New requirements on the use of cloud computing services in banking sector

The State Bank of Vietnam (SBV) recently issued Circular No. 18/2018/TT-NHHH providing for assurance of information systems safety and security in banking operations ("Circular No. 18"). Circular No. 18, issued on 21 August 2018, supersedes Circular No. 31/2015/TT-NHNN ("Circular No. 31") and will take effect from 01 January 2019.

Circular No. 18 is significant in that it introduces new regulations on the use of cloud computing services in the banking sector, as well as sets out criteria classifying information and information systems in the banking sector based on their level of importance. Some of Circular No. 18's notable points are provided below.

1. Classification of information and information systems based on their level of secrecy

Information, which is processed and archived via the information system, is classified into the following three categories:

(i) **Public Information**: Information disclosed to all subjects without a verification process;

(ii) **Internal Information**: Information owned by entities authorized to manage, exploit for its subject(s) and

(iii) **Confidential Information**: Information that is categorized as (i) "Confidential" in accordance with the relevant entity's regulations and is restricted from access; or (ii) "Confidential", "Highly Confidential", or "Top Confidential" in accordance with legal regulations on protection of state secrets.

Information systems of entities are classified based on the level of importance:

(i) **Normal Information System (Level 1)** serves internal operations or clients, but does not process confidential information.

(ii) **Important Information System (Level 2)** describes one of the following:

- an information system that processes confidential information;
- an information system that serves the entity in carrying out its daily internal operations and its non-operating times cannot exceed four (4) working hours;
- an information system that serves clients at all times and all plans regarding non-operation times must be prepared beforehand;

---

• an information system that provides online trading services to customers.

(iii) Especially Important Information System (Level 3) describes one of the following:

• an information system in the banking sector that serves to develop e-Government, and operates at all times and all plans regarding non-operation times are prepared beforehand;

• an information infrastructure system jointly used in the banking sector that facilitates the operation of offices and organization across the country, and operates at all times and all plans regarding non-operation times are prepared beforehand.

In cases where an information system is composed of numerous systems, all of which differ in terms of levels of importance, such information system shall be classified according to the importance level of the component system responsible for the overall system’s main technical and business activities.

2. Requirements when using cloud computing services provided by a third-party service provider

Article 32 provides that existing banking industry customers, prior to entering into a contract with a third-party for cloud computing services, must:

A. Conduct information technology risk assessment and operational risk minimization, which includes the following:

a) Risk identification, analysis and estimation of level of harm, forecast of threat to information security;

b) Ability to control business processes, ability to provide continuous service to customers, ability to fulfil obligations to provide information to state agencies;

c) Roles and responsibilities of related parties in ensuring service quality are clearly defined;

d) Measures to minimize risks, prevent and respond to problems and overcome them are thoroughly contemplated;

e) Review and adjust the risk management policy (if any).

B. When cloud services are used, in addition to meeting the selection criteria applicable to all IT services, the customer must also:

a) Classify operations and businesses planned for deployment on cloud computing based on the assessment of impacts of such operations and businesses on the operation of organizations;

b) Develop a contingency plan for components of information systems classified Level 2 or higher. The backup plan must be tested, assessed, and ready to replace the activities and operations deployed on cloud computing;
c) Develop a criteria for the selection of a third party provider;

d) Review, supplement, and apply measures to ensure information security of organizations, limit access from cloud computing to information systems of organizations.

C. If a third party is hired to perform all administration-related activities of information systems classified at Level 2 or higher, the customer must organize the risk assessment in accordance with Section A above and submit the risk assessment report to the SBV's Information Technology Department.

Criteria for the selection of third-party cloud computing service providers must include, at a minimum, the following:

(i) Service providers must be enterprises established and operating under the law;

(ii) Service providers are equipped with IT infrastructure fitting to the service provided, which satisfies:

- Current Vietnamese regulations; or
- Possesses valid international certificates on information security.

3. Contracts for use of IT services provided by third parties

Contracts for the use of IT services between an existing banking industry customer and a third-party IT service provider must include the following:

A. Commitment of the third party on assurance of information safety, which includes:

a) Satisfaction of the criteria for the selection of third-party cloud computing service providers as mentioned above;

b) No acts of copying, changing, use or provision of data by the service using entity for other individuals, entities, except for when the competent authority demands so in accordance with the law – in such cases, the third party must notify the service using entity before providing data, unless such notification violates Vietnamese laws.

c) Informing the third party's personnel participating in the execution of the contracts of the regulations on assurance of information safety of the entity and on the implementation of compliance-assurance supervision measures.

B. Provision of the maximum time a service can be interrupted and troubleshooting time, requirements related to assurance of continuous operation (onsite reservation, data backup, disaster prevention), requirements related to the capacity to handle, calculate, archive and other measures conducted when the quality of service is not guaranteed.
C. The third party’s use of sub-contractors will not change the responsibilities of third party regarding the services used by the entity.

D. The data incurring from the process of using service will be the property of the entity. Upon termination of use of service:

a) The third party shall return all implementing data and data incurred during use of service;

b) The third party shall commit to completing deletion of all the entity's data within a specified period of time.

E. The third party must notify the entity upon detection of violations of regulations of information safety regarding services used by the entity.

F. The contract of cloud computing service use, in addition to the what has been provided above, must also include that:

a) The third party shall provide an audit report of information technology compliance conducted by an independent audit organization on an annual basis during the contract execution time;

b) The third party shall provide cloud computing service quality control tool, procedures relating to supervising the cloud service provider, and controlling the quality of cloud service;

c) The third party shall be clear as to where data centres outside of Vietnamese territory are located (e.g., cities, countries) for implementation of services for the entity;

d) The third party shall provide how it will be responsible for protecting the data and preventing illegal data access on the service distributing channel from the third party to the entity;

e) The third party shall support, cooperate to investigate in cases of demand from Vietnamese competent authorities in accordance with the law;

f) The entity’s data shall be separate from other client's data used on the same technical platform provided by the third party.

* * *

Should you have any questions on the above, please do not hesitate to contact us.