Polish Cloud

THE IMPLEMENTATION STANDARD INFORMATION PROCESSING IN CLOUD COMPUTING

Polish Bank Association

The implementation standard in public or hybrid cloud computing has been developed as part of the working group set up at the Banking Technology Forum of the Banking Association and the Electronic Banking Council of the Banking Association.

STANDARD AUTHORS

Banking working group at the Polish Bank Association:

Alior Bank S.A., Bank BPH S.A., Bank Handlowy w Warszawie S.A., BNP Paribas Bank Polska S.A., BOŚ Bank S.A., Credit Agricole Bank Polska S.A., Getin Noble Bank S.A., Idea Bank S.A., ING Bank Śląski S.A., Pekao S.A., PKO Bank Polski S.A., with active participation of Operatora Chmury Krajowej sp. z o.o.

consisting of:

Grzegorz Pędzisz (przewodniczący) [Idea Bank S.A.],
Aneta Ostrowska [PKO Bank Polski S.A.],
Bartosz Ptak [Operator Chmury Krajowej sp. z o.o.],
Jacek Skorupka [Idea Bank S.A.],
Marek Dryjański [Bank Handlowy w Warszawie S.A.],
Adam Gutenbaum [PKO Bank Polski S.A.],
Maciej Leśniewski [Pekao S.A.], and
Magdalena Przyżycka [Idea Bank S.A.], Tomasz Fryc [Alior Bank S.A.], Artur Rudziński [Alior Bank S.A.], Magdalena Perfońska [Bank BPH S.A.], Marcin Wiśniewski [Bank BPH S.A.], Bogusław Borgosz [BNP Paribas Bank Polski S.A.], Krzysztof Turek [BOŚ Bank S.A.], Konrad Ciukaj [Europejski Fundusz Leasingowy S.A.], Jacek Mainda [Credit Agricole Bank Polska S.A.], Miłosław Sabiniarz [Credit Agricole Bank Polska S.A.], Michał Cichocki [Getin Noble Bank S.A.], Szymon Sobczak [Getin Noble Bank S.A.], Andrzej Mandel [Getin Noble Bank S.A.], Łukasz Śledzikowski [ING Bank Śląski S.A.], Adrian Dorobisz [ING Bank Śląski S.A.], Norbert Górski [ING Bank Śląski S.A.], Michał Jurga [ING Bank Śląski S.A.], Mikołaj Kujawa [ING Bank Śląski S.A.], Jacek Cholc [PKO Bank Polski S.A.], Jacek Zegan [PKO Bank Polski S.A.].

The presidium of the banking working group at the Polish Bank Association:

1. Wojciech Pantkowski, Director of the Payment Systems and Electronic Banking Group, Polish Bank Association
2. Joanna Barbrich, Payment Systems and Electronic Banking Team, Polish Bank Association
3. Maciej Kostro, Advisor to the Management Board, Polish Bank Association
4. Grzegorz Pędzisz, CIO, Idea Bank S.A.
5. Marek Dryjański, Head of the Office of New Technologies and Strategic Relations, Bank Handlowy w Warszawie S.A.
6. Jacek Cholc, Director of the Operation and Infrastructure Division, PKO BP S.A.

Consultant:

Accenture sp. z o. o.:

1. Łukasz Jęczmiński, Cloud Transformation and Migration, Manager
2. Grzegorz Żurawski, Security Strategy and Risk, Consultant
3. Łukasz Kundziewicz, Security Strategy and Risk, Senior Analyst

Legal Coordinator:

Kochański & Partners sp.k.:

1. Daniel Kozłowski, Advocate, Financial Services Sector, main legal coordinator of cloud implementations
2. Aleksandra Piech, legal advisor, New Technologies Sector, specialist in cloud implementations
3. Dr Agnieszka Serzysko, legal advisor, Partner, Financial Services Sector

The developed standard was reached in consultation with the following members:
mBank S.A., Google Poland sp. z o.o., Oracle Polska sp. z o.o., Hitachi Ltd, Dell sp. z o.o., Cisco Systems Poland sp. z o.o., Microsoft Polska sp. z o.o.

TABLE OF CONTENTS

1. INTRODUCTION

To meet the expectations of the banking market in Poland in terms of the possibilities of implementing solutions based on cloud computing in entities covered by banking supervision, a working group was established at the Association of Polish Banks and the Banking Technology Forum.

The banking sector in Poland exists within the framework of laws, regulations, as well as recommendations and guidelines of financial supervision regulating its activities. Adaptation of the latest technological solutions in banking under these regulations is not an easy task. Interest in the banking sector, with little practice by banks in the use of cloud services, has prompted the authors of this study to propose to banks a joint initiative to develop a standard for the implementation of IT solutions based on cloud computing in banks in accordance with applicable regulations.

In October 2017, the Office of the Polish Financial Supervision Authority published a communication regarding the use by supervised entities of cloud computing services, which on the one hand explicitly allowed the use of cloud services, but on the other hand had a restrictive effect on the banking market regarding the implementation. Despite this, there were examples of implementations by banks, both regarding production applications processing data covered by banking secrecy, test solutions or simple applications (like e-learning), based on cloud computing

On January 24, 2020 (issued on January 23, 2020), the Office of the Polish Financial Supervision Authority published another message regarding the processing of information in the cloud by supervised entities public or hybrid computing (the "Communication"), which explained many issues previously raised by banks. With the active participation of banks and the National Cloud Operator (National Cloud Operator sp. z o.o.), we wanted to use the experience of previous implementations and analyze the provisions of the Communication and work together to develop a standard, constituting of a broad set of banking group practices and solutions enabling banks to easily go through the process of adapting to the cloud, both throughout their organization or with selected solutions offered by cloud service providers.

The Communication itself, in accordance with its wording, supplements and details selected recommendations in the field of outsourcing, described inter alia in Recommendation D and the ‚Banking Law'. It was necessary to take these adjustments into account in determining the options and the actual implementation of the solutions based on cloud computing. The communication presents a national approach (reference model), which means that guidelines, recommendations or other documents presenting the position of the European Banking Authority (EBA) that relate to the processing of information in public or hybrid cloud computing, including - Eur guidelines. The guidelines of the European Banking Authority of 25 February 2019 do not apply to Polish banks.

This Standard presents the tasks, procedures, processes and analyzes that a bank should carry out and document the organization's preparation for operating in the field of cloud services to individual entries of selected regulations.

2. ASSUMPTIONS

1. This Standard refers to the requirements for the use of cloud solutions by entities covered by banking supervision within the meaning of the Act of 21 July 2006 on financial market supervision (i.e. Journal of Laws of 2019, item 298, as amended). The standard therefore does not refer to requirements of cloud solutions for entities covered specified by other supervisions than this Act.

2. The standard analyzes the requirements of the Communication, and thus presents the requirements of the Supervisory Board Office Financial in the case of processing information in entities subject to banking supervision in the public cloud or hybrid cloud.

3. The standard also summarizes the requirements of the Banking Law (as defined below) applied in addition to the Statement in the reference model indicated in item 1 above (Introduction).

3. APPLIED TERMINOLOGY. EXPLANATION OF SELECTED DEFINITIONS FROM THE COMMUNICATION

Bank - an entity subject to banking supervision, including a bank within the meaning of the Banking Law (domestic and foreign), a branch of a domestic bank abroad, a branch and representative office of foreign banks within the meaning of the banking Law, branch and representative office of a credit institution within the meaning of the Banking Law and a cooperative bank within the meaning of the Act on the operation of cooperative banks, their associations and affiliating banks (supervised entities within the meaning of the Act on supervision are excluded from the scope of this Standard) financial market other than entities subject to banking supervision).

Cloud computing - has the meaning given to the term "cloud computing" in the Communication. For the requirements of the Standard, by cloud computing we mean public cloud computing and hybrid cloud computing.

Hybrid cloud computing - has the meaning given in the Communication to the term "cloud computing hybrid".

Public cloud computing - has the meaning given in the Communication to the term "cloud computing Public".

Private cloud computing - has the meaning given in the Communication to the term "cloud computing private".

Social cloud computing - has the meaning given in the Communication to the term "social cloud computing".

CPD - has the meaning given to the term "CPD" in the Communication.

Provider - has the meaning given in the Communication to the term "cloud service provider".

EEA - means the European Economic Area.

Civil Code - means the Act of April 23, 1964 - Civil Code (i.e., Journal of Laws of 2019, item 1145, from changes).

Announcement - announcement by the Polish Financial Supervision Authority of January 23, 2020 regarding the processing of information by public entities in the public or hybrid cloud computing.

KNF - Polish Financial Supervision Authority.

PFSA - Office of the Polish Financial Supervision Authority.

Special cloud outsourcing or Special outsourcing - has the meaning given in the Communication, the term "special outsourcing of cloud computing".

Banking Law - means the Act of 29 August 1997 - Banking Law (i.e., Journal of Laws of 2019, item 2357).

Recommendation D - recommendation issued by the Office of the Polish Financial Supervision Authority in January 2013, regarding the management of areas of information technology and ICT environment security in banks.

GDPR - means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation).

Standard - this study.

Banking secret - has the meaning given in art. 104 of the Banking Law, so "all information regarding banking activities obtained during negotiations, during the conclusion and implementation of the contract, based on whose bank does this".

Cloud computing service - has the meaning given in the Communication to the term "cloud computing service".
EBA guidelines - Guidelines of the European Banking Authority of 25 February 2019.

The table below additionally presents the definitions contained in the Communication, together with their meaning in which they are used in this Standard and in accordance with the adopted Assumptions, and, where applicable, bear comment or explanation:

Message definition	Meaning accepted in Standard or comment/explanation
"social cloud computing"	Social cloud computing can be both: a) Private cloud computing when available for the exclusive use groups of entities related by capital or under a joint agreement or managed by an entity from the group b) Public cloud computing when available for exclusive use groups of entities related by capital or pursuant to a joint agreement, but is also managed by the Supplier.
"Legal information protected"	Banking secret
"outsourcing particular computing clouds"	Only as an auxiliary, we include criteria (references) in the scope of evaluation, whether the activity is significant / basic (based on the criteria proposed by the EBA Guidelines): a) whether the outsourcing agreement relates directly to banking activity, b) the potential impact of disruption or non-performance by the Supplier of the test activity on the agreed guaranteed level of services on a continuous basis on: I. short- and long-term resilience and financial condition, including if II. concerns, its assets, capital, costs, financing, liquidity, profits and losses, business continuity and operational resilience, III. operational risk, including conducting business, information and communication technologies (ICT) and legal risk, IV. reputational risk, V. planning for corrective action, if applicable and resolution, the possibility of effective resolution and operational continuity in the event of early intervention, remedial action and resolution, c) the potential impact of ordering the audited activity on the Bank's ability to: I. identify, manager and monitor risk level II. meet all legal and regulatory requirements, III. conduct appropriate audits regarding functions which are subject of outsourcing, Standard - this study. Banking secret - has the meaning given in art. 104 of the Banking Law, so "all information regarding banking activities obtained during negotiations, during the conclusion and implementation of the contract, based on which bank does this." Cloud computing service - has the meaning given in the Communication to the term "cloud computing service". EBA guidelines - Guidelines of the European Banking Authority of 25 February 2019. d) potential impact on services provided to clients, e) any outsourcing agreements, the Bank's total exposure to the same The provider and the potential combined impact of outsourcing contracts in the same area of activity

	f) size and complexity of the given area of activity, g) the possibility of extending the scope of the proposed outsourcing contract without replacing or changing the base contract, h) the ability to transfer the proposed outsourcing contract to another Supplier, if necessary or desirable, both on the basis of contracts and in practice, including estimated risks, obstacles to continuity related activities, costs and time frames, i) the ability to reintegrate outsourced activities to the Bank if it is necessary or desirable and j) data protection and possible impact of confidentiality breach or failure to provide data availability and integrity for the payment institution or institution and its clients, including but not limited to compliance with the GDPR.
"subcontractor"	A sub-supplier within the meaning of the Communication is an entity that owns or can have identified access to information processed by the entity supervised. Through identified access to information processed by the Bank is understood as access that meets the following criteria: a) enables the sub-supplier to identify the Bank as the payer, b) the processed data (information) is disclosed, understanding of this term, depending on further explanations of the KNF, may be subject to change.
"subject supervised "	Bank
"principle of proportionality"	Only incidentally, we provide an explanation of the principle of proportionality, which is missing in the Communication. In line with the EBA's guidelines, the purpose of the proportionality principle is to ensure that management principles, including those on outsourcing, are consistent with the individual risk profile, nature and model business institution or payment institution and the scale and complexity of its operations so as to effectively achieve the objectives of regulatory requirements. Banks, in accordance with the principle of proportionality, should take into account the complex nature of outsourced functions, the risk arising from contract outsourcing, the critical or significant importance of the outsourced function and the potential impact of outsourcing on business continuity. Banks, when applying the proportionality principle, should take into account the criteria set out in the EBA's title and guidelines on internal management in accordance with art. 74 section 2 of Directive 2013/36/ EU. It also seems that "proportionality" may be equated with "adequacy" depending on the overall situation of the Bank.

4. DOCUMENT ORGANIZATION

1. The standard has been divided into chapters devoted to regulations having an impact on the manner of implementation Cloud computing services in the banking sector.
2. In Chapter 5 and Chapter 6, recommendations and legal regulations are described, together with relevant standardized actions, which in the authors' opinion should be taken to implement the Cloud Service in accordance with the given regulation.
3. Each chapter includes, where applicable:
   1) citing in the chapter header the given regulation point,
   2) summary of the description of requirements resulting from the regulation,
   3) indication of requirements (products) on the side of the Bank,
   4) an indication of the requirements (products) on the side of the Supplier and
   5) indication of templates or examples of documents.

5. THE COMMUNICATION

5.1. POINT IV OF THE COMMUNICATION - "APPLICATION GUIDELINES"

IV. Application guidelines

1. To ensure the proper functioning of the financial market and its stability and security, based on art. 4 paragraph 1 of the Act on Financial Market Supervision, Supervision expects supervised entities to apply this model reference during activities related to the preparation, implementation and termination of information processing in cloud computing, treating it as a clarification of existing legal requirements and without prejudice to those requirements if:

   1) the information processed belongs to legally protected information within the meaning of this communication or

   2) the processing of information is a special outsourcing cloud computing as defined in this communication and the processing of information is carried out in a public or hybrid cloud (in the scope based on public cloud computing).

2. The superior task of the supervised entity during information processing within cloud computing is to ensure the security of processed information and the lawfulness of the manner and scope of this processing. The application of this communication should respect the principle of proportionality, taking into account in parallel the reference model. The principle of proportionality should be found its concretization at the stage of estimating the risk associated with the planning of activities processing and adequacy of applied safeguards of processed information. The PFSA Office emphasizes that the principle of proportionality should not be interpreted as approval for use by smaller supervised entities of less effective security of processed information than described in this message.

3. Supervision underlines that the requirements described in this communication should be applied by supervised entities before starting to process information within cloud computing.

4. In order to properly apply the provisions of this communication, the supervised entityshould specify for each cloud computing service planned to be or in fact used:

   1) whether legally protected information is processed and

   2) whether the processing activity can be defined as specific cloud outsourcing computing.

Application matrix		Cloud computing outsourcing other than specific	Cloud computing outsourcing - specific
Information	Information other than legally protected	The communication can be used	The communication should be used
	Information legally protected	The communication should be used	The communication should be used

5. If the activity or information is qualified to more than one category according to the matrix above, the more stringent requirement should be applied.
6. Notwithstanding the foregoing, the communication shall not apply if a specific provision:
   1) excludes the possibility of processing specific information in the cloud or excludes the possibility of performing specific activities in the cloud processing;
   2) imposes a requirement to meet specific technical or organizational requirements regarding the processing of specific information that would exclude the possibility of meeting the requirements of this communication.
7. This communication does not need to be used when designing and operating test or development environments in cloud computing, as long as these environments do not legally protected information is processed.
8. The message does not apply to information processing in private cloud computing.

DESCRIPTION OF REQUIREMENTS

1. The message must be used in two cases:
   a) The processing of a bank secret or
   b) Outsourcing specific cloud computing.
   In any other case, the Message may be used if the Bank (also in agreement with the Supplier) so decides.
2. This message does not apply to private cloud computing.
3. The Bank determines the type of data (information) processed for a given Cloud Service on banking secrecy and the type of activity due to the special cloud outsourcing.
4. In the process of analysis and qualification of processed data, the Bank should refer to the existing ones at the Bank of inventory of critical processes resulting e.g. from the BIA or Recommendation H regarding the internal control system in banks issued by the KNF Office in April 2017.
5. If the Cloud Services are used only for processing test (information) data (anonymized), the message shall not be used.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. A document confirming the analysis carried out in the scope of the type of processed data (information), the planned Cloud Service and the type of processing activities, and its qualifications.
2. Document confirming that the analysis has been carried out in relation to the requirements of Special Outsourcing cloud computing.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED BY THE SUPPLIER

N/D

TEMPLATES

N/D

5.2. POINT V OF THE COMMUNICATION - "CLASSIFICATION GUIDELINES AND INFORMATION EVALUATION"

V. Guidelines for classifying and assessing information

1. The supervised entity shall classify in the documented process:
   1) legally protected information within the meaning of this communication;
   2) information whose protection results from legal regulations not included in this communication;
   3) information that is not subject to legal protection.

2. The information is evaluated in terms of the admissibility of its processing in the cloud, in particular taking into account:
   1) compliance with legal requirements and specific to the given sector or entity supervised by provisions and contractual obligations;
   2) scope of classified information, its type and validity;
   3) value of information for the supervised entity.

3. The supervised entity in the information classification and evaluation process includes:
   1) the scale of operations;
   2) corporate, group or other models or methods of assessment and classification, which take into account the above assumptions and are common to the group of entities, which includes the supervised entity;
   3) the responsibility of the supervised entity for the information processed.

4. The supervised entity should classify and evaluate information again, when:
   1) it intends to process a new type of information;
   2) it intends to use the new cloud service;
   3) a change in the law, regulations, regulations or provisions of contracts to which the supervised entity is a party, affects or may affect the compliance of the entity's conduct supervised in the context of information processing in the cloud;
   4) the processing scale increases or decreases significantly;
   5) the value of processed information increases significantly.

5. A supervised entity should regularly (but not less than once a year) review and confirm the validity of the classification and evaluation of information used for the current conditions of its operation.

DESCRIPTION OF REQUIREMENTS

1. The bank should monitor changes in legal and regulatory requirements on an ongoing basis to the extent that would require re-qualification of the information processed.

2. The bank should review and confirm the validity of the classification and assessment applied at least once a year information in relation to the current conditions of its activities.

3. The bank should verify at least once a year whether the Cloud Service or processed data (information) is not processed in a data center located in a different region than at the moment of starting to provide the Cloud Service or processing data (information) in the Cloud, however, the Supplier's statement is sufficient here in accordance with the proper representation or authorization.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. The described process of qualification and evaluation of information processed in the Cloud computing taking into account guidelines described in points 1.1. up to 1.3. and 3.1. up to 3.3. paragraph. V (Guidelines for the classification and evaluation of information) of the Communication.

2. Documented standard for the classification of data (information) used by the Bank.

3. Documented results of data classification (information) that should be included in the data processing plan (information) in the Cloud.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Informing the Bank about a change in the place of data processing (information) in the Cloud.

TEMPLATES

N/D

5.3. POINT VI OF THE COMMUNICATION - "GUIDELINES FOR RISK ESTIMATION"

VI. Guidelines for risk estimation

1. The supervised entity shall conduct comprehensive risk estimation in a documented proces (identification, analysis and assessment of threats, their occurrence and impact this occurrence on a upervised entity) as required by the current issue PN-ISO 27005 (Risk management in information security) standard or its equivalent in the European standardization system, or based on other, structured approaches. Risk assessment is carried out on a continuous basis, taking into account the practical implementation of the PDCA principle ("plan - do - check - act").
2. The supervised entity shall include in the risk assessment process in the context of results classification and e valuation of information processed in the cloud, at least:
   1) general threats to the use of cloud computing:
      a) geographical dispersion of processed information, in particular in the context of ensuring compliance of the information processing process with legal provisions, internal regulations, contractual obligations as well as declarations and others regulations;
      b) the possibility of losing compliance of the supervised entity with the regulation rights (including licenses or permits issued) by using cloud services computation unintentionally or other than as intended;
      c) access to processed information by employees and co-workers (e.g. sub-suppliers) cloud computing service providers;
      d) access to processed information, guaranteed by the jurisdiction of the country where the processing physically takes place (location of the data center), in particular a reference to the catalog of situations (or entities) where possible is to request information or access it without the express consent of the supervised entity, both by national and international administration authorities;
      e) lack of technological compatibility between the services of different cloud computing providers, resulting in attachment to one cloud computing service provider by limiting or not being able to transfer (use identical) services or processed information (vendor lock-in);
      f) failure of the isolation mechanisms of resources used to provide cloud services;
      g) vulnerability of service management interfaces that are provided by cloud computing service providers;
      h) limited ability to influence the scope, shape and changes of services, including in particular the process of retention of processed information and its removal after the completion of processing services;
      i) limited ability to control the cloud service provider and its sub-suppliers, including direct verification of physical, technical and organizational security mechanisms and control of service provision cloud computing; direct verification of physical

j) division of responsibility for the security of processed information between cloud computing service provider and the supervised entity;

2) specific threats to the specific (named) cloud services used:
   a) the possibility of using services in a manner inconsistent with the intentions of the supervised entity or in an environment that is not subject to the control of the supervised entity (e.g. private mobile devices, access from private or public networks);
   b) the possibility of unilaterally changing the technical conditions of using the service (in particular its parameters or configuration rules);
   c) using default or publicly available configuration parameters services, without their due verification and assessment of adequacy for the needs of the supervised entity;
   d) the authentication mechanisms used and their weaknesses;

3) specific threats related to the resources of the supervised entity:
   a) resources required and held, including established human resources;
   b) technological compatibility of the ICT environment and cloud computing environment, in particular integration mechanisms;

4) the value of information processed for the supervised entity and direct and indirect effects of loss of control over its processing;

5) a supervisory position regarding the encryption of information, according to which:
   a) encryption of information does not reduce the validity of information, nor does it change its classification and assessment;
   b) Information encryption and proper management of encryption keys prevents disclosure of information;
   c) there is no guarantee that the given encryption algorithm will be considered "completely secure". The supervision recommends using encryption algorithms, which - based on publicly available information (e.g. substantive studies, reports units dealing with cybersecurity or cryptography) - are not recognized as unreliable. In case of using an algorithm unreliable, the supervised entity should immediately take steps to ensure the security of processed information.
   d) information processed in the cloud should always be encrypted, when it is technologically possible and - in the opinion of the supervised entity - economically justified;
   e) legally protected information must always be encrypted "at rest" and "in transit". The supervision permits a situation in which legally protected information is encrypted "at rest" immediately after it is sent to the cloud based on the assumption that there is simultaneous use of "in transit" encryption and does not treat such a situation as disclosure of processed information;
   f) supervision allows a situation in which a supervised entity entrusts its service provider (including a cloud service provider) with generation or managing encryption keys that are used to encrypt information processed in cloud services of another cloud service provider, while the supervised entity should take into account the possibility of losing its access to encryption keys in the risk assessment process;

6)) supervisory position regarding the creation of an outsourcing chain, according to which:
   a) the creation of the outsourcing chain should always be assessed by a supervised entity from the erspective of specific legal provisions concerning specifically implemented information processing activities in the cloud computing, in particular:
      I. creating an outsourcing chain for supervised activities allowed only within the limits provided for by law;
      II. creating an outsourcing chain in a scope other than in the scope of supervised activity is permissible, unless it is explicitly prohibited by law contractual rights or provisions;

b) the scope of responsibility of the cloud service provider and its subcontractors to the supervised entity may be limited or excluded only within the limits of specific legal provisions regulating activities supervised entity, with the Supervision critically assessing such exclusions or restrictions if:

I. as part of the cloud service, legally protected information encrypted using encryption keys provided or managed is processed by the cloud service provider or its subcontractor or

II. the processing is outsourced to a particular cloud computing;

7) a supervisory position on the services (cloud service providers) that are used to provide its own services by direct suppliers of supervised entities, according to which:

a) the supervised entity should make sure to what extent a director provider provides the service using cloud computing services, and in particular whether legally protected information is processed in the cloud service;

b) depending on the actual use of cloud computing services and the scope of processed information, the supervised entity should ensure that the processing of information is carried out taking into account the provisions of this communication;

8) a supervisory position regarding the law of the contract between the service provider of cloud computing and a supervised entity , according to which:

a) the law applicable to the contract is Polish law or the law of another Member State of the European Union, unless the parties to the contract submit the contract to the law of a third country, and the law of a third country allows for effective performance of:

I. the provisions of the contract;

II. all requirements of Polish law imposed on the supervised entity;

III. supervisory authority guidelines, including within the scope of this Communication;

b) if the contract is subject to the law of a third country, the supervised entity should have a written legal opinion confirming that it is in accordance with the chosen law applicable to the contract, all provisions of the contract between the entity supervised and the cloud service provider meet the requirements of the law applicable to the supervised entity and the requirements of communication;

9) other significant threats that the supervised entity identifies in connection with the use of cloud computing services.

3. The supervised entity should consider the potential entity in the risk assessment process regarding:

1) the use of verified, updated sources of information on hazards specific for the use of cloud services, including in relation to specific (named) services;

2) using assistance from entities or persons with specialist competences both in the area of cybersecurity and cloud computing services, especially in the absence of such competence within the own organization of the supervised entity;

3) analyzing the available audit results of external cloud computing service providers in relation to cloud computing services and the information security management process, expanding the scope of analysis with available certificates issued to the cloud computing service provider confirming compliance with the requirements;

4) prior testing of cloud computing services, also using stress scenarios, both in terms of the way the service works and its configuration.

4. The supervised entity, based on the results of risk assessment, manages this risk, having regard in particular to:

1) the requirements of legal provisions, internal regulations and contractual provisions;

2) the degree of organizational complexity, division of the entity’s rights and responsibilities

supervised, concluded agreements, and analogous factors occurring in the capital group or group organization or association, to which the supervised e ntity should be;

3) the effectiveness of control and monitoring mechanisms used, in particular in relation to:
   a) identification of new threats;
   b) changes in the cloud service used or the mode and scope of its use;
   c) changes in the relationship with the cloud service provider, including the opportunity unplanned termination of cooperation by both the supervised entity and cloud computing service provider;

4) technical competence and organizational capabilities of the supervised entity, in particular in the context of the safe use of cloud computing services and implementation of contractual provisions;

5) the ability of the supervised entity and compliance with the law to transfer risk identified or acceptance of the estimated level of risk.

5. The results of the risk assessment should give rise to the assertion that the provision of the service cloud computing will be implemented in accordance with applicable law supervised entity, external and internal regulations and adopted by entity supervised by standards.

6. The results of the risk assessment should be formally approved and subject to periodic verification and updating. The approval should include the decision of the supervised entity regarding:

   1) cloud computing services that the supervised entity will use;

   2) the type and scope of information processed under these services.

DESCRIPTION OF REQUIREMENTS

1. The Bank shall carry out risk assessment in a documented manner and in accordance with its methodology.

REQUIREMENTS (PRODUCTS) TO BASE ON THE BANK SIDE

1. Documented process of risk classification and assessment in terms of admissibility of cloud computing.

2. Document "Risk assessment results" for each implemented Cloud Service including the plan dealing with the described risk.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Documentation of meeting the requirements / status, in particular:
   1) location of the CPD, data processing area (location of the Supplier from which the personnel accesses to Bank data). It is allowed to specify this at the country / region level;
   2) the method of controlling and monitoring access to processed information by the Supplier's and his personnel suppliers;
   3) description of the mechanisms of isolation of resources used to provide cloud services, along with information about the potential effects of failure of insulation mechanisms;
   4) documentation of the interfaces managing the Cloud Services, security information interfaces and their vulnerabilities, if any;
   5) the rules for requesting changes by the Supplier;
   6) the ability to control the Supplier and its sub-suppliers, in the scope of direct verification of physical, technical and organizational security mechanisms and control of the provision of Services cloud computing;
   7) sharing of responsibility for the security of processed information between the Supplier and the Bank;

8) mechanisms of controlling access to the service for users, in particular methods of restricting access from private devices;
9) possibilities of integration with other technologies indicated by the Bank;
10) technological stack to ensure environmental security, data (information) and Cloud computing resources, in particular encryption mechanisms;
11) the outsourcing chain as well as the quality control and assurance process.

TEMPLATES

1. Appendix_1_Risk estimation template.

5.4. POINT VII OF THE COMMUNICATION - "MINIMUM REQUIREMENTS FOR INFORMATION PROCESSING IN CLOUD COMPUTING"

VII. Minimum requirements for information processing in the cloud

1. These minimum technical and organizational requirements for the processing of information in cloud computing constitute a reference which should be verified by the supervised entity in terms of its adequacy to the results of the risk assessment and ensure their fulfillment.
2. Technical measures and organizational resources for the security of the processed information should result from the risk assessment process carried out, however - regardless of the results of this estimation - they must not weaken the requirements described below.
3. Ensuring competence

   3.1. The supervised entity ensures proper competence in the documented process for planned or ongoing information processing activities in the environment of cloud computing. These competencies include requirements for the education, training, skills and experience of employees or colleagues supervised entity inolved in the planning, implementation and testing process and maintaining information processing in the cloud and concluding and viewing the related contract.

   3.2. A supervised entity provides an understanding of the consequences of using specific cloud computing architecture, configuration rules, and responsibility sharing for the security of processed information, depending on the scope and type of the planned or used cloud computing environment and the model of the service provided, taking into account the requirements of business continuity of the supervised entity and its ICT infrastructure. Understanding the consequences of a given choice is relevant in the risk assessment documentation, ensuring the right resources in both qualitative and quantitative terms and in addition in all work (and contracts) related to the creation or development of dedicated software for use in the cloud and integration of services based on the own resources of the supervised entity.

   3.3. Competences of employees or associates of the supervised entity responsible for security and planning, configuration and management as well as monitoring of cloud computing services should be confirmed by appropriate documentation training or personal certificates to the extent applicable to the services used cloud computing (or result from skills and experience), including also cloud specific or specifically configured for a given service provider. This requirement also applies to the competences of the persons responsible for reviewing or verifying audit documentation, certificates and other supplier's documents cloud computing services, including contracts for the provision of cloud computing services and technical documents.

DESCRIPTION OF REQUIREMENTS

1. Bank to ensure security of information processed in the Cloud (or for which there is an intention to process), and should ensure an appropriate level of knowledge and skills of employees and colleagues, this appropriate level of knowledge and skills, as a rule, is determined on the basis of the results of the risk assessment. Maintenance and systematic improvement of qualifications (knowledge and skills) should be part of the Bank's good practices. Any deficiencies should be addressed through appropriate training or the support of service providers consultancy in the field of cloud computing. Competences of employees and associates should be documented, e.g. in the form of training certificates or Suppliers' certificates.

2. The bank should specify the roles in the organization along with the scope of the main tasks during implementation or at maintaining cloud solutions and matching the required areas of competence to them. Examples of role areas and competences matched to them in implementing and maintaining solutions in the public cloud are:
   1) architecture (the role of the Architect);
   2) safety (role of Security Engineer);
   3) development (role of Developer, DevOps Engineer);
   4) maintenance (Administrator roles, Network Administrator, DevOps Engineer);
   5) business (the role of the service business supervisor); and
   6) finance (role of financial controller).

3. Roles and competences matched to them should ensure safety and architectural coherence and provide appropriate support for solutions, as well as accountability and financial control of cloud computing Services used.

4. The Bank as part of maintaining production information processing systems in the Cloud Computing should have active support of Suppliers or use the support of companies providing consulting services in the field of cloud computing.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Documented division of roles and corresponding competences in the organization along with the scope of the main tasks for the needs of implementing or maintaining systems in the Cloud.

2. Documented training or certification for individual roles.

3. Documented records confirming the active support of Suppliers or companies providing consulting services in the field of Cloud Computing.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Documented training, confirmed by certificates.
2. Documented support of the Supplier's staff for the Bank.

TEMPLATES

N/D

4. Contract with a cloud computing service provider

4.1. The supervised entity has a formalized contract (and other documents, including statements, regulations, terms of service, also in electronic version) with a cloud computing service provider that, where relevant in relation for the services used and the scope of information processed - it contains or indicates sources information, including:

a) clear division of responsibility in relation to the security of processed information, including the model of service provision, business continuity services (including RTO and RPO parameters where appropriate) and the declared SLA together with the measurement and reporting method;

b) a clear definition and indication of the location of information processing and its methods verification and safeguarding compliance by at least a reference to the right documents, configuration descriptions, methods and tools;

c) the law applicable to the contract (including the court with jurisdiction and dispute settlement rules);

d) confirmation of the compliance of the rules for the processing of personal data with European Union law, if applicable;

e) ownership of the information processed during the contract and after its termination (expiry, termination), also in an unplanned manner;

f) guarantees, warranties, insurance (insurance policies of a cloud service provider computational penalties), contractual penalties, determination of force majeure, events covered by the scope force majeure and rules of conduct in such situations, if applicable;

g) determining the scope of liability for damages caused to the clients of the entity supervised (if applicable), as required b y applicable law;

h) clear indication of the suppliers (name, location, scope of activities) of the supplier cloud computing services and conditions for granting access to information processed by the supervised entity;

i) a clear indication of the principles according to which tasks, scopes of powers and responsibilities as well as the accountability of the sub-suppliers of cloud computing service providers are transparent and clearly identified by the supervised entity;

j) sources of authorized information about planned changes in standards cloud computingservices provided (including technical changes);

k) sources of technical documentation and declaration of conformity (including compliance with applicable law), along with configuration instructions cloud computing services;

l) the scope of additional information and documentation provided by the service provider of cloud computing in connection with the provision of cloud computing services;

m) the right of the supervised entity to carry out inspections at locations information processing, including the right to conduct a 2nd or 3rd audit parties at the request of the supervised entity (if the need arises from the risk assessment);

n) the right for supervision to perform control obligations, including room control and documentation related to the processing of supervised entity information, processes and procedures, organization and management, and compliance confirmations;

o) licensing rules (including the right to update used security software or its components) and intellectual property rights, including - if applicable, the right to dispose of processed information;

p) the rules for changing the content of the contract, including the technical parameters of the services used cloud computing;

q) the rules for terminating the contract, including the rules and deadlines for returning or deleting processed information;

r) support rules, including scope and time windows (including time zones), the mode and manner of reporting problems with cloud computing services;

s) rules for the exchange of information, in particular in the field of security and management of current incidents, including both employees of the supervised entity and the provider of cloud services, and in the case of significant exposure to the effects of a given incident.

- also other parties (e.g. customers, subcontractors), in order to ensure the adequacy of the proceedings to the level of significance of the incident.

4.2. Without prejudice to legal requirements and subject to the provisions of this message, the supervised entity may use framework shared agreements by cloud computing service providers, in particular when they relate to services cloud computing created for a group of entities (including a supervised entity) under corporate or group agreements, including social cloud computing. In this case, the supervised entity should:

t) verify the extent to which the framework agreement and related documents, risk assessment esults, and legal, organizational and technical requirements take into account the provisions of this communication and are appropriate to the situation supervised entity and its intentions related to information processing in cloud computing;

u) assess the necessity or self-applicability of the requirements of this a message to the extent that it is not compatible with the framework agreement and related to it documents.

DESCRIPTION OF REQUIREMENTS

1. The Bank is obliged to conclude a written agreement with the Supplier. The law applicable to the contract should be Polish law or the law of another Member State of the European Union, unless the parties to the contract submit the contract to the law of a third country, and the law of a third country allows for effective performance of:
   1) the provisions of the contract;
   2) all the requirements of Polish law imposed on the Bank;
   3) supervisory body guidelines, including in the scope of the Communication.
2. It seems that in the case of processing Bank secrecy in the Cloud Computing and Outsourcing special, and therefore in two cases, where the use of the Service Message is always required Cloud computing will constitute the vast majority (and in the case of processed Mystery banking always) of banking utsourcing within the meaning of Art. 6a et seq. Banking law (subject to further different stance of the KNF Office in this respect). Therefore, it will be necessary to additionally meet the requirements imposed by the provisions of the Banking Law.
3. In accordance with the Civil Code, the contract has a written form when it is concluded in writing, with the declaration of intent submitted in electronic form.
4. If the contract is subject to the law of a third country, the Bank should have a written legal opinion confirming that, in accordance with the applicable contract law, all contractual provisions between the Bank and the Supplier meet the legal requirements and the requirements of the Statement in force Bank.
5. The contract with the Supplier should contain these elements (closed catalog) or indicate their sources listed in point 4.1. Communication that are reasonable regarding the services used and the scope of rocessing information. In addition, in accordance with point 4.2. Statement, the Bank may use framework agreements made available by Suppliers, provided that there is no prejudice to legal requirements and taking into account provisions of the Communication. Explanations to selected elements of the contract with the Supplier indicated in point 4.1. The message can be found in Appendix 2 Explanations and a list of selected clauses with examples.
6. If the contract is subject to the law of a non-EEA state - legal analysis regarding the possibility of effective implementation of the contract, all requirements of Polish law imposed on the Bank and the supervisory authority's guidelines regarding the Communication.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Contract in writing with the Supplier together with the necessary documents (statements, regulations, terms of service, etc.).

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Signing an agreement with the Bank that takes into account the requirements of the Communication and mandatory legal provisions.

TEMPLATES

1. Annex_2_ Explanations and list of selected clauses with examples.

> 5. Information processing plan in cloud computing
>   5.1. The supervised entity, based on the results of risk assessment, develops a documented plan on processing information via cloud computing, which includes at least:
>   a) the type (description) of information processed and, if applicable, information regarding pseudonymisation or anonymization;
>   b) the method of encrypting information and the place (or method) of managing encryptionkeys;
>   c) information on who has access to processed information and how this access is broadcast, managed, received and controlled;
>   d) date of conclusion of the contract with the cloud computing service provider and referencesto this contracts (number, duration, date of extension or amendment, date of starting to usethe services), and if the contr act is not yet concluded - the expected date of its conclusion;
>   e) applicable law to which the contr act is subject;
>   f) a description of the task carried out with the help of cloud computing services together withinformation on whether this is a specific outsourcing of cloud computing as defined in this communication or whether legally protected information is being processed.

DESCRIPTION OF REQUIREMENTS

1. The Bank as part of current and planned information processing (launching the initiative) in Cloud computing should have a documented plan for processing information in Cloud computing in accordance with Annex 3 to the Standard. This plan should in particular contain (preferably in the form of detailed documentation):
   1) description of the task carried out using the Cloud Service;
   2) the type (protected, unprotected), class (public, internal, confidential) and type (production, test) of information processed along with information on whether the processing meets the criteria of Special Outsourcing cloud computing;
   3) information security mechanisms (pseudonymisation, anonymization), information encryptionmechanisms, including the principles of management and storage of encryption keys, and a description of information access control.
2. The plan should precisely specify which data (information) the Bank processes as part of a specific initiative in the cloud.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Information processing plan, e.g. in the form of a completed template set out in Annex 3 to Standard).

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

N/D

TEMPLATES

1. Annex_3_Computing cloud information processing plan.

5.2. Production launch of cloud computing services should be preceded by a testing period during which scenarios adequate to the estimated risk are evaluated using test data (machine-generated or in some other random way), in a documented process.

DESCRIPTION OF REQUIREMENTS

1. The bank should conduct and document the service testing phase. Tests should be carried out on test data; test scenarios should be adequate to the estimated risk (as per paragraph VI of the Communication - Guidelines for risk estimation).

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Documented test scenarios.

2. Formal test results.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

N/D

TEMPLATES

N/D

5.3. The supervised entity has a documented, tested recall plan on its involvement in the processing of information in the cloud computing services of a given provider (also in an emergency), without prejudice to compliance of its operation with the requirements law and other regulations, including in particular related to licenses or permits granted for conducting specific activities.

DESCRIPTION OF REQUIREMENTS

1. The Bank has a plan to withdraw from the Cloud Service both when the strategy changes and in an emergency.
2. The plan should ensure that in the event of an emergency, there will be no prejudice to the compliance of the Bank's operations with the requirements of law and other regulations, including those related to licenses or permits granted for conducting specific activities.
3. The plan to withdraw from the service may assume a return to the "on-premise" environment, migration to another Supplier or other legitimate business scenarios.
4. The plan should be tested, with the scope and approach to testing arising from risk analysis (according to point VI of the Communication - Guidelines for risk estimation) and include issues such as volumes data, required resources etc. The test documentation should contain appropriate audit evidence e.g. test scenarios, expected results, logs or screenshots confirming the fact of carrying out tests as intended.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Plan to withdraw from the Cloud Service.

2. Test scenarios for a plan to withdraw from the Cloud Service.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

N/D

TEMPLATES

1 Annex_4_Template for the cloud exit scenario.
2. Annex_5_Exit from clouds - main issues.

> 5.4. The supervised entity should have a documented business continuity plan taking into account the potential loss of control over processed information at a given cloud computing service provider and the possibility of interrupting the service continuity. For a business continuity plan two or more cloud computing or two or more cloud service providers computational, the supervised entity regularly verifies its own ability to maintain the declared assumptions, in particular the compliance of the service configuration and the reproducibility of the ICT environment, especially after technological changes at one of the cloud service providers.

DESCRIPTION OF REQUIREMENTS

1. The bank should extend its business continuity plans with a scenario that takes into account the potential loss of control over information processed at a given Supplier and the possibility of interrupting the business of cloud computing.
2. The business continuity plan may be based on various scenarios, in particular assuming use on-premise environment, use of another Supplier or temporary alternative process implementation (e.g. manually).
3. The Bank may rely on Supplier's business continuity plans provided that it has supervision on the Supplier's activities in this area, i.e. regular verification of the adequacy of the plan and the results of tests of the business continuity plan and contingency plans (e.g. by verifying the results of independent audits, certifications etc.).
4. In the case of a business continuity plan based on the use of two or more Cloud Computers or two or more Suppliers, the Bank should regularly verify the feasibility of this scenario, especially after technological changes at one of the Suppliers.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. A business continuity plan for the Cloud Service, containing as a minimum the processes and procedures described in the following situations:
   1) the possibility of losing control over the information processed at a given Supplier;
   2) the possibility of interrupting the business of cloud computing.
2. Documentation related to Business Continuity Planning in accordance with the methodologyadopted at the Bank (containing in particular the results of business continuity tests).
3. In the case of a business continuity plan based on the use of two or more Cloud Computers or two or more Suppliers:
   1) documentation verifying the feasibility of this scenario, e.g. conducting a test migration with samples of data or services between two cloud services;
   2) confirmation of carrying out periodic verification of the possibilities of implementing the scenario from above, in particular regarding verification of the possibility of implementing the scenario after technological changes at one of the Suppliers.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

N/D

TEMPLATES

1. In accordance with the Bank's policy.

6. Requirements for cloud computing service providers

6.1. In the field of cloud computing services provided and according to their scale, the cloud computing service provider meets the requirements of ensuring compliance of its operations with the following standards or their equivalents in Polish or European standardization system, unless the supervised entity accepts (based on the results of risk assessment) no need to meet this requirement or part of it:

a) PN-ISO / IEC ISO 20000 regarding the management of IT services;

b) PN-EN ISO / IEC 27001 regarding information security management;

c) PN-EN ISO 22301 regarding business continuity management;

d) ISO / IEC 27017 regarding information security in the cloud;

e) ISO / IEC 27018 regarding good practices for the protection of personal data in the cloud.

6.2. The CPD of the cloud computing service provider meets the requirements of the PN-EN 50600 standard (Equipment and infrastructure of data processing centers) minimum class 3 or ANSI / TIA-942 minimum Tier III, or other appropriate and recognized normative for CPD assessment or containing requirements related thereto, the supervised entity may accept (in justified cases and based on estimation risk) some requirements are not met.

(...)

6.5. Compliance with the requirements may be confirmed by appropriate compliance certificates issued by independent certification bodies accredited in Polish or the European accreditation system.

DESCRIPTION OF REQUIREMENTS

1. Depending on the risk assessment, the bank decides whether the Supplier must fulfil the following either partially or fully:
   Supplier:
   1) the above-mentioned ISO standards;
   2) CPD requirements.
2. The scope of the above requirements for each implementation should be documented by the Bank.
3. Depending on the Bank's decision - the Supplier should undertake in the contract to ensure compliance of the Cloud Service in accordance with the above-mentioned standards or their equivalents (BS standards, standards PN-ISO, etc.).
4. Compliance can be achieved by obtaining independent certification by the Supplier (issued by the certification body); if the Supplier does not have formal certification, he should demonstrate compliance with the above standards by documenting the implementation of the individual requirements of the standards.
5. The scope of certification should include the entire service provided to the Bank, in particular for point 6.2. The message, all CPDs in which the Bank's data (information) is processed.
6. The documentation related to the certification, i.e. the certificate and the results of certification audits or compliance documentation provided by the Supplier, should be provided prior to the conclusion of the contract. and made available to the Bank at least once a year.
7. The bank should regularly verify documentation related to certification; in the event that the abovementioned documentation reveals material non-compliance, the Bank should agree a recovery plan with the Supplier and monitor its implementation.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Documented requirements of the Bank regarding the above mentioned norms and standards, in particular documentation of risk acceptance in case of resignation from selected requirements.

2. Obtaining the Supplier's certificate or other documentation of the Supplier's compliance with the standards.
3. A documented process for regularly assessing documentation related to certification / compliance.
4. Documented process of managing recovery plans agreed with the Supplier in the event of significant non-compliance with standards.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Certification in accordance with the above-mentioned standards, covering the scope of the service provided to the Bank or documentation of compliance with the above-mentioned standards prepared by the Supplier.

TEMPLATES

1. Annex_6_ Template for ISO27001 control documentation.

> 6.3. The supervision recommends that the CPD be located on the territory of the European Economic Area (EEA) country. This point applies with the proviso that supervised entities that:
>
> a) have been recognized by an appropriate decision as operators of key services within the meaning of Art. 5 paragraph 2 of the Act of 5 July 2018 on the national cyber security system and who they use the cloud service in the implementation of the key service or
> b) are critical infrastructure operators within the meaning of the Act of 26 April 2007. about crisis management and who use cloud computing in the scope of implementation of tasks of operating critical infrastructure, should first use CPD located in the Republic of Poland, provided that - in the opinion of the supervised entity - the conditions offered contractual, economic, operational, SLA or functional are no worse than CPD located outside the territory of the Republic of Poland.

DESCRIPTION OF REQUIREMENTS

1. It is recommended to select Suppliers offering CPD in the EEA, which does not exclude the possibility of processing data ((information)) by the Supplier outside the EEA.
2. If the service is to be provided in CPD within the EEA (or in Poland in accordance with item 6.3 of the Communication), the Bank using the services of a global Supplier should define control mechanisms ensuring that the services he uses are provided in CPD within the EEA (or in Poland in accordance with point 6.3 of the Communication).
3. Where the CPD is located in the EEA but the service is also supported by staff having access to data (information) located outside the EEA, it is required to ensure compliance with the provisions in this regard (in particular, obtaining permission from the PFSA is required). 4. Entities that are critical infrastructure operators or key service operators should prefer CPD located in Poland, as long as it offers not worse conditions (security, cost, SLA, etc.) than services located outside of Poland. Therefore, the banks being the above mentioned operators should before choosing a Supplier, verify the availability of an analogous service using CPD in Poland and provide a documented comparison of these services - in particular by comparing (estimating in accordance with the Communication) risk and costs for individual variants.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Unambiguous indication of CPD locations used in the service.
2. For critical infrastructure operators or key service operators (most of the Banks) documentation or control mechanisms confirming CPD locations in Poland (if applicable).

3. If the choice of CPD outside Poland is justified, documented analysis justifying such decision (cost or risk issues).

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Unambiguous indication of all CPD locations (country / region) used in each services (in the form of a Supplier's statement).

TEMPLATES

N/D

6.4. The provider of cloud services provides in its proceedings a documented principle of protecting the information supervised by the entity against unauthorized access or use by your employees or subcontractors by at least:

a) the default rule of no access to the supervised entity's processed information;

b) the default rule of no administrative or user account on virtual machines supervised entity or in other cloud computing services being launched;

c) the "minimum necessary" principle for service privileges granted only when it is necessary to perform the tasks required by the supervised entity (including removal of defects) and for their duration, the implementation of which activities are preceded by the order of the supervised entity, and the entire process of service and performance of activities is logged. The operating procedures in this regard can be additionally confirmed by an appropriate certificate (e.g. SOC 2 Type 2) issued by an independent certification body accredited in European accreditation system;

d) providing guidelines, model configurations, rules descriptions, etc. that clearly define the separation of processing and indicate verification methods configuration correctness;

e) default launch of a new environment (or cloud computing service) separated from other tenants, with "secure-by-default" settings.

DESCRIPTION OF REQUIREMENTS

1. The supplier should provide documentation of data access control mechanisms (information) processed in the Cloud Service, including for its employees (co-workers) and sub-suppliers.
2. The supplier should not have permanent access to data (information) or administrative, service etc. access. at the level of servers, databases, applications or devices.
3. Access to data (information) for the Supplier should be granted temporarily on the basis of a documented request associated with specific administrative, development or support work users (commissioned by the Bank).
4. The supplier should provide documentation confirming the separation of tenants and documentation of mechanisms ensuring the correctness of separation, so that periodic configuration verification can be made.
5. Newly started services should be separated by default (from the moment they are started) and configured in accordance with the best security practices (hardening).

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Documentation of access control mechanisms, assuming that as a minimum the following was adopted:
   1) confirmation of the default lack of access to data (information), administrative and service accounts etc .;
   2) description of mechanisms for granting administrative access.
2. Documentation of data (information) separation mechanisms:
   1) guidelines, model configurations, rules descriptions, etc., which clearly define separation processing;
   2) guidelines, model configurations, descriptions of rules for verification of the correctness of configuration.

3. Security configuration documentation for newly started servers and services ("secure-by-default").

4. Optionally, certificates and certification documentation (audit results, etc.) regarding the functioning of access control mechanisms.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

J.W.

TEMPLATES

N/D

> 7. Cryptography
>
> 7.1. A supervised entity should ensure that information processed in the cloud is encrypted in accordance with the principles set out in this message.
>
> In particular, the supervised entity should ensure that it:
>
> a) It has access to detailed and up-to-date instructions for configuring cloud computing service-sand methods for verifying the correctness of their configuration and operation, in particular regarding in the scope of encrypting processed information;
>
> b) It provides sufficient competence to implement the correct configuration of services cloudcomputing, in accordance with the guidelines of the cloud computing service provider, including the use of encrypted processed information;
>
> c) It uses dedicated cloud computing services or recommended by the service provider configuration settings to increase the security of services rendered cloud computing;
>
> d) legally protected information processed in the cloud is encrypted both at "rest" and "in transit".

DESCRIPTION OF REQUIREMENTS

1. Information processed in the Cloud is required to be encrypted. The mechanisms and scope of using cryptographic security should result from risk analysis (in accordance with point VI, point 5.2 Communication). In particular, the following are required:
   1) encryption, both during transmission and at rest ("at rest" and "in transit") of bank secrecy;
   2) the Bank being provided by the Suppliers with documentation of data encryption mechanisms (information), as well as mechanisms for verifying the correctness of configuration and operation of the above mechanisms;
   3) the Bank's competence in the correct configuration of services, including mechanisms encryption;
   4) use by the Bank of recommended settings to increase security (so-called hardening); these settings should be documented.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Documentation of the encryption mechanisms and methods for verifying the correctness of the encryption configuration.

2. Confirmation of competences held - see point VII. paragraph 3 of the Communication.

3. Documentation of service hardening, in particular encryption mechanisms.

4. Confirmation of data (information) encryption at rest and during transmission (technical documentation, screenshots etc.).

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

J.W.

TEMPLATES

N/D

> 7.2. The supervised entity should ensure that the information is encrypted with keys generated and managed by the supervised entity, unless estimated risk results that it is acceptable or advisable to use encryption keys generated or managed by the cloud computing service provider.
>
> (...)
>
> 7.4. The supervised entity in the documented process manages the creation, use (including access rules), protection, destruction of encryption keys and control of this process.
>
> 7.5. The encryption key management process should include storage within their own infrastructure, copies of encryption keys that have been generated or managed by a cloud service provider and are used in the outsourcing of specific cloud computing, except from risk assessment there is a justified lack of such a need.

DESCRIPTION OF REQUIREMENTS

1. If justified in the risk assessment, the Bank should ensure that the information is encrypted with keys generated and managed by the Bank. Failure to meet this requirement should be supported by an appropriate risk analysis (see point VI.2. Paragraph 5.a) of the Communication).
2. The process of managing the creation, use (including access rules), protection, and destruction of keys encryptors should be documented and have specific controls.
3. In the event of using keys generated or managed by the Supplier, the Bank should ensure that the process mentioned in point 2 above ensures the storage of keys in the Bank's infrastructure, unless the risk analysis justifies the absence of such a mechanism.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Technical documentation confirming that the information is encrypted with keys generated / supplied and managed by the Bank.
2. In the event that point 1 above is not met, a risk analysis indicating the admissibility of use encryption keys generated / delivered and managed by the Supplier.
3. Formalized (documented) process of managing the creation, use (including access rules), protection, destruction of encryption keys and storage of key backups in the Bank's infrastructure.
4. In the event that the encryption key management process does not provide storage of copies of the keys in the Bank's infrastructure, a risk analysis indicating a justifiable absence of such a need.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Description of the procedures and mechanisms for managing encryption keys, formalized (documented) the process of managing the creation, use (including access rules), protection, and destruction of encryption keys.

TEMPLATES

N/D

7.3. In the event that the risk assessment requires the maintenance and management of encryption keys using hardware solutions (HSM), this HSM can be provided by a cloud computing service provider, with including this element in risk estimation. HSMs should meet the minimum requirements of FIPS 140-2 Level 2 or equivalent.

DESCRIPTION OF REQUIREMENTS

1. Depending on the results of the risk analysis (point VI. Paragraph 2)

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Documentation of HSM used confirming compliance with FIPS 140-2 Level 2 or equivalent.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. As above, if HSM is made available by the Supplier.

TEMPLATES

N/D

8. Monitoring the information processing environment in cloud computing services
   - 8.1. The supervised entity has documented rules for collecting related logs with information processing in the cloud computing, according to the scope used cloud services, processed information and risk assessment results.
   - 8.2. The supervised entity protects logs against unauthorized access, modification or deletion for a period consistent with the established security principles resulting from the risk assessment and specific provisions in force in this respect.
   - 8.3. Authorized personnel of the supervised entity shall review the logs in accordance with documented security procedures and principles, depending on on the scale of operation, type and number of logged events, and security architecture - Supervision recommends using specialized correlating software event records (SIEM) and regular review and update of correlation rules.

DESCRIPTION OF REQUIREMENTS

1. An important element related to the use of information processing services in the Cloud is the issue of monitoring the information processing environment in the Cloud Service.
2. In accordance with the guidelines of the Communication, as regards monitoring the information processing environment in the Cloud Service, the Bank should:
   1) have documented rules for collecting logs related to information processing in the Cloud computing, according to the scope of cloud computing Services used, information processed and risk assessment results;
   2) secure logs against unauthorized access, modification or deletion for a consistent period with established safety principles resulting from risk assessment and applicable detailed provisions in this respect;
   3) Depending on the scale of operation, number of logs etc. consideration should be given to transferring logs from cloud computing to the SIEM system and developing correlation rules to detect a security incident in the cloud.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Documented rules for collecting logs related to information processing in the cloud.
2. It is recommended to use specialized software for correlating event records (SIEM).

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Documentation in the field of event logging in the cloud, as well as the possibility of integration of cloud logging mechanisms with the SIEM system used in the Bank.

TEMPLATES

N/D

> 8.4. Requirements for the supervised entity in the scope of managing service providers with remote access to cloud computing services used by supervised entity:
>
> a) the supervised entity ensures that only authorized personnel of the service provider have access to the indicated ICT systems or their selected ranges;
>
> b) the supervised entity requires the service provider's staff to use MFA authentication, the type and scope of which depends on the results of the risk assessment;
>
> c) the supervised entity ensures that administrative or privileged access is provided from the trusted networks of the supervised entity or supplier services and under control (including e.g. by recording the session and its parameters, then by analyzing the regularity and purposefulness of activities carried out), unless risk estimation indicates a justified lack of such a need.

DESCRIPTION OF REQUIREMENTS

1. The bank should ensure through control mechanisms or contractual records that access to the systems used in the cloud service has only authorized personnel on the side of the Supplier.
2. Access of the Service Provider's personnel to the systems used in the Cloud should be secured by strong multi-factor authentication.
3. The Supplier's personnel should only access from secure workstations / terminals located in a secure (trusted) network location.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Documented procedures or contractual provisions confirming the restriction of access only to the Supplier's authorized personnel from secure network locations and workstations / terminals.
2. Description of authentication mechanisms.
3. Documented procedures for periodic verification of the Supplier's access to the systems used in the service.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Use by the Supplier's personnel having remote access to the Bank's cloud computing environment, MFA authentication and secure stations in secure network locations.
2. Depending on the results of the risk analysis carried out by the Bank, other mechanisms to monitor access and accountability of the Supplier's activities, e.g. recording sessions and its parameters in the event of Supplier's administrative access or privileged access of the Bank's staff.

TEMPLATES

N/D

9. Documenting the activities of the supervised entity
   9.1. Where justified, depending on the scope and type of information processed, rules and regulations in force and adopted in the organization (including corporate and group relationships, if any) and risk assessment results and taking into account the principle of proportionality, the supervised entity has documentation containing:
      a) the organization of employees or associates responsible for cyber security, including positions or functions related to monitoring and analyzing and reporting incidents related to information processed in the cloud computing, together with the required competences, permissions and responsibilities described;
      b) architecture of networks, systems and applications as well as interconnection points of internal networks supervised entity with untrusted networks, including solution architecture in cloud computing, also taking into account test environments and contingency scenarios;
      c) rules for categorizing information or systems for cloud computing calculation or reference to currently functioning classifications if they can be used;
      d) principles of applied technological safeguards and organizational solutions;
      e) business continuity management policies;
      f) the principles of ongoing security of processed information and in the event of planned or unplanned termination of cooperation with the cloud service provider;
      g) compliance management rules (including software licensing processes), including compliance with regulatory requirements;
      h) principles of review and management verification of the associated security system using cloud computing services;
      i) rules for reporting, reviewing and verifying quality parameters of cloud computing services;
      j) contracts with cloud computing service providers with additional statements, if necessary to confirm compliance with the requirements;
      k) processes, procedures or instructions for:
         I. threat analysis and risk assessment, including sources of information about the threats specific to the cloud computing services used and the financial sector;
         II. ICT environment management (networks, systems, applications, databases, etc.) including cloud services, including planning, development and maintenance;
         III. log management;
         IV. encryption key management;
         V. managing security incidents;
         VI. conducting internal audits of ICT security taking into account the specifics of cloud computing.
   9.2. The documentation is protected against unauthorized access, unauthorized change, damage or destruction. Principles of document management entity supervised is defined within the organization management system.

DESCRIPTION OF REQUIREMENTS

Section VII.9 of the Communication sets out the organizational and documentation requirements that the Bank should have (e.g. as policies or other regulations) wanting to implement cloud services.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

1. Documenting the organization of the Bank's employees or associates responsible for cyber security, including elements from point 9 a) of the Communication.
2. Documenting the architecture of the network, systems and applications as well as the interconnection points of the Bank's internal networkswith untrusted networks, including the architecture of the implemented cloud

computing solution, including test environments and emergency scenarios.

3. Documenting the rules for categorizing information or systems for processing in the Cloud.
4. Documented principles (policy) of technological security solutions and solutions used in the organization organizational in relation to cloud computing solutions.
5. Documented principles (policy) of business continuity management.
6. For the implemented Cloud Service, documented rules for ongoing security of processed information, as well as for planned or unplanned termination of cooperation with the Supplier.
7. Documented principles (policy) of compliance management (including software licensing processes), including compliance with regulatory requirements.
8. Documented principles (policy) of review and management verification of the associated security system with the use of cloud computing (e.g. annual review).
9. Documented principles (policy) of reporting, reviewing and verifying quality parameters the functioning of cloud computing services.
10. Agreement with the Supplier together with additional statements, if necessary to confirm compliance requirements.
11. Description of processes, procedures or instructions regarding the areas indicated in items i. To vi. point 9.1. Communication.
12. Documented policies for managing policies and documentation within the organization's management system, ensuring protection against unauthorized access, unauthorized alteration, damage or destruction.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE SUPPLIER'S SIDE

1. Documenting the solution architecture in the cloud computing, including test environments and contingency scenarios.

TEMPLATES

N/D

5.5. POINT VIII OF THE COMMUNICATION - "RULES FOR INFORMING THE PFSA ABOUT THE INTENTION TO PROCESS OR INFORMATION PROCESSING IN THE CLOUD"

VIII. Rules for informing the PFSA about the intention to process or information processing in the cloud

1. In cases of outsourcing specific cloud computing or processing legally protected information, a supervised entity within 14 days before commencing information processing in the cloud (and in the case when the processing is already being implemented - no later than August 1, 2020) must inform the KNF about:
   1) the type and scope of information planned for processing / processed in the cloud;
   2) the name of the cloud service provider and the type of services planned to be used / used cloud services;
   3) the date of signing the contract with the cloud service provider and its dates validity,and if the contract is not y et concluded - expected the date of its conclusion;
   4) location (country, region or other equivalent) data center (CPD) providing cloud computing services;

5) meeting the requirements described in this communication;
6) contact persons or positions regarding the use of cloud computing in a supervised entity.

2. The above information should be signed by an authorized representative of the supervised entity and delivered to the KNF Office using the form attached as Annex 1 to this communication.

DESCRIPTION OF REQUIREMENTS

1. The message requires informing the PFSA about the intention to process or process information in the Cloud only in two cases: (i) Cloud services constitute special Outsourcing or (ii) a Bank Secret is being processed in the Cloud.
2. Applications must be made 14 days before processing information in the Cloud (or while the service is already being provided at the date of the Communication), which means that the meaning is not the same conclusion of an outsourcing contract, but transfer of Supplier's data (information), including those covered by Secrets banking (regardless of whether it is in the pre-production phase or already in the production phase).
3. Persons authorized to sign the information referred to in point VIII. The message is both the Bank's management (as represented in the National Court Register), as well as persons duly authorized by the management board. The decision can take the form resolutions of the board.

REQUIREMENTS (PRODUCTS) TO BE DEVELOPED ON THE BANK'S SIDE

4. Annex 1 of the Communication, completed and signed by duly authorized persons.

REQUIREMENTS (PRODUCTS) ON THE SUPPLIER'S SIDE

N/D

TEMPLATES

N/D

6. BANKING LAW

The following commentary to the provisions of the Banking Law applies only to the situation when the Cloud Service is also banking outsourcing within the meaning of Art. 6a et seq. Banking Law. As already indicated in this Standard (and as long as the KNF Office does not express otherwise), Cloud Service computation, on the basis of which the Banking Secret is processed, is always banking outsourcing within the meaning of Art. 6a et seq. Banking law (only the ordering of banking activities is related with the disclosure of Bank Secrets). when it comes to special outsourcing, banking outsourcing will usually take place.

6.1. ART. 6A. BANKING LAW

6.1.1. OUTSOURCING AGREEMENT

1. Contract for the supply of cloud computing services, which is an outsourcing contract within the meaning of art. 6a The Banking Law meets the following criteria:
   1) is always in writing;
   2) has the form of an agency contract regulated by the provisions of the Civil Code from Art. 758 to art. 764 (9) if it concerns activities specified in art. 5 and art. 6 of the Banking Law and consists of the provision of services indicated in art. 1 clause 1) from a) to j) of the Banking Law (Article 758 § 1 of the Civil Code: "By contract the agent accepting the order (agent) undertakes, in the scope of its enterprise, to permanently mediate, for remuneration, when concluding contracts with clients for the employer or to conclude them on his behalf ");
   3) if it relates to activities other than those indicated in point 2) above, the outsourcing agreement will havethe form of unnamed contracts exercising their freedom of contract;
   4) contracts with Suppliers will additionally require KNF authorization, when Cloud Services will consist of:
      a) performing activities related to issuing and holding bank securities and other securities, as well as performing other commissioned activities related to the issue and handling of securities,
      b) recovery of the Bank's receivables,
      c) performing other activities, after obtaining the permission of the Polish Financial Supervision Authority.

6.1.2. SUB-OUTSOURCING

1. The possibility of outsourcing is limited to:
   1) chain outsourcing only one level down;
   2) permission for sub-outsourcing is required in the contract for cloud computing and additional services Bank's consent to conclude specific outsourcing; and
   3) there is no possibility of sub-outsourcing the subject of the service, the possibility of sub-outsourcing only activities auxiliary and technical services needed to implement the Cloud Service.

COMMENT

1. Agreements with Suppliers due to the subject of the service provided will be mostly unnamed contracts not requiring KNF approval (subject to further comments), which you rely on will be providing actual activities related to banking activities.
2. Explanation of the concept of actual activities related to banking activities indicated in art. 6a paragraph 1. point. 2) Banking law: actual activities shall mean: all activities that are not banking activities as indicated in art. 5 and art. 6 of the Banking Law, but they are in a direct and functional relationship with them.

6.2. ART. 6B. BANKING LAW

6.2.1. LIABILITY UNDER THE CLOUD SERVICES CONTRACT

1. **The Supplier's responsibility towards the Bank:**
   1) full liability towards the Bank for damages caused to customers for non-performance or improper performance of the contract for the Cloud Service. Cannot be turned off or restricted;
   2) the possibility of modification consisting only in the extension of such liability (liability on a risk basis, indication of the mechanism for calculating damage, extension of liability for lost profits).
2. **The Bank's responsibility towards the Bank's client:**
   1) the Bank's full liability to the Bank's customer for damages caused by non-performance or improper performance of the contract for cloud services may not be turned off or restricted;
   2) the possibility of modification consisting only in the extension of such liability (liability on a risk basis, indicating the mechanism for calculating damage, extending liability to lost profits).

6.3. ART. 6C. BANKING LAW

6.3.1. PERFORMANCE OF THE CLOUD COMPUTING CONTRACT AND RECORDS AGREEMENTS

1. A cloud service contract may be concluded and performed only if:
   1) the bank and the Supplier will have action plans ensuring continuous and uninterrupted operation in the field covered by the contract;
   2) entrusting the performance of activities under the cloud services contract will not adversely affect the Bank's operations in accordance with the law, prudent and stable management of the Bank, the effectiveness of the internal control system at the Bank, the ability to perform the duties of a certified auditor authorized to audit the financial statements of the Bank based the agreement concluded with the Bank and the protection of the Banking Secret (it is recommended to obtain a legal opinion on this range);
   3) the bank will take into account the risk associated with entrusting the performance of such activities in the management system risk.

COMMENT

1. The Bank is required to enter a contract for cloud computing services into the contract records by specifying at least in it:
   1) data (information) identifying the Supplier,
   2) the scope of the Cloud Service,
   3) place of performance,
   4) the duration of the contract.

6.4. ART. 6D BANKING LAW

6.4.1. PERMISSION TO CONCLUDE A CONTRACT FOR CLOUD SERVICES

1. Permits of the KNF Office will require:
   1) concluding a contract for Cloud Services with a Supplier whose registered office is in another country than an EU Member State; or
   2) concluding a contract for cloud computing services, which will be performed outside the EU member state (examining what part of services is performed in the EU and outside).

7. ANNEXES

ANNEX 1. Risk assessment template

ANNEX 2. Explanations and list of selected clauses with examples

ANNEX 3. Plan for processing information in the cloud

ANNEX 4. Template scenario for exit from the relationship with the supplier

ANNEX 5. Exit from the cloud - main issues

ANNEX 6. ISO27001 control documentation template

ANNEX 7. Cloud implementation plan

ANNEX 8. Cloud implementation diagram

ANNEX 9. Requirements for suppliers

RISK ASSESSMENT TEMPLATE

Threats	Risk description	Risk description	Inherent risk assessment (Low / medium / high)		Risk limiting factors	Action plan with risk./ Risk limits	Residual level risks (short/ average/ high
			Influence	probability			
1.	Geographic dispersion processed information (VI.1.a)	Risk of compliance of the processing process information with laws and regulations internal contractual obligations and declarations and other regulations			Cloud computing service is provided in the following locations: 1) .... 2) .... ***An example of a risk mitigation factor:*** ***Legal opinions were obtained confirming the ability to ensure process compliance information processing with banking law***		
2.	Possibility of losing compliance of the supervised entity with legal regulations (including issued ones licenses and / or permits) (VI.1.B)	Using cloud computing services unintentionally or otherwise than intended. Access to processed information through employees and co-workers					
3.	Access to processed information by unauthorized persons (VI.1.C)	Access to processed information through employees and associates (e.g. sub-suppliers) of a cloud computing service provider					

4.	Attachment to one supplier cloud computing services (VI.1.E)	No technological compatibility between services of different cloud computing providers, resulting in attachment to one cloud computing service provider					
5.	No technological compatibility between services of different cloud computing providers, resulting in attachment to one cloud computing service provider	Failures of resource isolation mechanisms used to provide cloud services computing					
6.	Limited ability to influence on the scope, shape and changes of services (VI.1.h)	Limited ability to influence the scope, shape and changes of services, in particular for the retention process of processed information and removing them after completion processing services					
7.	Limited ability to control cloud service provider (VI.1.i)	Limited ability to control cloud computing service provider and its sub-suppliers, including direct verification of physical, technical and organizational security mechanisms and control of cloud computing services					
8.	Division of responsibility (VI.1.j)	Division of responsibility for safety processed information between the cloud service provider and the entity supervised					
9.	Possibility of using services in a manner inconsistent with the entity's intentions supervised (VI.2.a)	The ability to use services in a manner inconsistent with the intentions of the supervised entity or in an environment that is not subject to the control of the supervised entity (e.g. private mobile devices, access from private ones or public networks)					
11.	Use default or publicly available parameters configuration services (VI.2.c)	Use default or publicly available configuration parameters services, without proper verification and evaluation adequacy for the needs of the supervised entity					

12.	Authentication mechanisms used (VI.2.d)	Weakness of the authentication mechanisms used					
13.	Human resources (VI.3.a)	Required and owned resources, including established human resources					
14.	Compliance of the technological environment (VI.3.b)	Technological compatibility of the ICT environment and the environment cloud computing, in particular integration mechanisms					
15.	Information encryption (VI.5)	Compliance of information encryption with supervisory requirements					
16.	Control of the "outsourcing chain" (VI.6)	Assessment of the "outsourcing chain" from the perspective of specific legal provisions regarding specifically carried out information processing activities					

EXPLANATIONS AND LIST OF SELECTED CLAUSES WITH EXAMPLES

In accordance with point VII. 4.1. Of the Communication, the contract with the Supplier should contain at least the provisions regulating:

a) clear division of responsibility in relation to the security of processed information, including the service provision model, service continuity (including RTO and RPO parameters where appropriate) and declared SLA along with the measurement and reporting method;

EXPLANATION:

1) It should be noted that the definitions of "RTO", "RPO" and "SLA" contained in the contract comply with the definitions contained in the Communication.
2) The liability model with regard to the security of processed information is based on practice market - it is important that the agreement clearly defines the division of responsibility.

b) a clear definition and indication of the location of information processing and methods for its verification and compliance compliance by at least a reference reference to the relevant documents, configuration descriptions, methods and tools;

EXPLANATION:

1) The message in its content indicates the requirement to provide the CPD address (precise location indication). Lack such information may pose a threat to the physical security of processed information, therefore as a minimum, an indication is sufficient, e.g. "access zones" or "region", and such an indication should at least include the country and approximate CPD location (e.g., city or geographic region). CPD should but it does not have to be in an EEA country.
2) We would like to draw your attention to the fact that, in accordance with the Communication, Banks that have been recognized as operators by an appropriate decision key services or are operators of critical infrastructure, should first use CPD located in Poland provided that - in the Bank's assessment - the contractual, economic and operational conditions offered, SLAs or functional are not worse than CPDs located outside the territory of the Republic of Poland.
3) There is no definition of "information processing" in the applicable law. Therefore, when creating an exemplary definition of information processing, the definition of data processing included was used in art. 4 point 2) GDPR.

EXAMPLE CLAUSES:

1. [Definitions] "Information processing": an operation or set of operations on information or sets of information carried out in an automated or non-automated manner, such as collection, recording, organizing, organizing, storing, adapting or modifying, downloading, browsing, using, disclosing by sending, distributing or otherwise sharing, matching or combining, limiting, deleting or destroying.

c) the applicable law of the contract (including the court with jurisdiction and dispute settlement rules);

EXAMPLE CLAUSES:

APPLICABLE LAW, JURISDICTION

1. This Agreement and any non-contractual obligations arising out of or arising in connection with it are subject to Polish law.

2. Each Party irrevocably agrees, unless the law provides for exclusive jurisdiction to any disputes that may arise in connection with this Agreement or which are related to its breach, denunciation or invalidity have been settled by a common court having jurisdiction over [e.g. The Capital City of Warsaw (Warsaw Śródmieście).]

or if the contract is subject to a law other than Polish:

1. This Agreement and any non-contractual obligations arising therefrom or arising from it law [________] [law of a state other than Polish].
2. Due to the fact that the Employer [Bank] is a supervised entity within the meaning of the Polish Act of 21 July 2006 on supervision of the financial market (Journal of Laws 2019.298), and the Employer's use of services that are provided by The Supplier under this Agreement is strictly regulated, the Supplier hereby declares that the law of the country to which the Agreement has been subject allows for the effective implementation of the provisions of this Agreement, the requirements of Polish law imposed on the Employer and the guidelines of the Polish supervision authority, including the Communication. Detailed description of the requirements Polish law and guidelines together with legal analysis regarding the possibility of their effective implementation under the law [_______] is attached as Annex [__] to the Agreement.
3. Each Party irrevocably agrees, unless the law provides for exclusive jurisdiction to any disputes that may arise in connection with this Agreement or which are related to its breach, denunciation or invalidity have been settled by a common court having jurisdiction over [______________________].

d) confirmation of the compliance of the rules for the processing of personal data with European Union law, if applicable;

EXPLANATION:

1) The current legal status is about compliance with the GDPR. For clarity, by the phrase "if applicable" it is a situation when data is processed on the basis of an outsourcing agreement in the Cloud personal.

e) ownership of the information processed during the contract term and after its termination (expiration, termination), also in an unplanned manner;

n/a.

f) guarantees, warranties, insurance (insurance policies of the cloud service provider), contractual penalties, determination of force majeure, events falling under force majeure and the rules to be followed in such situations, if applicable;

g) determining the scope of liability for damages caused to the clients of the supervised entity (if applicable), in accordance with the requirements of the law applicable to the supervised entity;

EXPLANATION:

1. In the case of banking outsourcing, the prohibition on limiting liability in relationships applies Bank - customer, Supplier - Bank. For the sake of clarity, the phrase "if applicable" means the situation when based on the contract for Cloud Services, information is processed that may be lost or disclosed cause damage to the customers of the Banks.

EXAMPLE CLAUSES:

1. The Supplier shall bear full and unlimited liability towards the Bank for damages caused to customers Bank as a result of non-performance or improper performance of the Agreement.

h) clear indication of the sub-suppliers (name, location, scope of activities) of the service provider cloud computing and conditions for granting access rights to information processed by the supervised entity;

EXPLANATION:

1) Updating the list of subcontractors requires a change (annexing) the outsourcing contract each time. A change of sub-supplier without the Bank's consent may be the basis for immediate termination by the Bank. It is also possible that the Supplier must inform the Bank in advance unilaterally updates the list of subcontractors. In this case, however, the Bank's refusal to update to the Supplier means the termination of the contract immediately.

2) We propose that the list of sub-suppliers be attached to the Agreement in the form of an attachment.

> i) a clear indication of the principles according to which tasks, terms of reference and responsibility and the accountability of the activities of all sub-suppliers of a cloud computing service provider, who have access to processed information are transparent and clearly identified by a supervised entity;

EXAMPLE CLAUSES:

1) [In the form of the Bank's statement in the section ‚Declarations and assurances'], the Bank represents and ensures that the tasks, scopes of rights and responsibilities as well as the accountability of the activities of all Sub-suppliers are transparent and have been clearly identified by the Bank.

> j) sources of authorized information about planned changes in provided standards cloud computing services (including technical changes);

EXPLANATION:

1) It seems that the purpose of this provision is to clearly indicate in the contract communication channels used to inform about planned changes in the standards of services rendered, e.g. through indication of a dedicated website address or e-mail address of an authorized employee of the Supplier and an employee of the Bank for communication.

> k) sources of technical documentation and declaration of compliance (including compliance with applicable law), together with instructions regarding the configuration of cloud services computing;

EXPLANATION:

1) It seems that the purpose of this provision is to clearly indicate in the contract the communication channels for sending technical documentation, declaration of compliance and service configuration instructions e.g. by indicating a dedicated website address or the email address of an authorized employee The supplier and the Bank employee for communication.

> l) the scope of additional information and documentation provided by the service provider cloud computing in connection with the provision of cloud computing services;

EXPLANATION:

1) The wording of the decision will always depend on the type of services rendered and arrangements of the parties.

> m) the right of the supervised entity to carry out inspections in information processing locations, including the right to audit the 2nd or 3rd party at the request of the supervised entity (if necessary due to risk assessment);

EXPLANATION:

1) Pursuant to the GDPR, the administrator in the entrustment agreement concluded with the processor must include a provision on enabling the administrator or auditor authorized by the administrator of audits, including

inspections. It is therefore necessary to include in the contract for the Service cloud-based capabilities and inspection principles. this possibility should not be excluded, irrespective of the results of the risk assessment. However, depending on its results, you can get addicted the right to conduct an audit / inspection by the Bank (high risk) or a third party (medium and low) risk). The right of inspection may, however, be contractually restricted, e.g. by indicating that it will only be used if other control measures fail, are impossible to carry out or they would be insufficient in the given facts.

n) the right for supervision to perform inspection duties, including room inspections and documentation related to the processing of supervised entity information, processes and procedures, organization and management, and compliance confirmations;

EXPLANATION:

1) The supplier must be aware that the contract contains the authorization for banking supervision (UKNF) to perform control responsibilities.

o) licensing rules (including the right to update the security of used software and / or its components) and intellectual property rights, including - if concern - the right to dispose of processed information;

p) the rules for changing the content of the contract, including technical parameters of the cloud computing services used computing;

n/a.

q) the rules for terminating the contract, including the rules and deadlines for returning and / or deleting processed information;

EXPLANATION:

1) The contract should regulate the date of implementation of these obligations, as well as the method of confirming the deletion of copies processed information.

r) support rules, including scope and time windows (including time zones), mode and how to report problems with cloud services;

n/a.

s) rules for the exchange of information, including in particular in the field of security and management of current incidents, covering both employees of the supervised entity and the provider of cloud services, and in the event of significant exposure to effects of a given incident - also other parties (e.g. customers, subcontractors, etc.) for the purpose ensuring the adequacy of the proceedings to the level of materiality of the incident.

n/a.

INFORMATION PROCESSING PLAN IN THE CLOUD COMPUTING

1. INFORMATION ON FULFILLED TASKS AND PROCESSED INFORMATION

System / application name, whose information is processed	…
Description of the task being carried out using the service	…
Type of information processed	☐ Protected (banking secret) ☐ Other protected (from other legal provisions) ☐ Unprotected
Classification of information[1]	☐ Public ☐ Internal ☐ Confidential
Information Type	☐ Production ☐ Test
Special outsourcing	☐ Yes ☐ No
Description of the format and structure of the information	… *(may be a reference to detailed documentation)*

2. INFORMATION PROTECTION

Security mechanisms Information	☐ Masking ☐ Pseudonymisation ☐ Anonymisation ☐ Other
Description of mechanisms of information security	… *Describe what fields and how they are subjected the following security processes*
Description of mechanisms of information encryption	… *(may be a reference to detailed documentation)*
Management and storage of encryption keys	☐ Supplier ☐ Bank
Description of access control to processed information	… *information on who has access to processed data and how this access is granted, managed, received and controlled*

3. CONTRACT WITH THE SUPPLIER

Provider	
Contract No.	
Law applicable to the contract	
Duration of the contract	
Date of last change to the contract	
Date you started using the service	

4. OTHERS

Date of next plan verification	
The date the plan was last updated	
The scope of the last update	

EXIT SCENARIO FROM THE SUPPLIER RELATIONSHIP

1. DESCRIPTION OF THE SERVICE

Agreement ID	
Service (subject of the contract)	
Provider (entrepreneur's name / company)	
Planned date of complete processing data in the Cloud:	
Contract notice period: a) by the bank b) by the supplier	

2. PROCEDURE IN RELATION TO THE EXPIRY OF THE CONTRACT

Strategy assumed	**Extending the relationship with the current supplier:** □ Conclusion / extension of the contract with the current supplier **Implementation of the service by another entity:** □ Selecting a new supplier **The service is provided by other current suppliers** □ Continuation with existing suppliers **Return to bank:** □ Takeover of the business by a bank unit **Cessation of activity:** □ Failure to continue after the contract expires **Other:** □ …………………………………. □ ………………………………….
	Choose the preferred option from those listed above:

3. KEY ACTIONS ENABLING IMPLEMENTATION EXIT SCENARIO

Extension of relationship	
Implementation of the service by other entity	
The service is provided by the bank (return to the bank)	
Cessation of activities	
Other	Examples

4. BANK IMPLEMENTING UNITS INVOLVED IN EXIT SCENARIO

Scenario implementing units	
Supporting units	
Units informed on the implementation of the scenario	

5. DOCUMENT HISTORY

Created review / change date	Authorizing (Director / Manager Team in the unit of Functional Owner)	Comment / scope of changes

EXIT FROM THE CLOUD - MAIN ISSUES

CHAPTER I

SERVICE WITHDRAWAL PLAN

1. WITHDRAWAL SCENARIOS

1. Specify the anticipated withdrawal scenarios for the service, e.g. on premise migration, change of provider etc.
2. It is allowed to specify alternative scenarios depending on the situation - e.g. sudden cessation of service provision, resignation from the service after the end of the contract, etc.

2. IMPACT OF CHANGE ON ORGANIZATIONS

1. Describe the impact of change on organizations, i.e. changes in critical processes, impact on human resources and organizational structure, training requirements etc.

3. DESCRIPTION OF THE SERVICE AND DATA TRANSFER

1. High-level description of the process of service and data migration, required tools etc.
2. Transfer of Services is the entirety of activities (including legal acts) leading to the return of the Customer's equipment to the Customer, the Customer's software, all Customer Data processed at the Customer's request and, depending on legal circumstances, the transfer to the Customer of contracts with third parties required for implementation Services defined in the Agreement in a manner that guarantees the uninterrupted performance of the Services.

4. WITHDRAWAL TEST SCENARIOS AND ACCEPTANCE CRITERIA

1. Test scenarios for migration processes.
2. The Customer together with the Supplier is obliged to perform periodic tests of the Exit Plan with the recommended frequency not less frequently than once every 12 months.

5. DATA BACKUP AND MIGRATION TIMES

1. Estimate the time needed to prepare the switching project, start operational works, obtaining appropriate consents and informing service users about the planned switchover.
2. Specifying the time to download data for migration from the Supplier. Time must include contractual provisions with the supplier for data extraction and physical transfer (including network conditions and time to mount data).
3. Specifying the time for the process of service switching in the initial and target dimension of data migration, as well as starting the service on the restored data. This time may not violate the adopted RTO and RPO for the service.
4. For services critical for the Bank's business continuity, a local backup of data transferred to the cloud should be kept to minimize the service switching time. Backup range and retention time data should be defined in terms of risk to business continuity. Backup aims to only minimizing the initial switching time of the most critical data. Total Migration Time assumes obtaining all data from the Supplier.

6. MIGRATION SCHEDULE

1. Estimated migration schedule for "on-premise" or to another service. It should be a project schedule, containing the required resources, tasks and milestones.

7. ROLES AND RESPONSIBILITIES

1. Defining roles and responsibilities in the migration process

2. Supplier's obligations

3. In the event of termination or termination of the Agreement for any reason, the Cloud Service Provider shall provide the Customer, immediately after the expiry or termination of the Agreement, the ability to transfer Customer Data through:
   1) enabling the Customer to download Customer Data from its infrastructure within the time limit set by Customer and Cloud Service Provider,
   2) issue of logins and passwords in accordance with the Agreement,
   3) ensuring proper protection of customer data contained in the logs of shared systems,
   4) return of the Customer's equipment brought into the Supplier's infrastructure, if such a situation took place,
   5) return of documentation in paper version (if there was one).

4. The cloud service provider will provide the customer, depending on legal circumstances, the possibility of continuous uninterrupted use of licenses necessary to maintain the continuity of services, including providing the option of transferring, depending on legal circumstances, the license referred to in the item above to the Customer.

5. The cloud service provider is obliged to:
   1) irreversibly delete the Customer's data and the Customer's software from the Supplier's resourcesand cooperating subcontractors,
   2) in particular, irreversible deletion of Customer data from the resources of the Supplier and cooperating subcontractors having the nature of personal data and data covered by banking or professional secrecy,
   3) cooperation with the client in the field of data transfer to the client or other entity indicated by Client
   4) ensuring the cooperation of its subcontractors in the implementation of the exit plan,
   5) determining together with the Customer: a) a detailed schedule of the exit plan, b) a detailed scope of activities carried out, c) a detailed way of implementing the exit plan, d) responsibility Parties, e) technical measures necessary to implement the exit plan, if needed.

8. REQUIREMENTS FOR SERVICE WITHDRAWAL (HARDWARE ETC.)

8.1. SCENARIO 1 ON-PREMISE MIGRATION

1. Define local environment parameters in terms of availability, performance and capacity to take over the cloud service they are in.

2. The exit plan should also include:
   1) appointing dedicated managers responsible for carrying out the transfer process cloud services,
   2) preparation for transport, in a manner agreed by the Parties, of all the Customer's equipment, if any element of service provision,
   3) issuing passwords and logins to the Customer allowing for further use of customer data, including passwords and logins for databases and all systems covered by services,
   4) providing by the cloud service provider of all information regarding the method of providing and servicing rendered services relevant from the point of view of transfer of services and transfer maintenance competences of another entity,
   5) providing a secure ICT connection on the side of the Cloud Service Provider platform, used to provide cloud services, to the IT system indicated by the Customer, using a secure ICT network, to carry out customer data transfer,
   6) providing by the Customer technical resources on the part of the Customer's IT system enabling the establishment of an ICT connection,
   7) ensuring the transfer of all data to the ICT system indicated by the Customer the client in a manner ensuring their full security and integrity, and the level of transfer enabling efficient transfer of all client data within the time agreed by the Parties, as well as issuing all backup copies of customer data (if made in accordance with the Agreement),
   8) the provision of cloud services by the Service Provider specific knowledge of implemented cloud services, to the extent that it will be necessary for the further implementation of services by the Customer or a third party indicated by the Customer,

9) immediately after the termination of the provision of cloud services, removal by the Supplier and contractors Providing cloud services in a sustainable manner and in line with best practices in this respect, all copies of the customer's data, if any (after prior transfer of such data to the Customer or an entity designated by the Customer) and all data and information (e.g. configuration files specifically used for a given Customer but not constituting part of the Provider's Cloud Services) used for configuration, operation, backup and archiving of the system or its individual components.

3. The requirements include:
   1) the appropriate number of servers including their location in data centers,
   2) provide free space in data centers along with ensuring the physical possibility of connecting to the infrastructure,
   3) appropriate server configuration to ensure appropriate performance (the appropriate number of processors, the appropriate amount of RAM, appropriate network connections, adequate disk resources),
   4) the appropriate amount of disk space that is necessary to take over stored data in the cloud service. This space must be foreseen for one year and updated once a year in the switching plan.
4. The defined environment is available in one of the following approaches:
   1) physically purchased and configured for the needs of migration,
   2) not purchased, but available from the manufacturer in the given configuration. Such availability is confirmed a letter of intent or an agreement with the supplier specifying the time to acquire and deliver the infrastructure,
   3) has infrastructure used for other purposes, which may be in the event of commissioning plan released and in the transition period for purchase, can be used to perform the switch.

8.2. SCENARIO 2 MIGRATION TO ANOTHER SERVICE PROVIDER

1. Alternative cloud services with suppliers, commissioning time and cost.

Alternative service	Key functionalities not available in the alternative service	Start time services / Estimated time migration	Expense

2. Determining the minimum security requirements for service withdrawal:
   1) security requirements for the target solution after withdrawal,
   2) security requirements for the migration process.
3. The process of data migration and service switching.
4. The process must take into account the following points together with their operational development and technical details. Execution instructions for all roles defined in the process should be developed for process description.
   1) formal decision to withdraw or switch. Determining the rules for issuing such a decision and its procedure,
   2) informing users about launching the switching plan, together with the expected times and effects for users,
   3) acquiring and configuring infrastructure,
   4) extracting data from the supplier and physically transferring it,
   5) mounting data from backup in the Bank's environment and informing about the initial launch of the service,
   6) mounting data from the Supplier and informing about full service switching.
5. The customer may decide to exclude the implementation of certain obligations arising from the exit plan. If the Customer makes such a decision, the Parties shall adapt the exit plan to the changes introduced by the

Customer - in particular in connection with the resignation from specific tasks, the Customer may request shortening the exit plan implementation schedule.

6. During the implementation of the exit plan, the Parties shall provide technical staff with the competence and knowledge enabling the implementation of the exit plan agreed by the Parties on the agreed date.
7. The Parties shall provide access to information necessary to perform the tasks entrusted under the plan outputs, including details of the relevant IT system.
8. The parties during the contract period prepare detailed exit plans for individual services and undertake to test them partially or completely during the term of the contract.
9. The entire exit process should end with the signing of a protocol in which one party confirms acquisition of equipment, licenses, software, etc., the other party confirms the deletion of customer data.
10. The parties during the contract period will make an approximate assessment of the costs of the exit plan.

CHAPTER II

1. A PLAN TO ABRUPTLY CEASE PROVIDING THE SERVICE

1. In the event of a sudden and prolonged lack of access to the service due to problems on the part of the service provider (longer than assumed by the SLA), anticipating the restoration of the service within [] hours, a plan should be made at this point.
2. Technical requirements coincide with Chapter I, assuming a return to the cloud service used.
    1) Determining what accounts and what permissions will be used for switching,
    2) Switching the service assumes access to only the selected range of data in the emergency mode. Enter the scope and type of data that will be available and how it will be obtained. Therefore, one assumes the risk of not having one access to all data and launch the functionality of sending current messages,
    3) Documented instructions for System Administrators with prepared service requests (RFCs) for all switching tasks,
    4) In case of problems at the CRITICAL level, the relevant department within the structure is notified The Bank's IT system and the Supplier is launched as part of the purchased support service. At the same time, a problem is recorded, the service of which is carried out as part of a separate problem management process Bank,
    5) If the Bank has no problem management process defined, a dedicated one should be developed instructions, roles and tasks for the service switch coordinator. First of all, it contains such instructions rules for informing users about switching services,
    6) Return to the cloud service is described as above through instructions for administrators and written works.

ISO27001 - CONTROL DESCRIPTION ON THE SUPPLIER'S SIDE

Security ID (Annex A)	Purpose of use	Security	Compatibility from ISO 27001	Description of security implementation	Security testing and auditing	Test rules	Plans of repair (in the absence of compliance or partial compliance)
A.5.1.1.	Policy of information safety	Security A set of information security policies should be developed, approved by management, published and communicated to employees and relevant external parties	Yes	*Example description*	Example description	Self-assessment	
A.5.1.2.	Review of policies of safety and information	Security Information security policies should be reviewed at scheduled intervals or when significant changes occur to ensure that they are still relevant, adequate and effective	Yes			Self-assessment	
A.6.1.1.	Roles and responsibility for safety information	Security Responsibility for information security should be defined and assigned	Yes			Self-assessment	
A.6.1.2.	Separation of duties	Obligations and responsibilities that are in conflict with each other should be separated to limit the opportunity to unauthorized or unintentional modification or abuse of the organs of the organization	Yes			Self-assessment	
A.6.1.3.	Contacts with authorities	Security Appropriate contacts with relevant authorities should be maintained	Yes			Self-assessment	
A.6.1.4.	Contacts with groups of interested specialists	Security Appropriate contacts should be maintained with groups of professionals or other professionals specialist forums and professional associations in the area of security	Yes			Self-assessment	

A.6.1.5.	Security of information in management of project	Security Information security should be included in project management, regardless of type design	Yes			Self-assessment	
A.6.2.1.	Policy on the use of mobile devices	Security A policy should be introduced and the security supporting it to manage the risks arising from the use of mobile devices.	Yes			Self-assessment	
A.6.2.2.	Telecommuting	Security Policy and supporting safeguards should be implemented to protect downloaded information, processed and stored in places where telework is performed	Yes			Self-assessment	
A.7.1.1.	Verification proceedings	Security The history of all job applicants should be verified in accordance with the relevant regulations legal, regulation and ethical principles and in proportion to business requirements, classification of information for which access will be needed and perceived risks	Yes			Self-assessment	
A.7.1.2.	The conditions of employment	Security Agreements with employees and contractors should specify the parties' responsibility in the area of information security	Yes			Self-assessment	
A.7.2.1.	Management responsibility	Security Management should require that all employees and contractors apply information security principles in accordance with the policies and procedures in force in the organization.	Yes			Self-assessment	
A.7.2.2.	Awareness, education and training in the field of safety of information	Security All employees of the organization and, where applicable, contractors, should pass appropriate awareness raising and training, and regularly receive policy updates and procedures related to their job position	Yes			Self-assessment	
A.7.2.3.	Disciplinary proceedings	Protection Disciplinary proceedings against employees who violate information security principles should be conducted on the basis of the rules set and presented to them	Yes			Self-assessment	

A.7.3.1.	End of employment or change in range of duties	Security Identify and present to the employee or contractor which responsibilities and obligations in the field of information security, they will remain valid after termination or change of employment, and then enforce them	Yes			Self-assessment	
A.8.1.1.	Asset inventory	Collateral Identify assets related to information and information processing means and prepare and maintain records of these assets	Yes			Self-assessment	
A.8.1.2.	Ownership of assets	Collateral The assets in the records should be attributed to their owners	Yes			Self-assessment	
A.8.1.3.	Acceptable use of assets	Collateral Identify, document and implement policies for the acceptable use of information and assets related to information and information processing means.	Yes			Self-assessment	
A.8.1.4.	Return of assets	Security All employees and users of external entities, at the end of employment, agreements or arrangements should return all of the organization's assets	Yes			Self-assessment	
A.8.2.1.	Classifying information	Security Information should be classified taking into account legal requirements, values, criticality and sensitivity to unauthorized disclosure or modification	Yes			Self-assessment	
A.8.2.2.	Information tagging	Security An appropriate set of compliant information marking procedures should be developed and implemented with the information classification scheme adopted in the organization	Yes			Self-assessment	
A.8.2.3.	Asset management	Collateral Asset management procedures should be developed and implemented in accordance with the organization's information classification scheme.	Yes			Self-assessment	
A.8.3.1.	Managing removable media	Security The organization should implement procedures for managing removable media in accordance with the classification scheme adopted in the organization	Yes			Self-assessment	

A.8.3.2.	Withdrawing media	Protection Media that will no longer be used should be safely withdrawn according to formal procedures.	Yes			Self-assessment	
A.8.3.3.	Transferring media	Protection Media containing information should be protected against unauthorized access, abuse and loss of integrity during transport.	Yes			Self-assessment	
A.9.1.1.	Access control policy.	Security Access control policy should be established, documented and reviewed in accordance with business and information security requirements.	Yes			Self-assessment	
A.9.1.2.	Access to networks and network services	Security Users should only have access to those networks and network services to which they have received explicit permissions	Yes			Self-assessment	
A.9.2.1.	Registration and deregistration of users	Security A formal registration process should be implemented to allow access rights to be allocated and unregister users	Yes			Self-assessment	
A.9.2.2.	Granting access to users	Security A formal process should be implemented to grant access to users to grant or revoke access to all systems and services to all categories of users.	Yes			Self-assessment	
A.9.2.3.	Rights management of privileged access	Security The allocation and use of privileged access rights should be limited and supervised	Yes			Self-assessment	
A.9.2.4.	Confidential information and credentials management	Assigning confidential credentials should be subject to a formal process management	Yes			Self-assessment	
A.9.2.5.	Review user access rights.	Security Asset owners should review user access rights at regular intervals	Yes			Self-assessment	

A.9.2.6.	Receiving or adjustment of access rights	Security Access rights to information and resources allocated to employees and external users information processing should be received after termination of employment, contract or agreement, or adapt to changes	Yes			Self-assessment	
A.9.3.1.	Use of confidential authenticating information	Security Users should be required to comply with the organization's policies confidential credentials	Yes			Self-assessment	
A.9.4.1.	Restricting access to information	Security Access to information and functions of the application system should be limited in accordance with the access control policy	Yes			Self-assessment	
A.9.4.2.	Procedures of secure logon	Security Where access control policy requires it, access to systems and applications should be controlled by secure login procedure	Yes			Self-assessment	
A.9.4.3.	Password management system	Security Password management systems should be interactive and ensure the selection of good quality passwords	Yes			Self-assessment	
A.9.4.4.	Use of the privileged utilities programs	Security Utilization of utility programs to bypass system security and application, should be subject to restrictions and strict supervision	Yes			Self-assessment	
A.9.4.5.	Access control to source codes programs	Security Access to the source code of programs should be limited	Yes			Self-assessment	
A.10.1.1.	Application policy of cryptographic security	Security A policy to use cryptographic security for protection should be developed and implemented information	Yes			Self-assessment	
A.10.1.2.	Key management	Security A policy should be developed regarding the use, protection and validity of keys cryptographic and implement it at all stages of the key's life cycle	Yes			Self-assessment	

A.11.1.1.	Physical boundary of a secure area	Security Determine the security limits and use them to secure areas containing sensitive or critical information and information processing means	Yes			Self-assessment	
A.11.1.2.	Physical security of entrances	Security Secure zones should be protected by appropriate entry safeguards ensuring access only to authorized persons	Yes			Self-assessment	
A.11.1.3.	Office, rooms and objects security	Security Design and use physical security for offices, rooms and facilities	Yes			Self-assessment	
A.11.1.4.	Protection from external and environmental threats	Security physical and anti-natural disasters should be designed and used attack or accidents	Yes			Self-assessment	
A.11.1.5.	Work in safe areas	Safety Work procedures in safe areas should be designed and applied.	Yes			Self-assessment	
A.11.1.6.	Delivery and loading areas	Security Supervise access points such as delivery and loading areas and others points through which unauthorized persons can enter rooms and, if possible, isolate them them from the means of information processing to prevent unauthorized access	Yes			Self-assessment	
A.11.2.1.	Location and security equipment	Security Equipment should be placed and protected in such a way as to reduce the risks arising from hazards and environmental hazards, and opportunities for unauthorized access	Yes			Self-assessment	
A.11.2.2.	Assistive systems	Protection Equipment should be protected against power failures and other interruptions caused by failures of assistive systems	Yes			Self-assessment	
A.11.2.3.	Cabling security	Protection Power supply and telecommunications cabling, data transfer or supporting information services should be protected against interception, interference or damage	Yes			Self-assessment	

A.11.2.4.	Equipment maintenance	Protection Equipment should be properly maintained to ensure its continuous availability and integrity	Yes			Self-assessment	
A.11.2.5.	Asset carrying out	Security Equipment, information and programs should not be taken outside the organization’s headquarters without obtaining prior authorization	Yes			Self-assessment	
A.11.2.6.	Security of equipment and assets off premises	Security Assets carried out outside the organization’s headquarters should be secured against the occurrence of various risks related to off-site work	Yes			Self-assessment	
A.11.2.7.	Safe disposal or forwarding for reuse	Security Check all equipment for disposal or disposal components containing information media to ensure that all sensitive data and licensed programs have been removed or securely verwritten	Yes			Self-assessment	
A.11.2.8.	Leaving equipment of user without care	Security Users should ensure adequate protection of equipment left unattended	Yes			Self-assessment	
A.11.2.9.	Clean desk and screen policy	Security A clean desk policy for paper documents and portable storage media as well as a clean screen policy for information processing means should be introduced	Yes			Self-assessment	
A.12.1.1.	Evidence of consumables procedures	Security Operating procedures should be documented and made available to all those in need of their users	Yes			Self-assessment	
A.12.1.2.	Change management	Security Monitor and adapt resource usage and anticipate required capacity in the future to ensure proper system performance	Yes			Self-assessment	
A.12.1.3.	Capacity management	Security Monitor and adapt resource usage and anticipate required capacity in the future to ensure proper system performance	Yes			Self-assessment	

A.12.1.4.	Separating environments of development, test and manufacturing	Security Development, testing and production environments should be separated to reduce associated risks with unauthorized access or changes in the production environment	Yes			Self-assessment	
A.12.2.1.	Security against harmful software	Security Detection, prevention and restoration measures to protect should be implemented against malware, combined with the proper awareness of users	Yes			Self-assessment	
A.12.3.1.	Backup copies of information	Security Backup copies of information, software and system images should be regularly performed and tested in accordance with the established backup policy	Yes			Self-assessment	
A.12.4.1.	Event logging	Security Create, store and systematically review event logs that record activities users, exceptions, glitches and information security related incidents	Yes			Self-assessment	
A.12.4.2.	Information protection in event logs	Means for recording events and information in event logs should be protected against manipulation and unauthorized access	Yes			Self-assessment	
A.12.4.3.	Administrators and operators activity recording	Security The actions of administrators and system operators should be recorded and logs must be protected and systematically browse	Yes			Self-assessment	
A.12.4.4.	Clock synchronization	Security Clocks of all relevant information processing systems in an organization or security domain should be synchronized with one standard time source	Yes			Self-assessment	
A.12.5.1.	Installation of software in systems of manufacturing	It is necessary to implement procedures for supervision over software installation in production systems	Yes			Self-assessment	
A.12.6.1.	Management of technical vulnerability	Security Information about the technical vulnerabilities of the information systems used should be immediately acquire, assess and take the organization’s exposure to these vulnerabilities appropriate measures to counter the risks associated with them	Yes			Self-assessment	

A.12.6.2.	Limitations in installing software	Security Establish and implement rules for software installation	Yes			Self-assessment	
A.12.7.1.	Security of information systems audit	Security Audit requirements and verification activities should be carefully planned and agreed production systems to minimize disruption to business processes	Yes			Self-assessment	
A.13.1.1.	Network Security	Network Security should be managed and supervised to protect information in systems and applications	Yes			Self-assessment	
A.13.1.2.	Security of network services	Security Contracts for all in-house or outsourced network services outside, they should contain identified security mechanisms, levels of service and management requirements	Yes			Self-assessment	
A.13.1.3.	Network separation	Security Groups of information services, users and information systems should be separated in the network structure	Yes			Self-assessment	
A.13.2.1.	Information transfer policies and procedures	Security Formal information transfer policies, procedures and safeguards should be implemented to protect information transmitted using all types of communications	Yes			Self-assessment	
A.13.2.2.	Agreement regarding upload of information	Security Agreements should include secure transmission of business information between organization and external entities	Yes			Self-assessment	
1.13.2.3.	Electronic messages	Security Information provided in the form of electronic messages should be properly protected	Yes			Self-assessment	
A.13.2.4.	Confidentiality Agreements	Security Contract requirements should be identified, regularly reviewed and documented on confidentiality towards non-disclosure of information in a way that reflects the needs of information protection organizations	Yes			Self-assessment	
A.14.1.1.	Analysis and specification of requirements of safety information	Security Information security requirements should be included in the requirements for new ones information systems or expansion of existing systems	Yes			Self-assessment	
A.14.1.2.	Securing services of application in public networks	Security Information sent in public networks related to services provided by applications, you should protect against unfair activities, contract disputes and unauthorized use and changes	Yes			Self-assessment	

A.14.1.3.	Protection of application of services transactions	Security Information related to transactions carried out as part of the services provided by applications must be protected to prevent transmission interruption, routing errors, and unauthorized changes in messages, unauthorized disclosure, unauthorized duplication or reproduction	Yes			Self-assessment	
A.14.2.1.	Policy of development work safety	Security Rules for working on software and system development should be established and applied in development work carried out within the organization	Yes			Self-assessment	
A.14.2.2.	Change Control Procedures for Systems	Protection Changes to systems should be monitored during their lifecycle using formal change control procedures	Yes			Self-assessment	
A.14.2.3.	Technical review of application after changes in the production platform	Security After making changes to production platforms, a critical review should be performed business applications or test them to ensure that the changes were not adversely affected impact on the organization's activities or security	Yes			Self-assessment	
A.14.2.4.	Limitations regarding changes in software systems	Security Modifications to software packages should be made with caution and limited to changes necessary and closely supervise all such changes	Yes			Self-assessment	
A.14.2.5.	Design principles of secure systems	Security Establish, document and maintain design principles for secure systems and apply them to all implementation work on information systems	Yes			Self-assessment	
A.14.2.6.	Safe development environment	Security Organizations should establish and properly protect safe development environments intended for systems development and integration works covering the whole cycle developmental processes	Yes			Self-assessment	
A.14.2.7.	Development works commissioned to external entities	Security The organization should supervise and monitor development work on commissioned systems external entities	Yes			Self-assessment	
A.14.2.8.	Testing safety systems	Security Safety functions should be tested during development works	Yes			Self-assessment	

A.14.2.9.	System acceptance tests	Security For new information systems, their modernization and new versions of systems, acceptance test programs and criteria associated with them should be established	Yes			Self-assessment	
A.14.3.1.	Protection of test data	Protection Test data should be carefully selected, protected and supervised	Yes			Self-assessment	
A.15.1.1.	Policy of safety of information in relationships with suppliers	Security You need to agree with the supplier and document the purpose of information security requirements reducing the risks associated with the provider's access to the organization's assets	Yes			Self-assessment	
A.15.1.2.	Inclusion of safety in agreements with suppliers	Security All relevant information security requirements should be established and agreed with any provider that can access, process, store, transfer or provide elements of the ICT infrastructure for processing belonging information to organization	Yes			Self-assessment	
A.15.1.3.	Supply chain of information and telecommunications technology	Agreements with suppliers should include requirements regarding risks in information security related to information technology services and telecommunications and the product supply chain	Yes			Self-assessment	
A.15.2.1.	Monitoring and service review provided by providers	Security Organizations should regularly monitor, review and audit external service delivery	Yes			Self-assessment	
A.15.2.2.	Management changes in services provided by providers	Security Manage changes in the provision of services by suppliers, including maintenance and improving existing information security policies, procedures and safeguards, taking into account the criticality of the information, systems and business processes they concern and reassessing the risk	Yes			Self-assessment	
A.16.1.1.	Responsibility and procedures	Security Provision should be made for management responsibility and procedures to ensure prompt, effective and organized response to information security incidents	Yes			Self-assessment	
A.16.1.2.	Event reporting related with security information	Security Information security incidents should be reported through appropriate channels management as soon as possible	Yes			Self-assessment	

A.16.1.3.	Reporting weaknesses related with security information	Security Employees and contractors using service systems should be required information organizations to record and report any observed or suspected weaknesses related to information security in systems or services	Yes			Self-assessment	
A.16.1.4.	Assessment and making decision in the matter related events with security information	Security Information security incidents should be assessed and a decision taken classifying them as incidents related to information security	Yes			Self-assessment	
A.16.1.5.	Responding to related incidents with security information	Security The response to information security incidents should be consistent with documented procedures	Yes			Self-assessment	
A.16.1.6.	Drawing conclusions from incidents related with security information	Security Knowledge acquired during analysis and resolution of security incidents information should be used to reduce the likelihood of occurrence or effects future incidents	Yes			Self-assessment	
A.16.1.7.	Collection of evidence material	Security The organization should define and apply procedures for identification, collection and acquisition and recording information that may constitute evidence	Yes			Self-assessment	
A.17.1.1.	Continuity planning safety information	Security The organization should specify information security and continuity requirements information security management in adverse situations, e.g. during a crisis or disaster	Yes			Self-assessment	
A.17.1.2.	Implementing continuity in safety information	Security The organization should establish, document, implement and maintain processes and procedures and safeguards to ensure the required level of continuity at a disadvantage information security	Yes			Self-assessment	
A.17.1.3.	Verify overview and continuity assessment safety information	Security The organization should verify established and implemented security continuity safeguards information at regular intervals to ensure that it is current and effective in adverse situations.	Yes			Self-assessment	
A.17.2.1.	Availability of funds processing information	Security Information processing measures should be implemented with sufficient excess to be met accessibility requirements	Yes			Self-assessment	

A.18.1.1.	Term applicable legal and contractual requirements	Security All relevant legal, regulatory, contractual requirements and the organization's approach to them compliance should be identified, documented and updated for each system information and the whole organization	Yes			Self-assessment	
A.18.1.2.	Intellectual property rights	Security Appropriate procedures should be in place to ensure compliance with legal, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software	Yes			Self-assessment	
A.18.1.3.	Record protection	Security Records should be protected against loss, destruction, falsification and unauthorized access and unauthorized publication, pursuant to legal, regulatory and contractual requirements and business	Yes			Self-assessment	
A.18.1.4.	Privacy and data protection identifying a person	Security The privacy and protection of personally identifiable information should be provided as appropriate laws and regulations	Yes			Self-assessment	
A.18.1.5.	Regulations regarding cryptographic security	Security Cryptographic security should be used in accordance with relevant agreements and regulations	Yes			Self-assessment	
A.18.2.1.	Independent review of safety information	Security The organization's approach to information security management and its implementation (i.e. objectives security application, security policies, processes and procedures information) hould be independently reviewed at scheduled intervals or then, when significant changes occur	Yes			Self-assessment	
A.18.2.2.	Compliance with policies of safety and standards	Security Managers should regularly review the compliance of information processing and procedures with relevant security policies, standards and other requirements security, to the extent of the responsibility assigned to them	Yes			Self-assessment	
A.18.2.3.	Checking technical compliance	Security You should regularly review information systems to check their compliance with information security policies and standards in force in the organization	Yes			Self-assessment	

SERVICE IMPLEMENTATION STEPS OF DATA PROCESSING IN CLOUD COMPUTING IN BANKING

INTRODUCTION

This document describes the steps for implementing the cloud computing service. The process describes the implementation steps assuming that the Cloud Computing Service is a special outsourced cloud computing service. The implementation process for a non-outsourcing specific cloud computing is outside the scope of this document.The described steps supplement the standard processes functioning at the Banks with the necessary actions being the implementation of the requirements set out in the Communication of the Polish Financial Supervision Authority regarding processing of information in public cloud computing by supervised entities or hybrid ("Cloud Message").

1. IDENTIFY YOUR BUSINESS NEEDS

1. At this stage, the business need is identified and documented in accordance with the processes in force at the Bank.
2. A formal "project" or other initiative is being opened that allows the allocation of work related to the steps described below.
3. The units responsible for architecture, technology and cybersecurity determine the legitimacy of further analysis of this need in terms of the possibility of implementation in the cloud.

PRODUCTS

1. Description of business requirements.
2. The formal "Project / charter" opening the project.

2. INITIAL ASSESSMENT IN TERMS OF FEASIBILITY NEEDS IN THE CLOUD SERVICE

1. At this stage, a "pre-assessment" of the need for cloud computing is conducted.
   1) comparison of solutions in the cloud service vs. on-premise - preliminary assessment of the implementation of requirements and costs, including the analysis of potential cloud service providers;
   2) architecture, integration, target configuration - compliance with the Bank’s target architecture;
   3) initial PoC solutions if it is planned to use technologies completely new for the Bank;
   4) data inventory and classification, service relevance classification - depending on the results, a preliminary decision is made in terms of supervised outsourcing;
   5) examining the possibility of acquiring competences for the cloud and on-premise service;
   6) compliance with the Bank’s strategy;
   7) compliance with internal regulations.

PRODUCTS

1. Preliminary feasibility analysis for a cloud service vs. on-premise.
2. Service implementation steps cloud data processing computing in banking

3. DECISION POINT / DECISION ON THE ADMISSIBILITY OF IMPLEMENTING A CLOUD SOLUTION

1. At this stage a decision is made about further processing of the need; possible scenarios:
   1) Lack of possibilities / legitimacy of using a cloud solution;
   2) Acceptable cloud solution - supervised outsourcing required;
   3) Acceptable cloud solution - no supervised outsourcing required.
2. Further steps will be described only for scenario 2.

PRODUCTS

1. Documented decision on the possibility of implementing a cloud solution (persons authorized in accordance with with the Bank's organizational regulations).

4. DEVELOPING REQUIREMENTS - SUPERVISED OUTSOURCING

1. At this stage, a set of business, formal, cybersecurity and other requirements is created. The requirements are determined based on the requirements of the Bank's internal regulations and the Regulator's Cloud Message.
2. When creating requirements, consider the following:
   1) Are there cloud solutions on the market with references in the financial industry?
   2) Can potential bidders provide CPD within the EEA?
   3) If the Bank is a key service operator (in accordance with the Act on the National Cybersecurity System) - can potential bidders provide CPD in Poland?
   4) Is it possible to ensure appropriate competences on the Bank's side? Are additional training required for employees? What are the market opportunities? What costs should be taken into account?
   5) Has compliance with internal standards and regulations been confirmed (VII.4.1 point d)?
   6) Will the cloud be able to provide the required capacity and performance?
   7) Rules for providing information on incidents of information security breaches, understood as confidentiality, integrity and availability of processed information and resources, with particular emphasis on Confidential Information within the meaning of the confidentiality agreement concluded by the Parties,
   8) Rules for secure and permanent destruction of data in the cloud,
   9) Monitoring the parameters of cloud services used by the Bank,
   10) Rules for terminating cooperation with a cloud service provider,
   11) Performing obligations under the Agreement, within the agreed scope and time limit, with due diligence, taking into account the professional nature of the business and the current state of knowledge in the field of banking and information technologies.
3. Requirements resulting from the Cloud Message are defined in the requirements matrix being a part Cloud Standard.

PRODUCTS

1. Approved requirements document.

5. DEVELOPMENT AND DISTRIBUTION OF THE REQUEST FOR QUOTATION

1. Before starting the processing of queries, it should be verified whether there are addressing Agreements in the Bank requirements from point 4 in terms of the possibilities of their use.
2. At this stage, the RFP document is developed and sent to cloud service providers. Answers to inquiries should contain information on meeting the requirements set out in point 4 above.

PRODUCTS

1. Inquiry.
2. Answers to your inquiry.

6. RISK ASSESSMENT RELATED TO THE CLOUD SERVICE

1. Based on suppliers' replies, in particular responses to the requirements arising from the Communication Cloud-based requirements defined in the matrix, a risk assessment is carried out for each of the offered solutions. The requirements matrix also defines the minimum requirements that must be met to implement the cloud service. For other requirements, it is possible to propose temporary solutions or so-called compensating controls ensuring an acceptable level of risk.
2. Offers that do not meet the minimum requirements should be rejected.
3. The result of risk analysis, including functional requirements, financial aspects, etc., is the basis to decide on the choice of cloud service provider for the project.

PRODUCTS

1. Risk assessment (for individual offers that have not been rejected).
2. A proposed plan for dealing with identified risks (compensating controls etc.).

7. EVALUATION OF OFFERS AND ACCEPTANCE OF THE OFFER

1. At this stage, next to business issues, the offer is selected and the final risk assessment for the selected offer is made.
2. Arrangements are also made with the Supplier regarding risk management measures and developed there is a final plan for dealing with identified risks.

PRODUCTS

1. Selection of the offer with justification.
2. Updated risk assessment (for the selected offer).
3. A plan of dealing with the identified risks agreed with the Supplier.

8. SIGNING THE CONTRACT

1. Signing the contract in accordance with the requirements of the Cloud Message. Addressing identified risks by introducing contractual and formal provisions, recovery plans etc.

PRODUCTS

1. Signed contract (as per representation). It is recommended that the decision to enter the cloud technology was preceded by documented consent of the Management Board.
2. Updating the status of the plan for dealing with identified risks.

9. PRE-PRODUCTION IMPLEMENTATION - SERVICE CONFIGURATION

1. As part of the implementation, key milestones resulting from the Cloud Communication are implemented, especially:
   1) service documentation;
   2) adaptation of procedures;
   3) acquiring competences;
   4) developing a cloud computing plan;
   5) developing an exit plan;

6) modification of BCP / DRP plans;
7) implementation of safeguards and monitoring mechanisms (including integration with SIEM etc.);
8) tests (functional, acceptance, security, performance, etc.).

2. At this stage, production data has not yet been migrated.
3. After the implementation is completed, the status of recovery plans and risk assessment is updated to confirmation that the previously identified risks have been addressed as intended.
4. The date of data migration and production launch is also specified.

PRODUCTS

1. Documentation of the service and control mechanisms.
2. Updating the status of the plan for dealing with identified risks.
3. Cloud computing plan.
4. Exit plan for cloud services.
5. Updated DRP / BCP plans.
6. Test results and their formal acceptance.
7. Migration and production implementation plan.
8. Updated risk assessment (existing update).
9. Documentation of training / acquisition of competences for users and other key roles.

10. NOTIFICATION TO THE POLISH FINANCIAL SUPERVISION AUTHORITY

1. Report to the PFSA Office in accordance with the requirements of the Cloud Message.

PRODUCTS

1. Notification to the KNF Office.

11. MIGRATION OF PRODUCTION DATA TO THE CLOUD SERVICE

1. After reporting to the PFSA Office, it is possible to start data processing at the Cloud Service, and thus to start the migration of production data. Acceptance tests are required after data migration.

PRODUCTS

1. Data migration documentation.
2. Test results confirming data quality, encryption security in accordance with the communication, procedures Disaster Recovery etc.

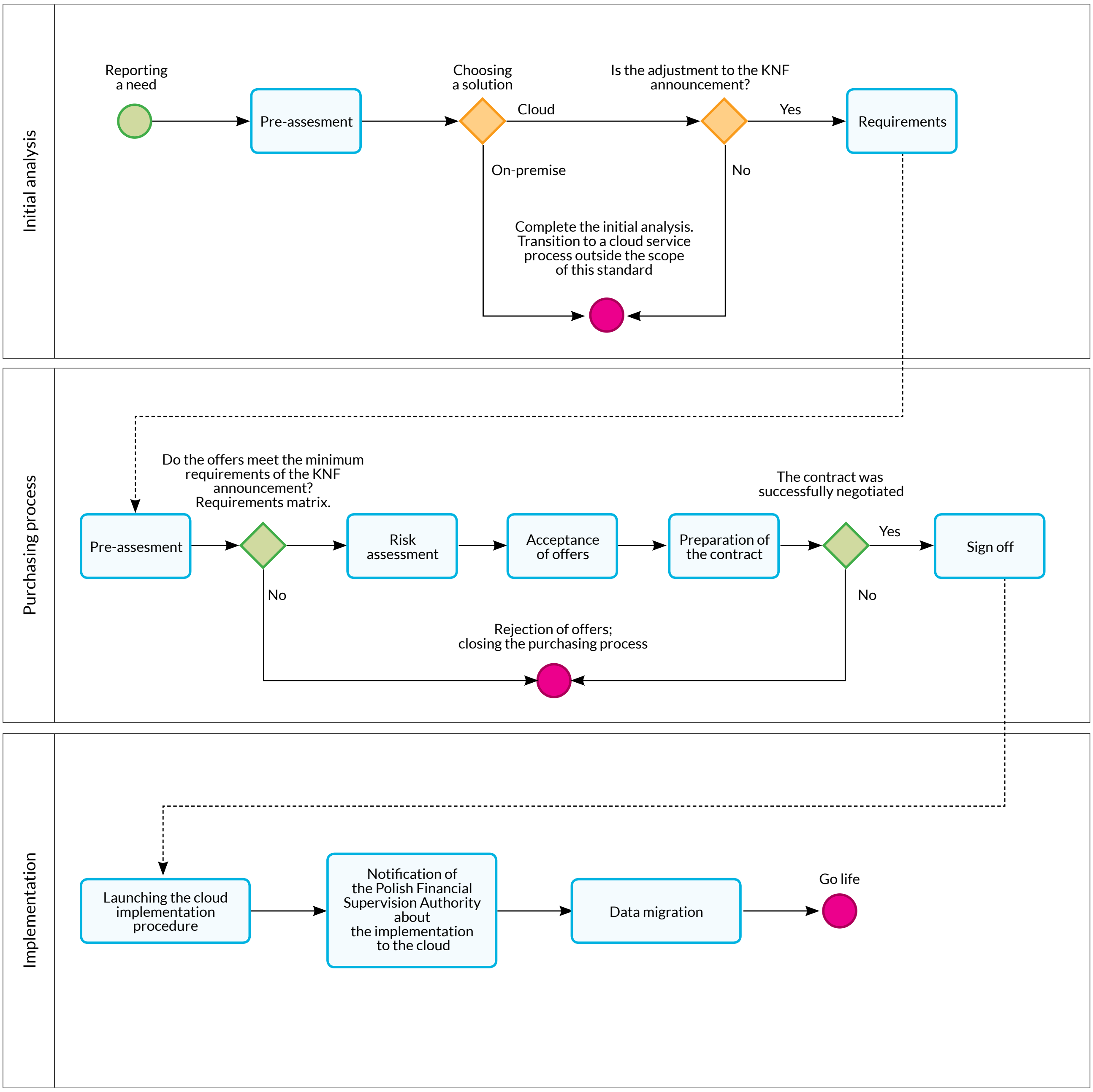
12. PRODUCTION LAUNCH

1. After completing and testing data migration, a formal production launch is possible, preceded by a formal decision in this respect and communication to users and other stakeholders.

PRODUCTS

1. The formal decision to start the service.
2. Internal communication at the Bank.

CLOUD IMPLEMENTATION SCHEME


Initial analysis
Reporting a need
Pre-assesment
Choosing a solution
Cloud
On-premise
Is the adjustment to the KNF announcement?
Yes
No
Requirements
Complete the initial analysis. Transition to a cloud service process outside the scope of this standard
Purchasing process
Pre-assesment
Do the offers meet the minimum requirements of the KNF announcement? Requirements matrix.
No
Risk assessment
Acceptance of offers
Preparation of the contract
The contract was successfully negotiated
Yes
No
Sign off
Rejection of offers; closing the purchasing process
Implementation
Launching the cloud implementation procedure
Notification of the Polish Financial Supervision Authority about the implementation to the cloud
Data migration
Go life

REQUIREMENTS FOR SUPPLIERS

Index	Requirement	Description of requirement	Supplier-side requirements	Products (refer to requirements on the supplier's side)
V.1-5	Guidelines to classification and evaluation information	Supervised entity carried in documented classification process and assessment of information under angle of admissibility their processing in the cloud computing	1. The supplier should specify CPD locations in which Bank information is processed (country, region) 2. Any area changes data processing require prior consent of the Bank	1. Documentation in the field CPD location and area data processing (information about what services are provided in individual locations) 2. The process of informing about the change data processing area
VI.1-6	Guidelines to estimation risks	Supervised entity carried in documented comprehensive process risk estimation	The supplier should provide The following information for the bank: 1. Information about dispersion geographical processed information 2. Information on access rules to information processed by employees and co-workers (e.g. subcontractors) service providers cloud 3. access to processed information, guaranteed by jurisdiction of the country in which it takes place processing in particular reference to the situation catalog (or entities) where possible is requesting information or access to them without explicit permission entity 4. Information about mechanisms isolation of used resources to provide cloud services computational, including information about security incidents related to the violation isolation mechanisms 5. Information on the possibility of migration services / data to other providers cloud for mitigation attachment to one supplier cloud computing services 6. Information on interfaces service managers, which are shared by cloud service providers and theirs vulnerabilities	1. See V.1-5. 2. See VII.3.2. 3. Legal opinions in the field of non-contractual options access to processed information guaranteed by jurisdiction of the country in which data processing takes place 4. See VII.3.2. 5. See VII.3.2. 6. See VII.3.2. 7. Rules for requesting and entering requested changes 8. Supplier control rules, especially: a) rules on access to documentation certification b) rules on access to results security audits and tests c) principles of conducting control direct and indirect 9. Target SLAs and rules quality supervision provided services 10. See VII.3.2. 11. Control mechanisms users and devices at access to the cloud service 12. Rules for changing the terms of service 13. List of subcontractors together with the scope provided by them tasks and info on bank data access.

			8. Information about the possibilities controlling the service provider cloud computing and its subcontractors, including direct verification physical, technical and organizational mechanisms security and control of performance cloud computing services 9. Information on the possibilities controlling the quality of cloud services computing 10. Division information responsibility for processed security information between the supplier cloud computing services and a supervised entity 11. Access control options and access devices end users 12. Rules for changing conditions agreement 13. Information on used sub-suppliers and scope their services and information on their access to data.	
VII.3.1	Minimal requirements for processing information in cloud computing	Assurance of competences	1. Determination of the required competence when exercising from the service, specify paths training and certification	1. List of required and recommended training / certificates at using the service for individual roles and list recommended by role provider resulting from the division responsibility between bank and supplier
VII.3.2	Minimal requirements for processing information in cloud computing	Segregation of duties and consequences application	1. Clear definition of the division responsibility for processed security information when using the service. 2. Enabling the Bank understanding the consequences use of specific architecture cloud computing environments and rules for its configuration	1. Defining documentation division of responsibility for information Safety between the Bank and the supplier services 2. Documentation setting out the rules service configuration. 2.1. Service architecture 2.2. Key documentation service security issues, especially: a) description and scope of processed information and information if used, about their pseudonymization or anonymization b) encryption method information and place and / or key storage method encryptors, both at rest, as well as in transit

				c) confirmation of use encryption algorithms no are widely considered to be discredited d) information on who has access to processed information and how this access is granted, managed, received and controlled e) dedicated documentation and / or recommended by the supplier configuration settings increasing safety services rendered, in particular regarding processed encryption information f) detailed and up-to-date instructions service configuration and validation methods their configuration and operation, in particular regarding processed encryption information g) description of login mechanisms and the ability to transfer logs to SIEM on the Bank's side h) information on mechanisms isolation of used resources to provide cloud services computing i) documentation of the guidelines, model configurations, descriptions rules etc. which in unambiguous the way they define separation processing and point to validation methods configuration j) interface information service managers, which are shared by cloud service providers and their vulnerabilities (results susceptibility testing or testing safety) k) supporting documentation native launch of a new one environment and / or services separated from other topics, with "secure-by-default" settings 2.3. Description of access mechanisms remote provider included the following requirements: a) authentication two-component with access remote to the environment the cloud

				b) remote access option from secure network locations c) the ability to record sessions administrative and inspection by Bank staff in session recordings
VII.4	Minimal requirements for processing information in cloud computing	Contract with the supplier cloud services computing	1. Signing the outsourcing contract in accordance with the Banking Law 2. Including requirements in the contract specified in point VII.4.1 cloud message 3. Information on applicable law for the contract (including the court with jurisdiction and dispute resolution rules)	1-2. Confirmation of consent for conclusion of a compatible contract with contractual clauses attached 3. Information on applicable law for the contract (including the court with jurisdiction and dispute resolution rules) 3.1 In the event of submission of the contract third country law analysis legal regarding options effective exercise contract provisions, all requirements of Polish law on the Bank and supervisory authority guidelines in terms of the message
VII.5	Minimal requirements for processing information in cloud computing	Processing plan information in the cloud computational (5.1)	1. Architecture information and configuration service constituting contribution to the development of the plan information processing in the cloud	See VII.3.2.
VII.6.1-2,5	Requirements for suppliers cloud services computing	Supplier compliance with standards	In terms of rendered cloud service provider computing meets total compliance requirements its operation with standards or their equivalents in Polish or European system standardization, unless the entity supervised accepts (based on estimation results risk) no need meet this requirement either parts of it. 1. PN-ISO / IEC ISO 20000 regarding IT service management 2. PN-EN ISO / IEC 27001 concerning security management information 3. PN-EN ISO 22301 concerning business continuity management 4. ISO / IEC 27017 regarding information security in the cloud 5. ISO / IEC 27018 regarding good hedging practices personal data in the cloud computing	Confirmation Documentation compliance with standards (if applicable): 1. PN-ISO / IEC ISO 20000 regarding IT service management 2. PN-EN ISO / IEC 27001 concerning security management information 3. PN-EN ISO 22301 concerning business continuity management 4. ISO / IEC 27017 regarding information security in the cloud 5. ISO / IEC 27018 regarding good hedging practices personal data in the cloud computing 6. PN-EN 50600 minimum class 3 or ANSI / TIA-942 minimum Tier III. Acceptable documents: - Confirmation certificates compliance with standards - Supplier's statement on meeting the requirements of the standards

			6. CPD of cloud service provider computing meets the requirements PN-EN 50600 minimum class 3 or ANSI / TIA-942 minimum Tier III, or other normative relevant and universally recognized for CPD assessment, however The bank can accept (in justified cases and on risk assessment basis) none meet part of the requirements	
VII.6.3	Requirements for suppliers of cloud computing services	Location of the CPD	1. It is recommended that the CPD be located in the EEA (if this is justified from a perspective cost, quality, risk etc.) 2. Banks that are service operators key should prefer CPD in Poland	1. See V.1-4
VII.6.4	Requirements for suppliers cloud services computing	Information Protection and access control	Security requirements information: 1. Default no access policy to processed information supervised entity 2. No administrative account or user on machines virtual entity supervised and / or other started services 3. The ‚minimum necessary' principle for service authorization broadcast only in a situation of necessity activities required by supervised entity and for their duration, precedence is the entity's order supervised and the whole process service and performance is provided logged. Applicable to this scope of service procedures can be additionally confirmed appropriate certificate (e.g. SOC 2 Type 2) published by independent certification body accredited in European accreditation system 4. Providing guidelines, model configurations, descriptions rules etc. which in unambiguous the way they define separation processing and point to validation methods configuration	Confirmation of compliance with the requirements in the field of information protection through a description of mechanisms or indication of contractual provisions / procedural assurances the following functionality: 1. Default no access policy to information processed by provider 2. No administrative account or user on machines virtual entity supervised and / or other started services 3. The ‚minimum necessary' principle for service authorization broadcast only in a situation of necessity activities required by supervised entity and for their duration, precedence is the entity's order supervised and the whole process service and performance is provided logged. Applicable to this scope of service procedures can be additionally confirmed appropriate certificate (e.g. SOC 2 Type 2) published by independent certification body accredited in European accreditation system

VII.7	Requirements for suppliers of cloud computing services	Cryptography	Information in the cloud computing must be encrypted. Requirements: 1. Detailed delivery and current configuration instructions services and verification methods the correctness of their configuration and actions, in particular in the field of encryption processed information 2. Using dedicated and / or recommended by the supplier configuration settings increasing safety services rendered, in particular regarding processed encryption information 3. Encryption both "at rest", and "in transit" information legally protected processed in the cloud 4. Information is encrypted generated keys and / or delivered and managed by a supervised entity 5. Encryption algorithms used are not generally considered to be discredited 6. Where with estimation risk arises necessity maintenance and management encryption keys at hardware usage solutions (HSM) then HSM can be provided by the service provider cloud-based, taking into account this element in estimation risk. HSM should meet FIPS 140-2 minimum requirements Level 2 or equivalent 7. Key management process encryptors should take into account storage under own copy infrastructure encryption keys that have been generated or are managed by the service provider cloud computing, unless risk assessment results justified lack of such a need	1-3 See VII.3.2. 4. Can encrypt with keys generated and / or delivered and managed by the entity supervised, technical description solutions 5. See VII.3.2. 6. Can be used own HSM or HSM from suppliers - technical description solutions; confirmation suppliers that HSM meets FIPS 140-2 Level 2 requirements or equivalent 7. Where the keys have been generated or are managed by the service provider cloud computing, an option storage under own key copy infrastructure encrypting Bank

VII.8	Monitoring environment processing information in cloud computing services	Event logging	The provider provides mechanisms event logging and access Log bank: 1. Logs can be forwarded to the Bank, in particular to SIEM. 2. Logs are secured by against unauthorized access, modification or deleted.	See VII.3.2
VII.8.4	Monitoring environment processing information in cloud computing services	Remote Access to the cloud environment	Remote access to the environment the cloud: 1. It is possible only for authorized personnel of the supplier 2. Requires the use of MFA. 3. Is initiated from specific, secure network locations 4. It is implemented under supervision Bank (e.g. by recording session)	See VII.3.2.

Polish Bank Association
ul. Kruczkowskiego 8
00-380 Warsaw
www.zbp.pl