RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RECOMMENDATIONS ON HOSTING SENSITIVE INFORMATION SYSTEMS IN THE CLOUD

TABLE OF CONTENTS

1 THE CLOUD: BOTH A CHALLENGE AND AN OPPORTUNITY

"Cloud computing" technology is a defining component of modern digital practices and is increasingly used by both the public and the private sectors. This trend is, in part, owed to the leverage and opportunities which the technology can provide in the realm of digital transformation.

The use of cloud computing, however, does also come with its fair share of security issues which may endanger our data and information systems (IS). More sensitive IS are particularly vulnerable. Cyberthreat reports indeed show that attackers have, for several years now, identified cloud solution providers and their infrastructures as ideal targets for cyberattacks. Cloud infrastructures are being targeted due to the concentration of data and transactions hosted within them, and because they entail the use of shared virtualisation and administration solutions. Another element to take into consideration is the application of extraterritorial laws, which require subjected hosts to forward their clients' data to the relevant authorities.

The evolution of cloud use has pushed public and private entities to reconsider which cloud offerings may best suit the specificities on their respective information systems.

2 A DECISION-MAKING TOOL

In order to meet this challenge, ANSSI has developed specific recommendations for cloud hosting, identifying the most appropriate cloud offerings depending on the type of information system used, the sensitivity of the data, and the level of associated threat.

These recommendations serve as an effective decision-making tool for entities which may be considering a switch to cloud hosting for their restricted information systems, for the sensitive IS of critical operators and service providers, and for information systems of critical importance (SIIV). It should however be noted that ANSSI's recommendations do not apply to classified information systems and cloud solutions are not suitable for all information systems. These recommendations are consistent with the French government's "**cloud at the centre**" ("cloud au centre") doctrine, whose implementation is assured by the Interministerial Digital Department (DINUM).

3 PRECAUTIONS FOR USE

The application of these cloud-hosting recommendations presupposes that a number of precautions have been taken by entities in their migration project.

Impact study and risk analysis

The decision to migrate information systems to cloud solutions befalls the concerned entity's highest authority. ANSSI recommends that this decision be informed by a business and legal impact study, and by a risk analysis. The risk analysis should – at the very least – take into consideration the following elements:

- The maximum level of threat to which the different information systems may be exposed;
- The specific risks linked to cloud hosting (e.g. the exposure of services on the internet and the mutualisation of infrastructure between clients);
- The sensitivity of processing and of the concerned data – with a particular focus on confidentiality, integrity, and availability;
- The legal risks associated with the extraterritorial scope of laws. Some cloud providers may be subject to extraterritorial legislation requiring the transfer of data to the relevant national authorities.

Selecting cloud security mechanisms

ANSSI recommends that – regardless of the type of offer chosen – entities select the services and licences most relevant to their needs, in order to obtain suitable security options and mechanisms.

A number of important responsibilities also befall the client – notably, the configuration of security options. For instance, the deployment or migration of an information system to cloud infrastructure will require the configuration of access control and filtering services; the client will need to ensure that only legitimate users can access the solution's administrative and supervisory interfaces.

It is also important to draw up a reversibility clause, so as to facilitate migrations from one cloud technology to another and, subsequently, to limit the client's dependency on a single cloud offering and its functional and security developments.

Team training

Lastly, ANSSI recommends that – in the context of a migration project – the training of technical teams and project managers in cloud usage be taken into consideration. This precaution should help to ensure the quality of the study on the migration of the information system to cloud hosting, and should facilitate cost and deadline management. It should also allow for the exhaustive study of the technical and organisational aspects of the migration process.

4 THE TOOLS NECESSARY TO THE IMPLEMENTATION OF THESE RECOMMENDATIONS, AND THE ASSOCIATED TERMINOLOGY

ANSSI's recommendations for cloud hosting are founded on three key elements:

- **The typology of cloud offerings;**
- **The state of the threat;**
- **The nature of information systems.**

Depending on the nature of the information systems, data, and processing involved, the threat may vary and require that one cloud offering be chosen over another. These three elements – detailed below – must be taken into consideration when deciding to migrate information systems to cloud offerings.

The typology of cloud offerings

The typology of cloud offerings around which ANSSI has formulated its recommendations comprises two main categories (commercial and non-commercial) – each of which caters to specific needs. Note that the term "cloud offering" encompasses several different services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Containers as a Service (CaaS), and Software as a Service (SaaS).

TYPES OF CLOUD OFFERINGS		DESCRIPTION
COMMERCIAL CLOUD OFFERINGS	Public	A cloud offering shared by all of the provider's clients.
	Private	A cloud offering whose resources (processor, network, and storage) are physically dedicated to the subscribing entity.
	Community	A cloud offering dedicated to a group of state-owned and private entities with shared interests.
NON-COMMERCIAL CLOUD OFFERINGS	Internal	A cloud offering deployed internally to meet the specific needs of the entity. The operation and supervision of infrastructures can be undertaken by either the entity itself or by a subcontractor.
	Community	In certain specific cases, entities in the same sector of activity may use their respective resources to set up a collective cloud. This infrastructure may then be considered both communal and internal.

NOTE : cloud usage leads to the progressive transformation and hybridisation of information systems architecture. Entities may indeed subscribe to different cloud offerings in order to meet their needs and supplement their pre-existing internal infrastructure.

The typology of threats

The second core element of ANSSI's recommendations stems from the state of the threat. Depending on the migration project considered, it is indeed necessary to measure the level of threat to which the concerned information system, data, and processing may be exposed. ANSSI has drawn up the following typology of cyberthreats:

TYPE OF THREAT	DESCRIPTION
STRATEGIC THREATS	This type of threat is defined by **persistent and targeted cyberattacks, conducted or funded by a State**. It is characterised by **significant technical and organisational means**, as well as by particular discretion. These attacks may be carried out for **espionage, pre-positioning, or destabilisation purposes** (i.e. cyber sabotage or data leaks). Note that the implementation of specific legislation or of **extraterritorial laws** by certain states can facilitate access to data hosted in the cloud, without the help of cyberattacks. Indeed, hosts subject to these laws are required to transfer their clients' data to the relevant authorities – without the possibility of appealing or even obtaining information.
SYSTEMIC THREATS	**Systemic** threats may affect a large number of entities. They may take the form of a **cybercriminal threat**, characterised by predominantly **opportunistic cyberattacks**. These attacks are typically conducted for **financial gains**, by means of **ransomware** or **fraud**. Systemic threats are also defined by the **proliferation** offensive **tools and services**, available **off the shelf** or commercialised by **private companies**. These services may be used to conduct **economic intelligence** or **industrial espionage** operations, or to allow certain states with limited resources to enhance their **offensive capabilities**.
HACKTIVIST OR ISOLATED THREATS	This threat is characterised by cyberattacks conducted by either an **isolated** individual or a **hacktivist group**, usually for **destabilisation purposes** (as revenge, for ideological reasons, etc.). These attacks may take the shape of denial of service attacks (DDoS) [1] or data leaks. **Isolated threats** may also involve individuals using unsophisticated tools or **benefitting from an entity's privileges** but **lacking significant means**.

1 The term "distributed denial of service" (DDoS) refers to a type of attack whereby the attacker uses a network of (often compromised) devices to disrupt one or more targeted services – such, for instance, as a website.

FOCUS ON SECNUMCLOUD STANDARDS AND QUALIFICATION

Formulated by ANSSI, the SecNumCloud standards lay out a set of security rules and best practices for cyber hygiene, thus guaranteeing the highest level of technical, operational, and legal standards.

Within this framework, the SecNumCloud security qualification awarded by ANSSI enables the recognition of services offered by cloud providers – notably PaaS, IaaS, and SaaS services. The SecNumCloud qualification strengthens confidence in the cloud offering itself, and in the operational practices of qualified providers. It does not, however, vouch for the security level of the customer digital services supported by these cloud offerings.

Hence, hosting a website on a qualified offering does not obviate the need to secure the website itself. If security measures are not enacted to protect the website, the risk of compromise will remain high. For example, applying security patches to a website in order to fix a heavily exploited vulnerability in web technology – such as SQL injections [2] – is a responsibility which befalls the client and not the SecNumCloud-qualified host [3].

This "security Visa" allows users to identify cloud offerings which endeavour to protect sensitive data and processing from cybercriminal threats, and from the implementation of extraterritorial laws. The qualification of an offering also facilitates the certification of subscribing entities' digital services, by providing a certain level of guarantee on underlying infrastructures. SecNumCloud-qualified cloud offerings are listed on **ANSSI's website**.

2 SQL injections are a type of vulnerability which allows attackers to manipulate data bases and to access potentially important information therein.

3 Securing these digital services and configuring both the offering and the chosen configuration options remain the responsibility of the entities (see: "Precautions for use").

The nature of information systems

The third core element of ANSSI's recommendations revolves around the nature of the concerned information systems. Restricted distribution networks and the sensitive information systems of the State, of critical operators, and of essential service operators are, by nature, the ideal targets of espionage or profit-driven attacks. Given the sensitivity of their data and processing, information systems of critical importance (SIIV) are particularly and systematically targeted by strategic offensive actors. It is therefore crucial to take the specific nature of the information system into consideration.

TYPOLOGY OF INFORMATION SYSTEMS	DESCRIPTION
Restricted distribution (RD) information systems	Information systems responsible for processing restricted data [4].
Sensitive information systems **covered by the government's "cloud at the centre" policy**	Information systems – excluding SIIVs – responsible for processing sensitive data, in accordance with the "cloud at the centre" policy.
Sensitive information systems of **operators of critical infrastructures** [5] and **operators of essential services** [6]	Information systems which are not regulated in the same way as SIIV, but which are nevertheless considered to be sensitive by virtue of the data processed.
Critical information systems (SIIV)	Information systems whose breach of security or malfunctioning could endanger the population and significantly hinder the security, the survival capabilities, and the military or economic potential of a nation [7].

4 As defined by the General Interministerial Instruction (IGI) 1300.
5 See the FAQ - Information systems of vital importance | ANSSI (cyber.gouv.fr)
6 See the FAQ - Operators of essential services (OES) | ANSSI (cyber.gouv.fr)
7 See article L. 1332-6-1 of the French Defence Code.

5 THE IMPLEMENTATION OF RECOMMENDATIONS

Capitalising on its experience and expertise, ANSSI issues the following recommendations, contingent on the sensitivity of the data and processing, and on the level of associated threat.

DR-level sensitive IS

- ANSSI recommends **non-commercial (internal and community) and private, commercial SecNumCloud-qualified cloud** offerings which provide **dedicated infrastructures** and thus limit the possibility of an attacker moving from one client's environment to another's.
- **Whether communal or public, commercial SecNumCloud-qualified cloud offerings may be considered** but will require the mutualisation of IT resources between clients (e.g. clients may store their data in a shared physical storage resource, or may host their websites on common physical servers).

Outsourced hosting, based on a SecNumCloud-qualified commercial cloud offer, is a decision which, for this type of information system, should be taken by the entity. ANSSI recommends that this decision be informed by a thorough risk analysis, **in order to demonstrate that the solution is adequately protected**.

Note: where access to information is contingent on nationality (e.g. Restricted Information – Special France), particular attention must be paid to the hosting location and to the administrators' nationalities. A non-commercial cloud offering may prove more apt when it comes to meeting this IGI 1300 requirement.

Sensitive IS covered by the State's "cloud at the centre" policy

- In accordance with the government's "**cloud doctrine at the centre**", these information systems must **only** be **hosted in SecNumCloud-qualified cloud offerings (whether internal, private, communal, or public)**.

Sensitive IS of critical operators and sensitive IS of essential service operators (including essential information systems)

- ANSSI **recommends** all types of SecNumCloud-**qualified** offerings.

IS of vital importance

Owing to the sensitivity of the processing and of the data processed, SIIV is a specific case requiring the informed decision of the head of the concerned entity.

- In the case of SIIV compatible with cloud technology, ANSSI recommends SecNumCloud-qualified non-commercial (internal and communal) and private commercial cloud offerings. These offerings provide a dedicated infrastructure and thus limit the possibility of an attacker moving from one client's environment to another's.
- ANSSI shall not oppose any other type of commercial cloud offering, provided that:
  1. It is SecNumCloud-qualified;
  2. The entity head's decision is informed by a thorough risk analysis of the outsourcing of hosting services for their SIIV, and that the regulatory obligations applicable [8] to the SIIV are complied with.

8 SIIV security is governed by regulatory measures which require the implementation of adequate risk management practices, in order to face the threat faced by the country's most fundamental interests.

Version 1.0 – Septembre 2024 – ISSN en cours

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr — communication@ssi.gouv.fr