Anticipating Risks and Adopting Cloud Computing with Confidence

Cindy Roth

May 2015

In partnership with

Business Digital Security
Secure & Accelerate Your Business

∑trategy Paper

CEIS is a strategy and risk-management consulting firm. Our mission is to help our clients grow in France and abroad and contribute to the protection of their interests. To do this, we systematically combine a prospective outlook with an operational approach, and management of information useful for decision-making with support of our clients' activities. CEIS particularly focuses on the field of digital trust and is one of the founding members of the Cloud Confidence association. This association, which brings together more than 15 cloud players, providers (SaaS, IaaS, PaaS, etc.), users and members of the cloud ecosystem, aims to accelerate cloud use for the benefit of its clients and the economy.

This white paper was written in partnership with ATIPIC Avocat and Business Digital Security (https://business-digital-security.com).

- Business Digital Security is a strategy consulting firm that focuses on the fields of cybersecurity, digital affairs and information technology in general. This trusted partner's mission is to support its clients in harnessing digital resources to create business value and in using cybersecurity to protect this value, and to facilitate relationships between end users and providers.

- ATIPIC Avocat is a law firm dedicated to all aspects of law relating to new technologies (technology, information, intellectual property and communication). We combine the most rigorous legal analysis with our in-depth understanding of technical operations and experience in the world of business to offer pragmatic and operational solutions that take all existing requirements into account.

"Discontinued products and services are nothing new, of course, but what is new with the coming of the Cloud is the discontinuation of services to which people have entrusted a lot of personal or otherwise important data – and in many cases devoted a lot of time to creating and organizing that data. As businesses ratchet up their use of cloud services, they're going to struggle with similar problems, sometimes on a much greater scale. I don't see any way around this – it's the price we pay for the convenience of centralized apps and databases – but it's worth keeping in mind that in the Cloud we're all guinea pigs, and that means we're all dispensable. Caveat cloudster."[1]

NICK CARR, author of *Does IT Matter?*, *The Big Switch* and *The Shallows*

"We believe we're moving out of the Ice Age, the Iron Age, the Industrial Age, the Information Age, to the participation age. You get on the Net and you do stuff. You IM (instant message), you blog, you take pictures, you publish, you podcast, you transact, you distance learn, you telemedicine. You are participating on the Internet, not just viewing stuff. We build the infrastructure that goes in the data center that facilitates the participation age. We build that big friggin' Webtone switch. It has security, directory, identity, privacy, storage, compute, the whole Web services stack."

SCOTT MACNEALY, ex-CEO of SUN MICROSYSTEMS

[1] *The Cloud giveth and the Cloud taketh away*, 23 November 2011: http://www.roughtype.com/?p=1553 (accessed on 30 April 2015).

ceis

Summary

Preface

Perhaps you are using it without really knowing what it is. Perhaps your employees have adopted it without informing you. Whatever the case, your company may belong to the 30% of business organisations that use cloud computing services.

The concept of cloud computing is on the rise. The aim of this white paper is to equip the client with everything it needs to take a reasoned approach to adopting a cloud service and to manage the associated risks. The goal is to provide the client with a powerful tool for managing, reporting and discussing major risks with top management, Risk Management/Compliance, professional departments and internal Auditing/Monitoring. This white paper is part of an effort to equip the client with a detailed and ongoing knowledge of its cloud environment and its strategic providers.

Introduction

Cloud computing may be defined as "*a means of handling a client's data in which operations are carried out over the Internet, in the form of services rendered by a provider*"[2]. The term 'cloud computing' was not selected by chance. For the client, it conjures up a mental picture of its data being stored everywhere and nowhere at once. The operational lightness and simplicity that is implicit in such a mental picture is merely superficial. In reality, even if the client does not immediately pick up on all of the ins and outs of cloud computing, it must deal with a complex mechanism that comprises several levels of service (IaaS, SaaS and PaaS). Software as a service (SaaS), the means of commercial operation of the software most commonly used by companies, existed well before the emergence of cloud computing.

The client also seeks cloud services that operate worldwide, with uniform performance regardless of the country of access. However, this often entails storing information at data centres in different countries on different continents. Before subscribing to a cloud service, the client must be aware that its data may be stored in China, the United States or South Korea. It is therefore essential to investigate the provider so that the client holds the keys and is familiar with the foreign legislation that is likely to apply.

We believe that the plan we are going to offer you will enable you to grasp the various facets of the Cloud and discover solutions that will reduce risks and enable a company to make the most of the opportunities available. While we sometimes present issues in a linear fashion, we do so bearing in mind that most issues are intrinsically linked. In addition, we find it more relevant to classify risks according to their impacts for the client.

Different categories of intrinsic risks to the provider and its service may be identified with a view to recognising risks, monitoring them throughout the life cycle of a subscription to a service and putting them into perspective with the client's professional issues and organisation.
Does the client know where its data are being hosted? Is it informed of the incidents that arise? Can it conduct audits? How are the data it holds (which are its own property or that of its clients) being handled or transferred? From one service to another? Can it recover these data? Be assured of their deletion? What traceability tools does it have at its disposal? How is the end of the contract organised? Is the client technologically dependent? Managing its data and

[2] Official Journal of the French Republic, 6 June 2010, p. 10453: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022309303 (accessed on 9 March 2015).

information systems necessarily involves being aware of the governance risks it is contemplating taking (I).

In order for the provider to win the client's trust, it must disclose information about itself and its legal environment (parent company, subsidiaries and shareholding structure). This is all the more necessary given that in recent years the cloud service market has witnessed the emergence of a host of new companies with different sizes that give little information about themselves. Several questions, then, arise regarding the provider's financial soundness. How long has the company been in business? What is the provider's interest in its activities in France? Can the client enter into a contract with the provider without the risk that the provider will later go out of business? Is the company owned by another company? Does the provider own its data centres? Other questions have to do with the provider's reputation. Has the provider experienced any financial troubles requiring the commencement of insolvency proceedings? Are its managers free from blame? Such are the risks linked to providers that should be analysed (II).

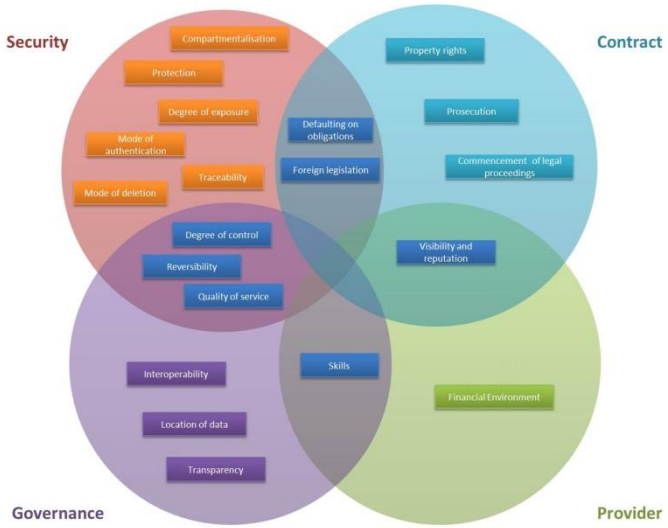
On a legal level, regarding the few issues not already mentioned above, a lack of information and caution may endanger the client's property rights over its data, especially if the data in question correspond to a work, patent or model subject to intellectual property rights. In addition, the client risks prosecution if it does not monitor its provider's activities. Such are the matters that must be provided for in the contract (III). The legal risks are also closely linked to the level of security surrounding data handling.

As regards information systems security, issues and risks relate to data confidentiality, availability, integrity and traceability (IV). Does the provider offer a means of deleting or destroying all the data at the end of the contractual relationship? Are staff members and subcontractors bound by confidentiality obligations? What are the means implemented to fight against the risks of physical and electronic intrusions? Does foreign legislation apply? How secure is the authentication of platform users? What level of service is offered by the provider? Are there means of ensuring the traceability of user activities?

All the above are risks that should be analysed before entering into any business relationship and, more importantly, into any contractual relationship. Indeed, with a bit of vigilance and a well-negotiated contract, the service may prove to be much more secure than internal resource management. Good strategy management necessarily involves a risk analysis. Certain associations such as Cloud Confidence aim to "*ensure the transparency of cloud services,*

manage business and legal risk, and promote a space for exchanges without infringing upon the principles of personal data protection".

A comprehensive vision that is regularly updated is all the more necessary to grasp the complexity of the Cloud and enjoy the simplicity its services offer without any nasty surprises.



1. GOVERNANCE RISKS

1.1. Risks linked to poor reversibility of data

What is reversibility of data? All information technology contracts that include outsourcing of services — in which a service is managed not internally by the company but by a third-party provider — come to an end at one time or another. This means that the client must be able to completely or partially recover the information technology environment that it entrusted to the third-party provider in order to orchestrate its transfer to another provider. This need for reversibility exists regardless of the reason why the contractual relationship ended: normal expiry, force majeure, client choice or failure of one of the parties to uphold the contract.

In cloud computing, it is necessary to be aware that complete and simplified reversibility of data is difficult to achieve. In negotiating the provisions of the contract, the client may minimise risks and make offers that facilitate reversibility in terms of formats and deadlines. In SaaS, data repatriation seems fairly simple, as it is standardised. However, integrating data from a SaaS application into an internal application can pose problems. In this case, the client will find itself in a lock-in situation, wherein it will be technologically and commercially dependent on the cloud provider and unable to switch providers at will. If the contract must end for any reason whatsoever, the client risks being unable to recover its data or ending up with data that cannot be used.

For this reason, certain services do not always guarantee the portability of data, applications and services. In practice, this means that the choice of a cloud service provider must be reviewed very carefully by the various company departments concerned. Meanwhile, technical solutions that circumvent this problem are being developed. For example, Docker, an open-source software program, makes it possible to toggle an application — placed in a virtual storage unit — between the cloud service platforms offered by Amazon, Microsoft and Google[3]. All the same, the client must be vigilant: open-source software programs do not offer the same security guarantees as licensed software programs.

[3] Crochet-Damais, Antoine. *Cloud : pourquoi Docker peut tout changer* (The Cloud: Why Docker May Change Everything), JDN.net, 13 February 2015: http://www.journaldunet.com/solutions/Cloud-computing/docker-definition-avantages-inconvenients.shtml (accessed on 27 April 2015).

However, legal solutions are available. First of all, a provision in the contract for reversibility should include several elements to limit the risks of data loss and technological dependence:

- The duration of the reversibility phase will vary depending on the client's needs. If the client stores its data in the Cloud for several years, it may easily be imagined that a 30-day period is much too short. An order issued on 30 November 2012 by the Regional Court (TGI) of Nanterre, in the case *UMP vs Oracle*, established a period of no less than 2 months in that case. It is also important to specify the starting point of this period.

- It is very important to determine the restoration format so that the client is able to use its data after the contract expires. The client is often offered a Microsoft format such as .csv. Nevertheless, it is better off if a format is identified that meets all its reversibility needs according to its information technology environment. The difficulty of transferring data to another cloud service from a third-party provider is also to be taken into account.

- The means of calculating the costs of reversibility are to be specified. Indeed, reversibility may be free or paid at the rate applicable at the time of the reversibility notification.

Following that, a detailed reversibility plan may be established and annexed to the contract. The plan should be updated, supplemented and/or amended at regular intervals between the parties.

1.2. Risks linked to a lack of interoperability

Certain cloud service providers enter into partnerships with other providers in order to allow interoperability of services. For example, the Microsoft–Salesforce partnership allows the clients of one company or the other to "*access, share, edit and collaborate on Office content from within Salesforce and on Salesforce1 using Office Mobile, Office for iPad and Office 365*"[4]. However, this is not always the case. Many providers wish to impose their standards to keep

[4] *La revue du digital. Microsoft et Salesforce resserrent les liens entre Office365, le CRM et Windows* (Microsoft and Salesforce Tighten the Links Between Office 365, CRM and Windows), 30 May 2014: http://www.larevuedudigital.com/2014/05/30/microsoft-et-salesforce-resserrent-les-liens-entre-office365-le-crm-et-windows (accessed on 4 March 2015).

clients from using other platforms (PaaS) or other services (SaaS). An open-platform model that gives rise to the availability of APIs is to be preferred.

While the cloud market is set to sky-rocket in the next few years, certain major players are lobbying hard to impose their standards. Discussions to draw up worldwide standards are under way at a national level. Opinions on this point are divided. According to Olivier Teitgen, project manager in the department of transportation, energy and communication at the French standardisation association (AFNOR) and secretary of the cloud standardisation commission in France, "*to impose standards (...) is to interfere with the business policy of providers*".

If standards are not publicly available, the provider must be asked to supply them so that a fully informed decision may be made.

1.3. Risks linked to a lack of information transparency

Provider transparency is a gauge of client trust. For this reason, and given that transparency will in any case soon be required by law, the cloud service provider must be prepared to inform the client of any incident, attempted system intrusion or personal data protection violation that concerns or potentially concerns the client, even if only as a matter of image. This notification, to which both the client and the entity responsible for handling the data may be legally bound, must be coordinated between these two players (crisis management, public relations, etc.).

To ensure this transparency, the client must be authorised by the provider to conduct, commission, use and have access to the results of audits, vulnerability tests and intrusion tests in relation with the provider's information technology assets to be assured of the overall service level, knowing it will be responsible for this security for its own clients.

This ability to conduct technical audits may be specified in the contract. The provider may offer the client the possibility of monitoring if it complies with established "security" technology frames of reference. The contract must specify several matters:

- The means by which audit procedures may be triggered (e.g. an alert provided with an agreed-upon advance notice);

- The frequency of audits (e.g. at least once per year); and

- The individuals authorised to conduct audits. It is advisable to hire an external auditor not affiliated with either party. In this case, a confidentiality agreement will be necessary. The expenses will be borne by the client.

It should be noted that, according to an analysis by the French Prudential Supervisory Authority (ACPR) on cloud computing published in July 2013[5], the banking and insurance industry affords itself, in an obscure way, all the latitude necessary to consider a simple support service to be an outsourced essential service from the time it is rendered on the Cloud. It must be remembered that outsourced essential services refer to "*services and other essential or major operational tasks*" introduced by the French Banking and Financial Regulatory Committee (CRBF) in its regulation no. 97-02, replaced by the order of 3 November 2014, imposing very specific constraints on financial institutions (specific clauses, ACPR right to audit, etc.). There is, then, potentially strong regulatory pressure spelling out and requiring in practice that banks oblige require their cloud service providers to guarantee that they will live up to their obligations[6].

By contrast, examples such as the 2014 Code Spaces affair show that it is not enough to rely on a service that allows sophisticated security solutions to be set up. The client itself must still activate and respect them, in order not to be held responsible by its clients or jeopardise its own existence. In this case, Code Spaces, a source code hosting company, failed to secure its authentication methods, and as a result, its account on the Amazon Web Services cloud platform it used was hacked. In the course of the company's struggle to regain control of its cloud account, the hacker destroyed the files stored on it. This caused the company to go out of business in 2014. Its end clients never recovered their data.

[5] ACP. *Analyses et Synthèses, Les risques associés au Cloud computing* (Analysis and Synthesis: The Risks Associated with Cloud Computing), no. 16, July 2013: http://www.acp.banque-france.fr/uploads/media/201307-Risques-associes-au-Cloud-computing_01.pdf (accessed on 1 April 2015).
[6] Coupez, François. *Pour l'ACPR, prestations dans le Cloud = externalisation de prestations de services essentielles (PSEE)* (For the ACPR, Cloud Services = Outsourced Essential Services). ATIPIC Avocat Blog, 25 September 2014: http://blogatipic-avocat.com/retour-vers-le-futur-1-juillet-2013-lacpr-et-le-Cloud-computing (accessed on 10 March 2015).

1.4. Risks linked to a lack of information on the location of data

To maintain control of its systems and data and meet existing obligations regarding the protection of the personal data it might handle, the client must know the locations of the data centres storing its data. However, it is often complex to pinpoint the location of data because it may be moved very quickly from one continent to another. Some providers opt for transparency and reveal the location of their data centres, disclosing at least the host country. It should be added that some providers, particularly smaller SaaS providers, may also rent their data centres, thereby complicating the task of reconstituting the "chain of transmission" of data.

2. PROVIDER RISKS

While the cloud market in France is expected to continue its double-digit growth in 2015 (21%, according to the firm Xerfi, versus 20% in 2014), there is a growing trend among large CAC 40 groups, anxious about the security of their data following the revelations of the PRISM affair, to work with French SMEs and subscribe to "local" services. Consequently, Salesforce, IBM, Microsoft and SAP have announced that they will open data centres in France by the end of the year.

At present, French providers are found in all cloud computing industries (IaaS, PaaS and SaaS), although American providers largely dominate IaaS and PaaS. France is home to many companies in the SaaS segment, for most niche players. Moreover, the cloud industry is expected to become heavily concentrated in Europe (through mergers and acquisitions) over the course of the next few years. All the above make choosing the "ideal" provider complex for organisations lacking substantial financial and therefore technical means: "the mistake", i.e. dealing with a company that goes bankrupt within a few months of signing the contract, may come at a high price. The clients of the company *Code Spaces*, which presented its service as "rock solid", can attest to this (see above).

While companies seek guarantees with respect to governance and security, they will also be anxious to forge business relationships with companies that are financially and legally sound and renowned for their expertise. These things go beyond mere sales brochures and promotional materials on social networks.

2.1. Risks linked to a mismatch in the provider's skills

Given that the industry is still taking shape, questions arise as to who is behind the trade names. A provider's degree of credibility may be assessed by investigating the company's history and the paths its managers and shareholders have taken. If said managers are found to be "marketers" or investors present on several markets at once, are they surrounded by a team with the necessary technical skills to offer a quality service? Does the provider's board of directors comprise information technology experts? Or has it delegated "technical" matters to subcontractors, thus adding another link to the chain of representatives? *In sum*, the client must be assured that it is working with "serious people" with "spotless" professional ethics. An initial investigation will shorten the list of potential providers.

2.2. Risks linked to an uncertain financial and/or legal environment for the provider

In order to prevent any risks linked to entering into a business relationship, it is essential to learn about the cloud service provider's legal and financial situation.

Indeed, many providers find themselves in a fragile economic situation or have been in the business for just a few years. A preliminary investigation will reveal whether the provider has gone through bankruptcy proceedings, reached a certain milestone in terms of activities (years of existence, number of employees, etc.), managed to turn a profit, etc. The provider's degree of interest in its French subsidiary is also a strong indicator: will it provide its subsidiary with financial support if needed, or will it opt to "sacrifice" it in favour of more profitable markets? For example, an American provider such as Salesforce has a great deal of interest in France and the French market, and as such is supported by the public authorities. The fact that Fleur Pellerin, former French Secretary of State for Foreign Trade, attended the opening of Salesforce's new Paris offices last June testifies to this support. Conversely, a weak interest in the French market owing to, for example, requirements regarding the location of data centres, or an attractive service associated with a hazy legal environment and moribund financial health, should alert the client to the viability of the entity's operations.

To ward off nasty surprises and maintain a certain level of control over its data, the client company must know whether the cloud service provider is independent and who is giving the orders. Was the provider acquired? It is also essential to know whether the provider owns its data centres. It may be less reliable in fulfilling its commitments if it does not manage them. In this case, it will be useful to conduct research to identify the operator of the data centres.

2.3. Risks linked to poor quality of services offered

To address this third and final important matter, the client must go beyond a "cold" study of the solutions offered by the provider. It must gather information through open sources or interviews on critical testimonies, whether positive or negative, on the availability of the company's leadership, on the means it has implemented to meet its clients' expectations and on the quality of the service offered. Too often, purchasers "overlook" these matters and prioritise financial considerations. Moreover, when the provider has relatively little visibility, it must be known whether the provider has an up-to-date and diversified client portfolio. If no trade referral is identified, it will be important to ask the provider for a recent client list.

3. CONTRACTUAL RISKS

A clause in the contract may list the documents that govern the contractual relationship, annex them, exclude them and specify a document hierarchy. The contract and its annexed documents will constitute the entirety of commitments made and supersede all prior spoken and written commitments. In the event of conflict, the document that ranks higher in the hierarchy prevails (see the diagram below; note that the list of contract documents mentioned is not exhaustive).

3.1. Risks linked to property rights

A contract between a cloud service provider and a company may force the company to give up some of its rights over its data. For example, Google Drive's general terms of service specify that the client remains the owner of the content uploaded to its service. However, Google more vaguely reserves the right to use these data for the purpose of "improving [its] Services"[7].

To whom, then, do the data stored on the Cloud and subject to copyright, trademark rights and software rights belong? The answer to this question may seem unclear, given that some foreign

[7] ZDNet. *A quel point Google Drive est-il propriétaire de vos données ?* (To What Extent Does Google Drive Own Your Data?) 25 April 2012: http://www.zdnet.fr/actualites/a-quel-point-google-drive-est-il-proprietaire-de-vos-donnees-39771132.htm (accessed on 26 February 2015).

economic players would sometimes like to impose rules that are not applicable (French intellectual property law does not contain any provisions that grant the provider any rights by virtue of storage on the Cloud *per se*). A response may readily be provided in the form of a clear contract clause. The contract serves as the "*law between the parties*". While mere storage on the Cloud does not grant the provider any specific rights, the provider may include in the contract, or a document that falls within the contractual framework, a clause specifying that the transfer of rights remains possible in a B-to-B relationship[8]. In any event, it is a good idea to recall, in an unequivocal clause in the document at the very top of the contractual pyramid presented below, that the client is and remains the owner of all the data that it uses through the services made available to it within the framework of the contract. The provider, for its part, remains the holder of the property rights over the information technology services and infrastructure it makes available to the client.

3.2. Risks of prosecution

Certain types of data in certain industries require specific measures. The client must comply on pain of liability. For example, the banking industry is subject to very strict internal monitoring regulations,[9] as is the insurance industry[10]. In the medical industry, the cloud service provider must be authorised by the French minister in charge of health to host health data[11].

[8] In a B-to-C relationship, the regulations that protect consumer rights could protect the consumer by declaring certain clauses to be "abusive" and therefore null and void. See recommendation no. 2014-02 "regarding contracts proposed by social networking service providers", which was adopted on 7 November 2014 by the French Commission on Abusive Clauses (available at http://www.clauses-abusives.fr/recom/14r02.htm). Among the 46 specific proposals issued in the document, 27 may apply to any electronic commerce site, and nine may apply to any site that handles professional data for a large client base. For a full analysis of this recommendation, see ATIPIC Avocat Newsletter no. 1, available at http://www.atipic-avocat.com/app/download/10877446/2015-1-Newsletter+ATIPIC+Avocat+JanvFev.pdf.

[9] CRBF regulation no. 97-02 of 21 February 1997, repealed and replaced by the order of 3 November 2014, available at Legifrance (accessed on 22 February 2015).

[10] Article R. 336-1 of the French Insurance Code, amended by decree no. 2014-1315 of 3 November 2014, available at Legifrance (accessed on 22 February 2015).

[11] Article R. 1111-10 of the French Public Health Code, amended by decree no. 2011-246 of March 2011, available at Legifrance (accessed on 22 February 2015).

3.2.1. The case of personal data

According to Article 2 of the "Information Technology and Civil Liberties" law of 6 January 1978[12], "*personal data consist of any information relating to a physical person who is identified or may be identified, directly or indirectly, by referring to an identification number or one or several elements unique to said person".* Information such as first name, last name or address of a client, employee or prospect constitutes personal data.

A client company that stores and handles these data is called a data controller[13]. It must take some specific precautions. Indeed, according to Article 34 of the 1978 law, the client must "*take all necessary precautions with respect to the nature of the data and the risks posed by their handling, to protect the security of the data and, in particular, prevent them from being distorted, damaged, or accessed by third parties".* It may choose to delegate the management of data handling, as in cloud computing, but it must ensure that the provider is offering all "sufficient guarantees" in terms of technical security. This is because, in any event, it only delegates handling, never responsibility for the data itself, as demonstrated by the sanction against the Orange company issued on 7 August 2014: client data were unduly accessed, not as a result of an attack on Orange's information system as such, but because the subcontractor of a subcontractor of Orange was the victim of a security breach[14].

In addition, Article 68 of the same law prohibits the transfer of personal data outside the European Union unless sufficient security guarantees are provided. Certain formalities imposed by the French National Commission on Information Technology and Civil Liberties (CNIL) are to be followed (standard contractual clauses, authorisations).

Regarding transfers to the United States, the American company or its subsidiary abroad must appear on the Safe Harbor list on the website of the U.S. Department of Commerce and fulfil the conditions for the protection of personal data, with the proviso that certain industries (the financial industry) are excluded from the agreement and that a provider adhering to the system in an entirely voluntary manner may cease to do so at any time. This adherence to Safe

[12] Law no. 78-17 of 6 January 1978 regarding information technology, files and civil liberties, available at Legifrance (accessed on 22 February 2015).
[13] Article 3 of the above-mentioned "Information Technology and Civil Liberties" law, available at Legifrance (accessed on 21 February 2015).
[14] See the sanction ruling by the French National Commission on Information Technology and Civil Liberties (CNIL) at http://www.cnil.fr/linstitution/actualite/article/article/la-societe-orange-sanctionnee-pour-defaut-de-securite-des-donnees-dans-le-cadre-de-campagnes/

Harbor, then, is to be monitored very carefully over time and calls for a specific framework. In March 2015, in a case of Facebook versus an Austrian Internet user and the Irish CNIL, the attorney for the Austrian government stated, "*Safe Harbor is not adequate for the data of EU citizens, but is at best a safe harbor for data pirates".* The user refused to allow his personal data to be used by American giants without his prior control. The ECJ is to issue its opinion on 24 June 2015[15].

The client is therefore advised to specify in the contract that the provider shall adhere to Safe Harbor throughout the duration of the contract and to reinforce the level of its obligations in the contract, as needed. It could then be preferable to sign the above-mentioned standard contractual clauses to protect the client from any disappointment arising from a provider that would cease to adhere to Safe Harbor some time after the contract goes into effect.

Indeed, it must be remembered that the client will incur penal sanctions should it fail to comply with the provisions of the "Information Technology and Civil Liberties" law, even if it delegates the management of data handling to a cloud service provider. In practice, the client will particularly incur sanctions from the CNIL. For the time being, matters of image outweigh the financial sums handed down (which only rarely exceed €100,000). However, this could change quickly and dramatically. There has been talk of sanctions set at a percentage of worldwide annual revenue (2-5%?), reinforced by the future information technology law (late 2015?) and, of course, by the European regulation on the protection of personal data. The wording of this bill is still under discussion, but it seems possible that it will be adopted in late 2015 or early 2016.[16]

Lastly, insufficient information on a cloud service's handling operations poses a risk for data controllers and concerned individuals, because if they are not informed of threats and potential risks, they will not be able to take the measures that they deem most appropriate. This could be considered a violation of individual rights with regard to data access, rectification and deletion owing to a lack of opportunities to intervene[17]. In practice, this is above all strictly contrary to an essential principle introduced by the above-mentioned European draft regulation:

---

[15] JournalduGeek.com. *[Safe Harbor] La Commission européenne conseille de quitter Facebook pour échapper à la NSA* ([Safe Harbor] The European Commission Advises Leaving Facebook to Escape the NSA). 30 March 2015: http://www.journaldugeek.com/2015/03/30/safe-harbor-commission-europeenne-quitter-facebook-echapper-nsa (accessed on 9 April 2015).

[16] A two-year period must elapse before the law may apply in all the countries of the European Union. The transposition phase that a directive would undergo is bypassed.

[17] Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing adopted on 1 July 2012.

accountability. This is essentially the data controller's obligation to not only ensure that a given datum is traceable at every step, from birth to death, but above all prove that capable of ensuring said traceability. Once this regulation is adopted, compliance shall be ensured, it being understood at the same time that the provider could hold joint legal responsibility for the protection of personal data. This will encourage the provider all the more in its pursuit of traceability and visibility.

3.3. Difficulties of the commencement of legal proceedings

It is important for the client to know which law governs the contract and before which court it may assert its rights. A client will have more or less bargaining power depending on the amount that the contract will earn the provider and its own weight on the market. In any case, it will be necessary to contemplate a contractual clause that expressly sets out the applicable law and jurisdiction. The client must keep in mind that the commencement of French legal proceedings will be much easier and less expensive than the commencement of foreign legal proceedings, the cost of which varies by country. In practice, the country in which legal proceedings commence in the event of dispute is a usual subject of negotiation between parties from different countries, and arbitration often offers a consensus solution.

4. SECURITY RISKS

The security risk factors intrinsic to the cloud provider and its platform are many and may infringe upon the confidentiality, integrity and availability of the service and of the data entrusted to the provider, and impact the client organisation (loss of reputation, loss of client trust, loss of revenue, etc.). Below is a non-exhaustive list of risks and risk-reduction measures.

Some start-ups specialise in cloud platform security. This is true of CipherCloud and Elastica, which provide encryption and data protection solutions as well as vulnerability assessments.

4.1. Risks linked to unsatisfactory deletion of data

At the end of the contract, each party must agree to return all copies of the documents and materials containing information that the client considers confidential. Thus, upon signing the contract, the client must classify the data it is entrusting to the cloud provider. However, it is necessary to double-check the effective destruction of all the data concerned, particularly by specifying in the contract how to destroy said data and how to control said destruction. This is due, on the one hand, to the above-mentioned requirements of the European draft regulation on the protection of personal data and of the datum traceability obligation, and, on the other hand, to the client's potential obligation to uphold specific commitments regarding the deletion of data by its own clients, regardless of the nature of the data themselves (manufacturing secrets, etc.).

Several recommendations have been issued on the subject. They essentially come from military services (U.S. Army, U.S. Department of Defense, U.S. National Institute of Standards and Technology [NIST], etc.), aiming to delete data as securely as possible. Cloud service providers may need to commit to upholding best practices with respect to data deletion and specify the applicable legislation, depending on the client's assessment of the sensitivity of the data handled (Are they personal data? Data with commercial value? Etc.).

4.2. Risks linked to a lack of compartmentalisation of resources

With the public Cloud and a multi-tenant architecture, there is a perceptible risk of data from several clients potentially being decompartmentalised. Technical isolation mechanisms (storage, memory) may be inadequate, and data integrity or confidentiality may be compromised. "High-end" infrastructure offers better data compartmentalisation than less expensive infrastructure and may be likened to a client's own private Cloud.

In addition, the client company must be able to identify the cloud service provider staff members who have access to its data. The provider's staff must follow a strict policy of controlled access to data, especially depending on their nature and sensitivity (health data, banking data, etc.), and sign exhaustive confidentiality agreements.

4.3. Risks of physical and electronic intrusions

According to a study published in June 2014, the annual cost of cybercrime is between 375 and 575 billion dollars worldwide. There are risks of theft of confidential client data, theft of internal operational data and damage to a company's image[18]. In April 2011, the banking data of 77 million users of PlayStation Network, an online games and media service distributed by Sony, were stolen. In 2014, Target, an American department store chain, was hacked. Massive theft of banking data was made possible by an intrusion into the information system of Target's air-conditioning vendor, which was interconnected with Target's information system. No fewer than 40 million bank card numbers were stolen[19]. In March 2015, IBM alerted Dropbox to a security breach affecting its Android application. This problem was resolved thanks to a security patch, but, in practice, a hacker could have gained access to sensitive user information[20].

[18] Plouin, Guillaume. *CLOUD COMPUTING, Sécurité, stratégie d'entreprise et panorama du marché* (CLOUD COMPUTING: Security, Business Strategy and Market Overview). Paris: Dunod, 2013.
[19] Hermann, Vincent. *Le piratage de la chaine Target viendrait de la réutilisation d'authentifiants* (Target Chain Hacking could result of Reuse of Authenticators), Nextinpact.com, 6 February 2014: http://www.nextinpact.com/news/85776-le-piratage-chaine-target-viendrait-reutilisation-dauthentifiants.htm (accessed on 7 April 2015).
[20] Gagliordi, Natalie. *IBM uncovers severe vulnerability in Dropbox SDK for Android*, ZDNet.com, 11 March 2015: http://www.zdnet.com/article/ibm-uncovers-severe-vulnerability-in-dropbox-sdk-for-android (accessed on 12 March 2015).

Thus, the client organisation must ensure, among other things, that the provider has technical procedures and processes in place (reinforced physical and electronic access control for the provider's staff, strong authentication of administrators, database encryption, securing of networks, security event detection, reporting, etc.) that are sufficiently robust to protect data and reduce the impact of a potential breach. The client organisation must ensure that the cloud service provider adheres to a comprehensive certification strategy[21] so that the compliance of its infrastructure and services with good practices and international standards may be recognised. Such recognition of the provider's expertise reinforces the chain of trust between the provider and its clients and partners. The following are examples of certifications to be considered: ISO/IEC 27001, PCI-DSS, SOC 1 Type II and SOC 2 Type II, Cloud Confidence, Cloud Security Alliance STAR, etc. It is also essential to analyse the scope of the certification. While certification does not guarantee a cloud service's level of security, it demonstrates that security matters are taken into account in the service rendered.

4.4. Risks linked to a weak authentication method

The cloud service provider must set up secure user identification and authentication to ensure data confidentiality and integrity. The absence of these guarantees creates a risk for its clients and its clients' clients. Indeed, it is essential to limit access to data.

Authentication, for an IT system, is a procedure that consists of verifying the identity of an individual attempting to access the system before granting access. If the provider does not have an authentication system, an attacker who obtains an administrator password may take full control of the system and, for example, delete all user accounts from the SaaS application, delete all user accounts of a PaaS service or even delete all email accounts of the entire company[22]. One example is the intrusion into Dropbox's online data storage space in June 2012. The hacker got hold of the email addresses of the start-up's clients and sent them spam messages. Following that incident, Dropbox set up a strong authentication system.

The provider must therefore ensure, if possible, a strong two-factor authentication method (for example, one that sends a text message with a unique code to the user's mobile device) to

[21] List of certification schemes referenced by the ENISA: https://resilience.enisa.europa.eu/Cloud-computing-certification

[22] Plouin, Guillaume. *CLOUD COMPUTING, Sécurité, stratégie d'entreprise et panorama du marché* (CLOUD COMPUTING: Security, Business Strategy and Market Overview). Paris: Dunod, 2013.

prevent unauthorised access to and modification of data. The provider must also make every effort to minimise the risks of physical and electronic intrusions.

Once the user of the service (or an administrator belonging to the provider's staff) has been authenticated, the cloud provider must have data access traceability mechanisms. Indeed, the client company must be able to access operations and security traces in order to monitor the security of the cloud platform and the data in real time, make *a posteriori* analyses and accord the information a certain amount of trust.

4.5. Risks linked to the application of foreign legislation

In 2015, China plans to adopt a counter-terrorism bill that would require American companies to hand over encryption keys and passwords and install back doors for monitoring purposes[23].

The American version is older and is known as the Patriot Act, or, more broadly, the Foreign Intelligence Surveillance Amendment Act (FISAA). These laws allow the American government to ask any company based in the United States to open its databases for purposes of counter-terrorism efforts[24]. However, the FISAA's scope of application has not been defined. This law is imposed on all American communications and service providers and their subsidiaries, regardless of location, and on foreign providers of these services that operate on American territory[25]. More concretely, the NSA and FBI may access the data that an American company hosts on the Cloud, whether the data centres are located in the United States or Europe since the Microsoft affair (New York federal court, 25 April 2014). In most cases, they keep providers from informing their clients of this access on pain of penal sanctions (under a gag order).

In France, parliamentary debates are currently taking place regarding the intelligence bill of 19 March 2015 and the access to data — particularly metadata — that it may afford. While it is too soon to make a precise analysis, especially based on mere discussion by the French

---

[23] Flechaux, Reynald. *Mesures protectionnistes chinoises : Obama s'énerve* (Chinese Protectionist Measures: Obama Gets Angry), Silicon.fr, 3 March 2015: http://www.silicon.fr/mesures-protectionnistes-chinoises-obama-senerve-109783.html (accessed on 10 March 2015).

[24] *Sécurité & Stratégie. Enquête au cœur des directions de sécurité et sûreté* (Investigation into Safety & Security Departments) *no. 4*, November 2013: http://www.securite-strategie.fr/international-informatique-en.html (accessed on 21 February 2015).

[25] Bonnet, Florence, Consultant, CIL CONSULTING. *Le Cloud Computing à l'ère post Snowden : et après ?* (Cloud Computing in the Post-Snowden Era: Now What?), 4 June 2014: http://www.village-justice.com/articles/Cloud-computing-ere-post-Snowden,17060.html (accessed on 21 February 2015).

National Assembly, the bill does not appear to seek to allow the level of intrusion and access that American law already grants — far from it.

More generally, a careful review of the applicable legislation reveals that each country has its own regulations, which may be quite specific in the field, and that said regulations will affect the client depending on its data hosting site. While certain cloud providers will only disclose the data that they are invited to disclose by a court decision and will inform their clients, others will disclose data more readily. In France, for example, regulations may also vary depending on whether the data are personal and/or tax data, whether a motion is filed with a judge, for example to have evidence in future proceedings, and even whether the data are used within the framework of criminal proceedings.

In addition, the legislation of each country where the data are hosted may apply. It is therefore essential to fully understand and duly analyse the regulations applicable to the providers in question that could lead them to disclose the data, perhaps without informing its client (under a federal gag order as mentioned above). Specifying the applicable law and jurisdiction in the event of dispute in a contract clause does not in any way guard against this. So-called "public order" provisions that may form part of the local legislation in any given locality prevail over the provisions of contracts agreed upon between parties.

4.6. Risks linked to the provider's degree of exposure

A major American cloud service provider will have more visibility than a second-tier provider and will more likely be targeted in attacks. The question is whether it will be better equipped in terms of security than a small-scale provider. It is important to know the number of attacks, the number of proven incidents and the frequency of these incidents. To be aware of the risks involved, it is vital to know the nature of the attacks. The consequences in terms of risks are not the same for attacks using security breaches than for attacks linked to a phishing attempt. For example, a provider as big as Salesforce.com is regularly, and quite naturally, targeted in phishing attempts. Since there is a human factor in these attacks, preliminary awareness-raising among the provider's staff and clients is necessary to resolve this type of risk.

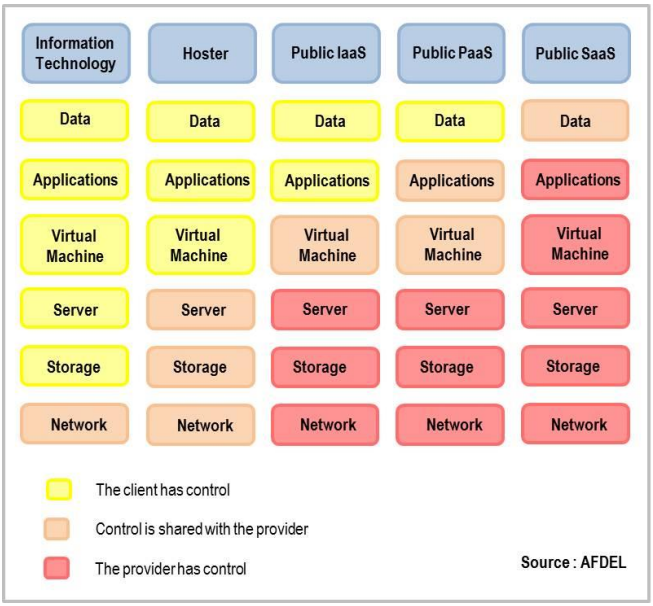
4.7. Risks linked to data integrity

The risks linked to data integrity and the means of protecting oneself from them are quite similar to those that apply to data confidentiality. The provider must ensure, if possible, a strong

two-factor authentication method (for example, one that sends a text message with a code to the user's mobile device) to prevent unauthorised access to and modification of data. The provider must also make every effort to minimise the risks of physical and electronic intrusions. Despite a high risk of attacks depending on degree of visibility of the cloud provider, the security of data integrity will necessarily involve respecting well-known technical standards.

4.8. Risks linked to the provider's degree of control

In using cloud services, the client often concedes total control of its infrastructure and information system, including security incident management, to the provider[26]. The more emphasis the client places on receiving a fully developed, ready-to-use service (SaaS application), the greater the risk it runs of losing control over its systems and applications. This will be more or less acceptable depending on its fields of activity.



[26] Plouin, Guillaume. *CLOUD COMPUTING, Sécurité, stratégie d'entreprise et panorama du marché* (CLOUD COMPUTING: Security, Business Strategy and Market Overview). Paris: Dunod, 2013.

In addition, the risk of data being "frozen" in the event of prosecution is to be considered. Megaupload's storage platform may be cited as an example. Its servers became inaccessible to Megaupload's clients, and as a result, so did the files stored on the platform[27].

4.9. Risks linked to quality of service

The provider must make a commitment regarding the quality of its service through a service level agreement (SLA). It will be important to agree on the type of obligation that is incumbent on the provider. Is it an obligation of means? A reinforced obligation of means? An obligation of results? An obligation of means is one in which the provider commits to making every effort to ensure the promised level of service, it being understood that proof of the contrary may be reported by the client. An obligation of results is one in which the provider must at all costs render the promised level of service on pain of liability. In a reinforced obligation of means, which is common for cloud services, the provider is to dedicate the necessary means to render the specified level of service and must prove that it has not committed any errors in case of dispute.

SLAs are an integral part of the contract and specify the rate of availability of the service, periods of interruption, backups to be made, response times and security metrics (e.g. incident response, data isolation and trace management).[28]

What is availability? Availability is client's ability to access the service offered by the provider. The level of availability will be higher or lower depending on the client's needs. The Gartner Group has developed the following classification system[29]:

- Class 1 concerns client-relations and partner-relations applications, which are critical for generating revenue. In this case, a 99.9% availability level corresponding to an interruption of less than 45 minutes per month is necessary. The recovery time

[27] Murray, Paul and Shrum, Sandy. *Common Risks of Using Business Apps in the Cloud*. US-CERT: https://www.us-cert.gov/sites/default/files/publications/using-Cloud-apps-for-business.pdf (accessed on 4 March 2015).
[28] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-Cloud-contracts/at_download/fullReport
[29] Jacquot, Thierry, *Reprise d'activité : n'oubliez pas le back up* (Resuming Activity: Don't Forget Backup), 01net.com, 5 August 2005: http://pro.01net.com/editorial/285929/reprise-dactivite-noubliez-pas-le-back-up (accessed on 10 March 2015).

objective (RTO) may not exceed two hours, and the recovery point objective (RPO) must be zero.

- Class 2 concerns functions that represent less critical sources of revenue and logistical functions. A 99.5% availability level corresponding to an interruption of less than three and a half hours per month is necessary. The RTO must be eight to 24 hours and the *RPO* must be four hours.

- Class 3 concerns a company's back-office functions. A 99% availability level corresponding to an interruption of less than five and a half hours per month is necessary. The RTO must be three days and the *RTO* must be one day.

- Class 4 concerns department functions. A 98% availability level corresponding to an interruption of less than 13.5 hours per month is necessary. The RTO must be four to five days and the RPO must be one day.

It is vital to specify whether the hours of non-availability are continuous or spaced apart. Indeed, a level of availability as high as 99.9% may correspond to eight hours of continuous non-availability per year. This information, like duration, is essential to resolve the incident. In a case decided by the Commercial Court of Paris on 12 July 2011, the provider had claimed to offer a 30-day response time. After 8 days of interrupted service (in this case, the company's email, stored on the Cloud), the client terminated the contract. The court considered the termination to be abusive and sentenced the client to pay damages to the provider.

Furthermore, despite promises of 99.9% availability, a cloud service provider is not immune to a technical failure leading to data loss or alteration that damages their integrity. According to the International Working Group on Cloud Computing Resiliency, which lists all failures, the leading 13 cloud service providers in the world have accumulated 600 hours of non-availability in the last five years[30]. It is therefore important to know whether copies of data are made on a regular basis in different geographic locations. For example, Microsoft's Azure cloud service experienced more than 100 service interruptions in 2014, versus 86 for Google's Compute

[30] Silicon.fr. *Comment garantir la sécurité du Cloud public* (How to Ensure the Security of the Public Cloud), 14 March 2014: http://www.silicon.fr/dossiers/comment-garantir-securite-Cloud-public (accessed on 20 February 2015).

Engine and 12 for Amazon's EC2[31]. In October 2012, Hurricane Sandy flooded American data centres and, indirectly, Amazon and Google infrastructure. *Ad hoc* contract clauses must provide for compensation for damages that the company may suffer if promises of availability are not upheld.

4.10. Risks linked to defaulting on service level obligations

It is very important to note the scope of the limitation-of-liability clause and the amount of fixed penalties. First of all, a provider that has specified very low penalties will prefer to default on its level-of-service obligations rather than meet its commitments if the latter is more expensive.

Indeed, the penal clause establishes a flat amount for damages in the event that the provider fails to uphold (defaults on) the contract. Nevertheless, Article 1152 of the French Civil Code adds that "*a judge may, even of his or her own motion, decrease or increase the penalty that had been agreed upon, it if is grossly excessive or derisory*". If the provider includes a release-from-penalty clause in the contract, the client will not be entitled to request any further compensation for damages caused by this same damage (Article 1229 of the French Civil Code).

The provider may also be exonerated from all liability thanks to a limitation-of-liability clause. However, the clause may be dismissed by the judge if it is at variance with the essential scope of obligation of the contract and essentially voids it (as in the 29 June 2010 ruling in the case *Faurecia vs Oracle*). Of course, in these two cases, the contract must be governed by French law.

4.11. Risks linked to traceability

The provider must have traceability mechanisms that monitor data access. Indeed, the client company must be able to access operations and security traces in order to monitor the security of the system and the data in real time, make *a posteriori* analyses and accord the information a certain amount of trust.

[31] ZDNet. *Cloud Public : Microsoft Azure, champion des pannes en 2014* (Public Cloud: Microsoft Azure, 2014 Failure Champion), 16 January 2015: http://www.zdnet.fr/actualites/Cloud-public-microsoft-azure-champion-des-pannes-en-2014-39813127.htm (accessed on 20 February 2015).

CUMULUS
A unique risk-management consulting service dedicated to cloud computing

Our expertise in Due Diligence & Risk Management on the one hand, and Cybersecurity Consulting on the other, allows us to work with our partners to offer our clients a cross-cutting and comprehensive approach to cloud services, including:

- Legal risk induced by contracts and general terms of sale,
- Commercial risk intrinsically linked to your providers, and
- IT risk, particularly in terms of safety.

To analyse and assess the risks linked to adopting cloud computing, CEIS, ATIPIC and Business Digital Security have developed a frame of reference based on the work of French and European authorities such as the French National Commission on Information Technology and Civil Liberties (CNIL), the French National Information Systems Security Agency (ANSSI), the European Union Agency for Network and Information Security (ENISA) and the French Prudential Supervisory Authority (ACPR) for the banking industry. It is also based on the work of organisations such as Syntec Numérique, Cloud Security Alliance (CSA), EuroCloud, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Cloud Confidence association.

We offer a personalised service, adapted to your organisation's level of maturity and your "appetite" for progressively adopting cloud solutions.

Whatever your organisation's level of maturity, our services always include an analysis of your strategic cloud solutions and providers in terms of strategy, security and legislation, as part of our due diligence and monitoring services.

For more information on Cumulus services:

Vincent Riou | Business Development Director | CEIS

vriou@ceis.eu

Tel.: (+33) 06 07 34 09 14

ceis

Systèmes d'information opérationnels et de communication en Europe
(Operations and communication information systems in Europe). April 2015

Quel référentiel pour les métiers de la cybersécurité ?
(What frame of reference for cybersecurity-related professions?) February 2015

NetMundial, un pas décisif dans l'évolution de la gouvernance Internet ?
(NetMundial, a decisive step in the development of Internet governance?)
February 2015

Comment développer la main d'œuvre spécialisée en cybersécurité ?
(How to develop a workforce specialised in cybersecurity?) February 2015

Cybercriminalité et réseaux sociaux : liaisons dangereuses ?
(Cybercrime and Social Networks: Dangerous Liaisons?) February 2015

L'entrainement « cyber », élément clé de la résilience des organisations
(Cyber training: a key element to improve the resilience of organisations)
January 2014 — English version available

Monnaies virtuelles et cybercriminalité — Etat des lieux et perspectives
(Virtual currencies and cybercrime - Current state of play and future prospects)
January 2014 — English version available

Cybersécurité des pays émergents — Etat des lieux
(Cybersecurity of emerging countries — Current state of play).
January 2014 — English version available

CEIS
Compagnie Européenne d'Intelligence Stratégique
(European Strategic Intelligence Company)
Limited company with a capital of €150,510
SIRET: 414 881 821 00022 — APE: 741 G
280 boulevard Saint Germain — 75007 Paris