credit institutions and insurance undertakings (companies) responding to the questionnaire confirmed that cloud computing poses greater risks compared to conventional IT outsourcing. The numerous risks identified include data privacy, unavailability of data and data processing, loss of integrity (especially the risk of non-reversibility or lock-in) and finally the area of evidence and control. They agree on the need for a stronger legal environment, the need for certain technical security measures, the need to audit the service provider, the need for the provider to commit to continuity of service and, finally, the need to obtain a guarantee from the service provider on the reversibility of the service.

However, opinions differ on the importance of the economic aspects surrounding cloud computing, with many companies claiming that security considerations should prevail in analysing its value. Moreover, it is noted that an overwhelming majority of companies use cloud computing in management areas considered outside the "core business", even if use in more sensitive areas is also beginning to emerge. It also appears that there are differences in the procedures for the adoption of cloud computing between the insurance and banking sectors.

[1] "*Vocabulaire de l'informatique et de l'internet*", in the Official Journal of the French Republic No. 129 of 6 June 2010.

As a result of this initial analysis, which shall be refined as changes in the use and the risks of cloud computing are observed, the *Autorité de contrôle prudentiel* (ACP – Prudential Supervisory Authority) is encouraging the companies it supervises to take suitable risk management measures in respect of the following aspects:

- Legal: by enforcing a mandatory contractual framework for cloud computing services;

- Technical: by encrypting data during transport and storage (in the absence of anonymisation);

- Supervision of the service provider: by ensuring audit capability and the right for the ACP to conduct audits;

- Continuity of the service: by ensuring that the expectations of the client company can be formalised in service contracts;

- Reversibility of the service: by defining the conditions of reversibility when subscribing to the service;

- Integration and architecture of information systems: by adapting the organisation and governance of information systems to the use of cloud computing.

These good practices form part of the broader framework defined for the supervision of outsourced services, including conventional outsourcing. The expectations of the ACP in terms of governance of decisions, risk analysis, contractual elements, monitoring and the internal control of cloud computing services are therefore similar to those currently in force in prudential supervision.

Study carried out:

- For the SGACP by Marc Andries (On-site Inspection Delegation), Guillaume Cassin (Supervision of Mutual Institutions and Investment Firms Directorate), Ayoub Bahhaouy, François Philippe and Yannick Foratier (Cross-Functional and Specialised Supervision Directorate);

- For the Organisation and Information Systems (OI) of the Banque de France, by Andres Lopez Vernaza and Franck Rigodanzo.

Non-binding translation

THE RISKS ASSOCIATED WITH CLOUD COMPUTING

Information systems are a strategic element in the proper functioning and stability of the banking and insurance sectors. The field of IT is also constantly evolving as technologies and solutions are constantly being renewed.

From among recent advances, the development of cloud computing, a new form of IT outsourcing, has become a focal point for the ACP.

This type of service consists in moving the mass processing of data and/or software to a service provider and accessing these via a network such as the Internet. In France, ANSSI discussed cloud computing in its *Guide pour l'externalisation* (Guide to Outsourcing, 2010) and is working on regulating the cloud via a certification mechanism. In 2012 the CNIL issued recommendations for companies considering subscribing to cloud computing services. In the financial sector abroad, the Federal Financial Institutions Examination Council issued a statement in July 2012. The Monetary Authority of Singapore updated its Technology Risk Management Guidelines in June 2012 to include cloud computing. In Europe, the *Banco d'España* and the *De Nederlandsche Bank* have published their positions on cloud computing.

In this context, the SGACP conducted a short survey to engage in a dialogue with companies in the banking and insurance sectors on the scope of cloud computing, the extent to which this type of solution is used, their awareness of risks and the security policies adopted, as well as the suitability of the current regulatory environment. A total of 14 companies from the insurance sector and 12 from the banking sector responded to the survey, giving a representative view on these topics.

This study gives the industry a report of the responses to the survey, administered in the form of a questionnaire (see Appendix). It describes a number of good practices, the implementation of which shall be examined by the SGACP, while closely monitoring the developments of risks associated with cloud computing.

1. Characteristics of cloud computing

1.1. Defining elements

The term cloud computing covers a variety of types of services likely to continue to evolve over time as new technical solutions emerge. In order to avoid the constraints of a framework that may quickly become obsolete, the SGACP chose to adopt a definition on the combination of different criteria, including those proposed by the NIST in the United States. The respondent companies confirmed that they agreed with the proposed definition criteria.

This definition, repeated below, describes the general concept of cloud computing, the types of services offered and the various deployment models reflecting the relationship between the client company and the service provider:

- **Concept**: cloud computing consists in using remote servers to store and process data traditionally located on local servers or on the user's terminal. It enables on-demand, self-service access via a network, usually understood to be the Internet, to virtualised and pooled computing resources typically charged for on a pay-per-use model.

- **Services**: in its most common forms, cloud computing provides three types of resources.

- Infrastructure as a Service (IaaS) offers IT infrastructure such as computing power, virtual machines including an operating system, storage, and backup services.

- Platform as a Service (PaaS) provides an integrated development and/or runtime platform, based on a catalogue of standardised software and technical components whose underlying infrastructure is invisible to the user.

- Software as a Service (SaaS) is an application-based solution addressing a specific field of use supporting a business function (customer relationship management, financial management, etc.) or a cross-functional service (messaging, collaborative tools, etc.)

- **Models**: cloud computing is deployed according to four models:

- Internal private clouds are managed internally by a company for its own needs and on infrastructure that it owns.

- External private clouds are dedicated to the needs of one company or a group of companies but are hosted by a service provider.

- Public clouds are managed by specialised companies that lease their services to many companies. The word "public" here refers to the meaning commonly used by cloud computing stakeholders, that is to say an open and multi-client environment.

- Finally, hybrid clouds dynamically combine public and private clouds.

Public clouds are a special form of IT outsourcing in which services are pooled for a large number of customers and customers are usually not informed of the location of data in the "cloud".

Naturally, the ACP's attention is mainly turned to the development of public or hybrid cloud services for banks and insurance companies: in these types of cloud, pooled services are made available to all customers and/or internal users, creating a risk of data permeability between different beneficiaries. However, the same can be said for any external private cloud model in which services provided to a company under the supervision of the ACP are pooled with those offered to other customers, even within the banking and insurance sectors. This is true of community clouds, for example, in which resources are shared among a limited number of partners.

1.2. Clarifications on the defining elements

While approving the defining elements proposed by the SGACP, some companies chose to add a few clarifications regarding the specific characteristics of cloud computing.

Pooling of geographically dispersed resources. Large international groups, in the insurance and banking sectors alike, recognise cloud computing as a means to extensively pool their resources without requiring specific developments. Doing so would greatly simplify multi-country and multi-entity deployment. One large international banking and insurance group also indicates that this practice enables data to be distributed over geographically dispersed data centres and ensures the availability, as backup, of many employees who are also geographically dispersed.

Greater adaptability of resources. One banking group emphasises the concept of service elasticity and the fact that with cloud computing, requested IT resources are automatically made available. According to one insurance group, the real-time adaptability of information systems is a prime characteristic of cloud computing. Not all respondents agree on the concept of self-service, which minimises interactions between the customer and the supplier in the provision of a service

(ready-to-use services depending on service levels): one insurance group questions the suitability of this term, since a contract must be signed in order to use the cloud computing service.

One respondent considers the proliferation of definitions of cloud computing to be proof that the concept is not yet stabilised, in particular with respect to "data fragmentation".

1.3. Distinction between cloud computing and conventional outsourcing

A large majority of companies consider cloud computing to be one particular method of IT outsourcing, and therefore it presents many of the same features and risks as conventional outsourcing. One large banking group even suggests that due to the industry's requirements with regard to cloud computing, in practice, cloud services may grow to resemble conventional outsourcing.

However, the opinion overwhelmingly shared with the SGACP is that cloud computing presents greater risks than conventional outsourcing.

Specific features that are often underlined are the greater scalability and flexibility of use of cloud computing, (such as that provided by the pay-per-use model) compared to conventional outsourcing. Conversely, cloud computing implies a loss of influence on the part of the client companies with regard to IT service providers:

- Cloud computing stakeholders rarely commit to an obligation of results but prefer an obligation of means, with weak or non-existent service level agreements (SLAs) in the cloud computing world being one clear indicator of this.

- Respondents highlight a loss of flexibility in designing the service offer: where conventional outsourcing makes it possible to receive a response tailored to stated expectations, for the time being, cloud computing only offers generic solutions.

- Respondents clearly fear a partial loss of control of the information system, due to loss of control of data (no knowledge of the location or resilience of the service) or dependency on service providers. With cloud computing services, maintaining operational readiness is routinely performed by the service provider: the tasks of managing developments, acceptance testing and planning rules are the responsibility of the supplier, as is the execution of version upgrades, which are sometimes carried out without even informing the client organisations.

2. Implementation of cloud computing services

2.1. Economic aspects

The SGACP sought to measure the level of enthusiasm for these services, in particular due to the potential economic benefits, on which the viewpoints appear to be divided.

Some respondents attest to reduced costs (in particular due to the pay-per-use model) and shorter implementation time frames, while warning of hidden costs that may ultimately diminish these benefits. One international banking group also notes that cloud computing can facilitate exchanges between partners, for example when synchronising export operations (the documentary credit workflow). Another company hopes to reduce infrastructure and implementation costs and streamline the management of its business continuity plan.

Without denying these theoretical economic benefits, others consider that the decision to use cloud computing or not should be guided by the associated risks.

2.2. Expected benefits

More flexible solutions. The speed of implementation, ease of management, flexibility and elasticity of cloud computing solutions are the key elements that are highlighted. Some companies emphasise the availability, performance, broad accessibility and increased mobility of cloud computing solutions, for which all that is required is a simple Internet connection. Cloud solutions would therefore be an advantage in areas requiring high computing power over limited periods, in insurance and reinsurance (modelling and pricing) as well as investment banking (risk calculations). One insurer cites IT developments with a limited lifespan as a potential target for cloud computing because of the required implementation time frames. A few respondents indicate, however, that this flexibility is still limited and that for the time being, cloud computing solutions will remain standard solutions or insufficiently developed or mature, since there is still too little available feedback.

Better access to cutting-edge technology. Cloud computing solutions are often associated with the latest technologies based on standard and interoperable components. Companies that feel they do not have the necessary critical mass, resources or expertise see a chance to benefit from an environment that will always remain state-of-the-art and comply with the requirements of customers and regulators. For a small bank, cloud computing enables the use of up-to-date and energy efficient data centres. With respect to the applications available through cloud computing, a number of companies hope to benefit from the latest features and updates as well as more consistent functions thanks to pooling and centralisation. One large international banking and insurance group believes, however, that the benefits of cloud computing are limited to "utility" and low-risk services and are similar to those of "off the shelf" solutions.

Reduced IT costs. Cloud computing should also represent a benefit in terms of cost, particularly thanks to the pay-per-use model and billing at full costs. More broadly, some companies are announcing a change in the economic model and a drop in investment, seen as an advantage by companies with tight budget constraints on investments, but less on operating budgets. One major international banking and insurance company sees an opportunity in cloud computing to remove a number of development and operating costs with low added value from internal information systems in order to focus its resources on needs with higher added value. Another sees the possibility of reducing its infrastructure management costs.

The financial benefit argument must, however, be put into perspective. Indeed, conversely the hidden costs of cloud computing are highlighted; these are caused by difficulties interfacing and integrating the subscribed service with the company's IT infrastructure, as well as the impact in terms of human resources and the processes of SaaS solutions.

However, the supposed advantage conferred by the cloud is not unanimously appreciated: one large banking institution and one insurance company do not see any benefit in cloud computing.

2.3. Perceived risks for the banking and insurance sectors

All of the companies appeared susceptible, albeit to varying degrees, to the specific risks arising from the use of cloud computing. To a large extent these risks are a hindrance to the use of this technology, particularly in the case of public and hybrid clouds. The main obstacle seems to be rooted in the very limited room for negotiation when taking out the contract for the services offered, which are mostly generic. Thus organisations are finding it difficult to obtain specific arrangements addressing the risks they have identified.

The **data privacy risk** is the one that is overwhelmingly highlighted. The weakness of security solutions (including on-the-fly encryption and management of cryptographic keys) is generally listed first. The lack of knowledge about the location of data or the right to access data in favour of certain States[2] is considered a severe regulatory risk: within a pooled infrastructure that can potentially be accessed by local regulators it is difficult to ensure compliance with regulatory requirements, such as those resulting from regulations on banking secrecy and the protection of personal data and more widely in terms of intellectual property. This risk would be further increased outside the European Union. One large international group even sees a sovereign risk in this (if the data and data processing of French companies were no longer located in France). Difficulty controlling data security throughout the supply chain, given the number of stakeholders likely to be involved in the provision of the service, is also noted. The same applies to the difficulty ensuring that the service provider cannot read confidential data through its systems' event logs. Difficulties of integration with the company's information system and the risk of proliferation of clouds interfaced with the information system are also highlighted as potential barriers; one bank even considers that the interconnection between its own information system and that of the cloud computing service provider may create a security breach. Finally, another banking group points to the difficulty of ensuring that the service provider has destroyed data when the service is terminated.

The unavailability of data and data processing is another risk often mentioned by respondents, who highlight a gap between the need for continuity of service and the concept of availability of service used by cloud computing providers. One company states that the supplier commits to an availability rate, but that non-compliance is only sanctioned by financial penalties. Some insurance groups consider that the tangled web of service providers entails a risk when it comes to identifying the entity responsible for the service and thus a weakening of the SLA. For that matter, several companies point out that the contractual commitment of the cloud computing service provider on the availability of the service must be put into perspective since the latter cannot guarantee the speed, and in certain circumstances even the availability, of the internet network, which, however, is a key element for availability of the application.

The loss of integrity, whether concerning the data or processing, is not explicitly mentioned but is apparent in the answers. Some fear for the overall integrity of their information system due to a loss of technical expertise, or even dependence on one supplier. Finally, the risk of non-reversibility or "lock-in" is seen as significant, particularly to the extent that it is difficult to assess the ability of the service provider to return the data in a usable format. One banking group notes that it will be difficult to re-internalise a service if the service provider's tools and formats are proper to the latter.

The **weaknesses of cloud computing in the area of control and evidence** are also identified by a large number of respondents. The difficulty of auditing a service provider, or obtaining a right to audit, due to the proliferation of stakeholders and their geographical location is highlighted. More generally, the difficulty of setting up an adequate internal control system is emphasised by one large international banking and insurance company. Some insurance groups note the increased risk of non-compliance, particularly because of the location of data and identification of the applicable law.

[2] The case of the Patriot Act of the United States of America is often cited as an example. It allows US security services to access personal data on their territory or abroad if they are held by US companies. Moreover, a recent report by the European Parliament (2012) indicates that the Foreign Intelligence Surveillance Amendments Act (FISAA), specifically focused on data from non-US persons located outside the United States, is likely to give a right of access to US government agencies to all data stored in the cloud.

Even if this type of service does indeed imply specific risks, the vast majority of companies reported that they use conventional risk analysis methods for analysing cloud computing solutions. However, some have supplemented their methodology with scenarios specific to cloud computing risks. One large banking group considers, for example, that an architecture risk is intrinsic to cloud computing owing to its integration into the company's information system. In the same vein, other respondent voices the idea that pooling means that exploitation of a security breach on one client could have a negative impact on other clients hosted by the provider.

Conversely, one small banking institution reported that cloud computing could enable it to access a higher level of security than it could implement itself.

2.4. Frequent use in the fields of management and IT support

The level of use of cloud computing solutions is ultimately consistent with the advantages and disadvantages that have been highlighted. However, these solutions, already commonly used,[3] are limited to support activities for the time being, although some companies are willing to make wider use of them.

Overwhelmingly, cloud computing is used in management areas considered outside the "core business", but without providing a definition of this term, such as human resources, finance (expense reports), procurement or external or internal communications (corporate social networks, messaging, calendars, web conferencing, document sharing). Some major insurance groups report that the applications that could constitute a competitive advantage are not designed to be located in the cloud. Other companies claim to use cloud computing depending on the confidentiality and location of the data, while recognising they do not have any guarantee on compliance with the confidentiality of data, notably outside Europe.

However, use in more sensitive areas is also beginning to emerge. One insurer says it uses a hybrid SaaS solution for its accounting while another uses the cloud to host data on regulatory compliance, accounting, finance, treasury and investment. Several major banking groups use cloud computing services for customer relationship management in retail banking, corporate and investment banking and financial services. One banking group says it uses cloud computing in the field of adverse possessions. Other major groups are using cloud computing for hosting institutional websites or for services related to IT security (filtering of internet access). Some insurers report they do not rule out the use of cloud computing solutions to meet infrastructure needs for development or testing purposes (planning phase).

2.5. Decision to commit to a cloud computing service

The answers suggest there are differences in the procedures for the adoption of cloud computing between the insurance and banking sectors.

The choice to use cloud computing in insurance would involve, in the vast majority of cases, the Board of Directors or the Executive Committee. The adoption of cloud computing for sensitive or "core business" data would also require approval from the Board of Directors. Another insurer reports that this decision would be the responsibility of its Information Systems department.

On the banking side, the process of adopting cloud computing follows the process of development of the information system with an initiative from the business lines or support functions and project management by the IS department following a risk analysis.

[3] Approximately half of the insurance companies that responded are using a cloud solution, of which two-thirds are the equivalent of a private cloud. This information is not directly available for the banks, but by comparing various data the orders of magnitude appear to be similar.

In this process, the Heads of Information Systems Security and IT services advise the business lines and examine the conditions for integration of the service within the information system. One large banking group indicates that in the case of a significant enhancement, the strategic committee would be called upon. A mutual group reports that the decision to commit to a cloud computing service could only come from the Information Systems department. A small bank reports that this decision would be taken by its Managing Director in consultation with the Head of Information Systems Security.

3. Requisite accompanying measures

As current cloud computing solutions seem to offer little guarantee in terms of compliance with provisions relating to the protection of personal data, the **need for a more secure legal environment** is clearly a point of agreement. Furthermore, certain contractual clauses such as those enabling restriction of outsourcing outside the European Union, an audit clause and a clause requiring the storage of data within the European Union seem necessary. For other companies, it would be appropriate to obtain stronger commitments from the service provider on the protection and privacy of personal data, their location and the reversibility of the service. A major banking group and an insurance company would lean towards "safe harbour"[4] style protection; unless a European solution is developed. Two large companies in the insurance sector would favour a European location of data. Another international banking group would prefer French or European suppliers. Conversely, some companies in the insurance sector believe that the "traditional" legal environment now applied to outsourcing is sufficient, since cloud computing is merely one particular form of IT outsourcing.

Among the technical security measures, the **systematic encryption of data** is the one most often referred to, especially to protect data whose location is not known. One major banking group says, however, that if the encryption of data during transport is mandatory, it is more complex to implement for storage. Some large international groups want encryption to be implemented by deploying a public key infrastructure that would not be managed in the cloud. One large international group (insurance and banking sectors) considers that encryption is only useful for sensitive data (but without giving a definition) and that anonymisation may be used in non-production environments. Insurers want access rights to be managed by the customer and require the partitioning of data between the supplier's different customers.

With regard to technical measures enabling the prevention of data loss, the majority response is the implementation of a **business continuity plan with data replication across separate locations**. One large banking group stresses the importance of support located in other regions. Another banking group wants to regularly test the backup functions and ensure that the copy is remote from the primary site. This institution recommends having an emergency plan tested by an independent body.

Almost all responses highlight the **need to regularly audit the service provider and the service**. One large international group even considers that the audit is a prerequisite for subscription to the service with the service provider. Many companies recall the good practices established by obtaining service providers' audit results, audits conducted by the company and conducting penetration and vulnerability tests (although some note, however, that this is not always possible on

[4] The EU prohibits its citizens' personal data leaving its territory. But the United States has obtained an agreement that data may leave on the condition that an environment with equal protection is provided and its Department of Commerce has established a certification mechanism for US companies that want to host European personal data. This mechanism, known as "Safe Harbour", enables American companies such as Google, Microsoft and Amazon to work in Europe without having data centres there. However, it does not create an exception to the Patriot Act or FISAA: American service providers, even if they comply with "Safe Harbour", are required to provide government agencies the data they may ask for in accordance with these laws.

a public cloud). The companies expect transparency on the part of the provider in terms of the results of internal audits but also in terms of its emergency exercises and incidents. Some believe that certification of the service provider and access to its certification reports may meet the requirements of control. One company expects the introduction of labels or certifications that would guarantee that the service is rendered in an identified geographical area.

Many stress the **need for the service provider to commit** to continuity of service (maximum accepted downtime duration and maximum allowable loss of data), to the location and tracking of data storage and to the partitioning of data especially for a public cloud. Companies report that all of these elements related to the provision of cloud computing services should be subject to a Service Level Agreement. One large international banking and insurance company considers that strengthening the service provider's obligations should be based on a prior risk analysis. Another international group (banking and insurance sectors) suggests that the service provider should inform its client six months in advance of a change to the location of data and obliges the service provider to give information in the event of an incident.

The need to obtain a guarantee from the service provider on the reversibility of the service (especially for SaaS) is pointed out, considering that a contractual clause, sometimes called a reversibility plan, must be included. This plan should describe the format of returned data, set out the conditions for the return of these data, address the question of their ownership and their destruction and specify the time frame for their return. One large international group says that to ensure reversibility, it would be necessary to have the means of mass retrieval of data, to test tools regularly and to maintain in-house expertise. Reversibility may take the form of a transfer of data to a new cloud computing service provider without necessarily going through the process of re-internalisation; one insurance group believes that portability to another service provider is the easiest to manage.

4. Adequacy of the regulatory environment

Opinions are divided on the adequacy of the regulatory environment both on the banking side and the insurance side.

On the banking side, for several institutions the duties of control of service providers, notably the right of audit, resulting from Regulation 97-02 of the *Comité de la réglementation bancaire et financiaire* (CRBF –Banking and Financial Regulation Committee), are difficult to uphold, particularly in the case of public clouds. One large international group reports that it would require compliance on the part of the service provider with the national regulations for the protection of personal data for each of the countries in which it has computing resources. Moreover, two major groups believe that the development of the regulation goes beyond the French and even European framework, since a cloud computing provider may operate from any country in the world; in this framework, several companies lean towards an increase in the liability of the service provider (the concept of co-responsibility of processing) as provided for in the draft revision of Directive 95/46/EC on data protection.[5] Finally, one large international group considers that cloud computing is only compatible with regulations if the solutions are encumbered with requirements in terms of location, resilience and control, but that these constraints would cause it to lose its benefit.

[5] In contrast, one institution considers CRBF Regulation 97-02 to be broad enough and well suited. Another banking group even adds that the regulatory environment is already adapted and suitable for outsourcing.

On the insurance side, one organisation considers that the provisions of Article R 336-1 of the French insurance code, for example, do not contradict the sensible use of cloud computing. However, most organisations consider that before allowing management of personal data, cloud computing solutions must comply with the provisions contained in the French data protection and civil liberties law, with a clarification of responsibilities to be given in particular for cases of multiple subcontracting. Some insurers also endorse the idea of an increase in the service provider's liability in the management of data processing. One group would like authorities to establish a certification process for subcontractors providing cloud computing services. Finally, one insurer considers that the regulatory framework is very strict for activities subject to approval (health data) and must regularly evolve with technology.

5. Key lessons and good practices that can be identified.

Based on lessons learned from these initial analyses, the ACP would like to draw some good practices with regard to use of cloud computing services in the banking and insurance sectors.

Firstly, a multi-criteria definition, inspired by that given by the American NIST, and which takes into account the evolving nature of these services (emergence of new providers, new solutions, etc.) can be obtained. This multi-criteria definition has the advantage of properly distinguishing the types of services and their associated risks.

The ACP pays particular attention to services likely to be implemented by companies in the banking and insurance sectors and that are based in whole or in part on public or hybrid cloud solutions, that is, solutions offered by a specialist company to a large number of customers, or where the location of data is unknown, or when the service can be accessed from the internet. In the following sections, it is to these cases that the term cloud computing refers.

Cloud computing services differ from conventional outsourcing of IT services. Cloud computing permanently transforms Information Systems (IS) functions, whether this is the features of the services provided (alignment with those of the cloud mainly with the objective of improving the quality of service delivered) or the origin of these services (outsourcing, primarily to reduce investment costs).

The increasing maturity of solutions on the market is likely to lead many companies to want to make use of cloud computing. It then appears necessary to anticipate future changes by including cloud computing in companies' information systems development strategies, which in particular shall cover the definition of a clear corporate policy on the nature of data and data processing that it is acceptable to outsource.

As the risks associated with cloud computing are many and new (without sufficient hindsight being available), the use of cloud services should only ever result from the demonstration that the benefits they bring are worth the risks taken. The key question of any discussion on the use of cloud computing is the control of information and its degree of sensitivity.

In organisational terms, cloud computing is a major transformation vector for operational processes, for the allocation of roles and responsibilities, and therefore for the organisation of IS functions themselves, but also for relations between the IS function, the Head of Information Systems Security and the different business lines. The introduction of cloud computing will also have a major impact on the necessary roles within the IS functions and therefore represents a problem of management of expertise.

Beyond the issues of organisation and skills raised by the use of cloud computing, the specific risks added to conventional risks associated with any IT outsourcing must be perfectly controlled in the banking and insurance sectors. The peculiarities of cloud computing concern the criteria of information security in particular:

- **Data privacy:** the protection of sensitive and personal data, as well as compliance with banking secrecy, are particularly difficult within pooled infrastructures that can potentially be accessed by local regulatory bodies. This risk is accentuated by the lack of visibility in terms of the location of data and therefore the applicable regulations and the number of stakeholders in a cloud computing solution. The question of data privacy is also an issue in terms of ensuring their effective destruction when the service is terminated, including backups in sites that may be geographically dispersed;

- **Availability of data and processes:** the dispersal of data and the multiplicity of parties involved undermine the company's ability to ensure these criteria. The asymmetric relationship that links the supplier to its customer, characterised in particular by the difficulty of including binding commitments (penalty clauses) on a minimum level of availability, may enhance this risk;

- **Data integrity:** the use of a cloud computing service creates a risk to the overall integrity of the information system owing to the loss of technical expertise or even dependency on the supplier. More specifically, management by the customer organisation of cloud computing services is more remote and restricted than in other cases of outsourcing, resulting over the long term in a significant risk of dependency: loss of knowledge of the information system and the associated expertise and being tied to the supplier's specific technology may prevent reversibility of the service;

- **Control and evidence:** the deployment of a suitable internal control mechanism is complicated by the difficulties in establishing a balanced contractual relationship, in auditing the service provider (multiplicity of stakeholders, potentially global geographic location, etc.) and in identifying the regulatory rules that apply to the data.

Architecture and organisation: use of a cloud-based IT service is likely to cause problems relating to integration in the information system and to reduce the system's flexibility and scalability in the medium term. The difficulties that arise are both technical (potentially inadequate integration of a highly standardised component in an information system) and sometimes organisational (ability of the IT organisation to adapt to sometimes very frequent changes in the cloud service).

While recognising the value that can be found in the use of cloud computing services, it is important not to commit to such a solution without having ensured perfect management of the risks identified. As such, compliance with existing regulations on internal control (R. 336-1f of the Insurance Code, R. 211-28f of the Mutual Insurance Code and R. 931-43f of the Social Security Code or CRBF Regulation 97-02) is an essential element:

- with regard to outsourcing of critical services or other important tasks, it is not obvious that functions considered as "support functions" are not, in practice, to be regarded as critical or important, given the role they play in the realisation of certain services and for business continuity (IT resources in particular);

- in terms of the protection of data security and data privacy, the current regulations also apply to cloud services. Services currently provided in the cloud may contain customer data, therefore confidential or sensitive information that is covered by professional secrecy (customer relationship management, messaging, archiving, etc.). Enforcement of the regulations must therefore not simply be done in light of the nature of the "support function" or "business line function" within the company, but rather with respect to the nature of the data likely to be placed in these environments.

The use of cloud services will henceforth tend to grow, driven by business lines that appreciate the ease of use and speed of implementation; and commitment to this type of service is sometimes based solely on a decision by the business line using such service, after consultation with the Head of Information Systems Security. On the contrary, given the significance of the risks, commitment to this type of service should systematically involve the institution's governing bodies, in accordance with good governance of the information system. These bodies should make their decision while having the independent view of the Head of Risk Management and the Head of Information Systems Security if the latter does not belong to the risk management department.

Where they concern core (and/or confidential) activities, the implementation of cloud services must be accompanied by suitable risk management measures:

- **Legal:** the contractual framework of the service is mandatory. The measures for data protection implemented by the service provider must be assessed before subscription to the service. Concerning the protection of personal data, the service must comply with European Directive 95/46/EC and more broadly with the rules of protection of intellectual property. Some elements transferred to the cloud are likely to become part of the company's intellectual property capital and must be the subject of a contractual clause. Moreover, any change in the nature of the service must be controlled, including changes to software versions. The corporate customer using a cloud solution must establish a form of ongoing contractual management, relying on penalty clauses to be applied in the event of shortcomings in the service rendered by the service provider. Finally, the contractual framework must also make it possible to obtain visibility into the service provider's organisation, particularly in terms of any subcontracting;

- **Technical:** in the absence of anonymisation, confidential data entrusted to the service provider must be encrypted during transport and during storage. The encryption solution must be controlled by the owner of the data (which implies that key management is performed by the company subject to the supervision of the ACP), and particular attention must be paid to the segregation of environments between customer companies and to the management of access rights;

- **Supervision of the service provider:** the ability to audit and the right to do so for the ACP is an essential contractual clause for any provision of cloud computing services. Conducting regular audits is expected. Conducting penetration and vulnerability testing is necessary for supervision of the service as is access to audit trails previously identified (the principle of partitioning data between different customers also applies to these trails). Certification of the service provider alone should not be considered as a measure of adequate risk control. It is necessary to maintain permanently the list of suppliers of cloud computing as well as the list of services that are entrusted to them;

- **Continuity of the service:** it is crucial for SLAs to be in place; these make it possible to formalise the expectations of the client company. Specific commitments on the part of the service provider are expected with respect to business continuity (including the maximum duration of downtime and the maximum allowable loss of data). Monitoring of the service must be based on reports on the availability, security incidents and location of the data;

- **Reversibility of the service:** conditions of reversibility must to be defined when subscribing to the service. Issues of the format of returned data and their destruction must be covered in the contract between the parties. This ability to withdraw from the service provider also leads to constraints on the side of the customer organisation. The latter must in effect ensure its ability to re-absorb the outsourced activity or to transfer it to another service provider with sufficient reactivity (management of functional, application-based and technical knowledge, ability to position resources and to develop their skills, budget allocation, etc.). Dependence on the provider of the cloud computing solution should be assessed regularly;

- **Integration and architecture of information systems:** the establishment of an appropriate organisation of the IT department, taking into account all external constraints on the company caused by a cloud service, as well as control of the architecture and development of the information system, are pre-requisites for the use of a cloud computing service. It is important that the provision of IT services remains the responsibility of the Information Systems department so that this is able to effectively manage the consistency of a broader information system.

All of these good practices form part of the broader framework defined for the supervision of outsourced critical services, including conventional outsourcing. The expectations in terms of governance of decisions, risk analysis, contractual elements, monitoring and the internal control of cloud computing services are therefore similar to those currently in force in prudential supervision.

Appendix: Survey on cloud computing (questionnaire sent out)

Purpose of the survey

In conducting this survey on cloud computing, the goals of the ACP are:

- to determine whether this concept or technological and commercial solution creates new risks in the banking and insurance sectors,
- to assess whether current security policies and regulations sufficiently address these risks,
- to collect suggestions.

1. Characteristics of cloud computing

Cloud computing consists in using remote servers to store and process data traditionally located on local servers or on the user's terminal. It enables on-demand and self-service network access to virtualised and pooled computing resources typically charged for on a pay-per-use model.

In its most common forms, cloud computing provides the following types of resources:

- IT infrastructure, such as computing power, virtual machines including an operating system, storage, and backup services. This is known as Infrastructure as a Service (IaaS);
- An integrated development and/or runtime platform, based on a catalogue of standardised software and technical components whose underlying infrastructure is invisible to the user. This is known as Platform as a Service (PaaS);
- An application-based solution addressing a specific field of use supporting a business function (customer relationship management, financial management, etc.) or a cross-functional service (messaging, collaborative tools, etc.). This is Software as a Service (SaaS).

There are several forms of cloud computing:

- internal private clouds, managed internally by a company for its own needs and on infrastructure that it owns,
- external private clouds, dedicated to the needs of one company or a group of companies but hosted by a service provider,
- public clouds,[6] managed by specialised companies that lease their services to many companies,
- hybrid clouds, dynamically combining public and private clouds.

Public clouds are a special form of IT outsourcing in which services are pooled for a large number of customers and customers are usually not informed of the location of data in the cloud.

Gartner defines cloud computing as:

"*A style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies.*"

In the following survey, questions relate to forms of cloud computing involving a service provider (external private clouds, public clouds and hybrid clouds).

*

[6] The word "public" here refers to the meaning commonly used by cloud computing stakeholders, that is to say an open and multi-client environment. It does not refer to initiatives by the sphere of government.

Question 1.1 – Do these defining elements accurately describe cloud computing services in the banking and insurance sectors? Do you see any other characteristics to further define the concept?

Question 1.2 – In the banking and insurance sectors, what are the key differentiators between cloud computing and conventional outsourcing?

Question 1.3 – Given your existing infrastructure, can cloud computing meet an economic need?

Question 1.4 – Do current cloud computing services as they currently stand appear to pose risks for you? (please specify)

2. Uses of cloud computing

Question 2.1 – In your opinion, what are the benefits driving the move toward a cloud computing approach in your fields of business? Which departments are initiating this move?

Question 2.2 – In your opinion, what are the factors slowing the adoption of cloud computing in your fields of business?

Question 2.3 – What are the applications or IT services for which you use or could use cloud computing services:

- **In the support functions (HR, accounting, data storage, data archiving, etc.)?**
- **In the area of office automation and collaboration tools (email, team site, etc.)?**
- **In the area of retail banking?**
- **In the area of corporate and investment banking?**
- **In specialised areas such as credit to individuals or businesses?**
- **In the area of life insurance?**
- **In the area of property and casualty insurance?**
- **In the area of reinsurance?**
- **In the specialised area of health?**
- **In other areas?**

And what type of cloud computing?

Question 2.4 – Conversely, what are the applications or IT services for which you would not use a cloud services provider (please explain)?

Question 2.5 – At what level of governance of your company is (would) this type of decision (be) taken?

Question 2.6 – Does your institution offer cloud computing services itself, for example, to customers or other institutions?

3. The legal environment of cloud computing

Question 3.1 – What do you think about the legal restrictions affecting the potentially extra-territorial storage and the protection of data?

Question 3.2 – If you have already subscribed to a cloud computing service, what were your contractual requirements with regard to the cloud service provider in terms of the security of data and data processing (confidentiality, integrity, availability) and the auditability of the services provided?

Question 3.3 – If you have not subscribed to such a service, what would be your main contractual requirements in terms of data protection and supervision of the service?

Question 3.4 – How do you assess the different types of cloud computing with regard to obligations relating to outsourced critical services?

Question 3.5 – In your opinion, is the regulatory environment governing the outsourcing of activities subject to approval suited to the characteristics of cloud computing services?

Question 3.6 – In your opinion, are European and national laws and regulations relating to data protection suited to the characteristics of cloud computing services?

Question 3.7 – In your opinion, in the event of dissatisfaction with cloud services, what are the key factors ensuring a successful re-internalisation process (reversibility, etc.)?

4. Risks and security measures associated with cloud computing

Data security is a fundamental issue for companies. With cloud computing, the service provider is largely responsible for security measures to ensure:

- data confidentiality and integrity (including in the event of service termination),
- protection from data loss,
- continuity of service,
- quality of service.

Question 4.1 – What risk analysis methodology do you use or would you use to identify the security objectives to be met and to define security requirements?

Question 4.2 – Appropriate security measures are required to protect assets (data and applications or infrastructure services). In your opinion, which measures are essential for:

- Ensuring data confidentiality?
- Avoiding data loss?
- Ensuring continuity and quality of service?

Question 4.3 – In your opinion, does the lack of control over the location of data require specific security measures? Is it necessary to encrypt data before they are hosted in the cloud, and do you think this requirement would be applicable? If so, to which elements do you think it should be applied (data transport, data storage, key management procedures, etc.)?

Question 4.4 – If cloud computing is used, how do you control or how would you control the level of security? Is the ability to conduct an audit a prerequisite for use of a cloud computing service?

61, rue Taitbout
75009 Paris
Téléphone : 01 49 95 40 00
Télécopie : 01 49 95 40 48
Site internet : www.acp.banque-france.fr