

SUPERVISION OF OUTSOURCING OF DIGITAL SERVICES BY BANKS



CONTENTS

1	INTRODUCTION	3
2	REGIONAL OVERVIEW OF THE OUTSOURCING OF BANKING ACTIVITIES AND ITS REGULATION AND SUPERVISION	4
3	CASE STUDY: THE MAIN CHALLENGES ARISING FROM THE OUTSOURCING OF BANKING ACTIVITIES IN THE REPUBLIC OF ARMENIA	9
4	OUTSOURCING OF FINANCIAL SERVICES: INTERNATIONAL PRACTICES	14
5	CONCLUSION	20
6	ANNEX 1: NOTIFICATIONS VS APPROVALS	21
7	ANNEX 2: INDIRECT SUPERVISION OF THIRD-PARTY SERVICE PROVIDERS	24
8	ANNEX 3: QUESTIONNAIRE ON OUTSOURCING	25
9	ANNEX 4: SUMMARY OF RESPONSES	27

ACKNOWLEDGMENTS

This case study is a knowledge product of AFI's Eastern Europe and Central Asia Policy Initiative (ECAPI) and its members.

Authors and contributors:

AFI is grateful to the task group experts from Central Bank of Armenia: Mariam Yeghiazaryan (lead author), Asya Bekyan, Armine Karapetyan and Vahe Petrosyan, and from The Central Bank of the Russian Federation: Nadezhda Prasolova and Ekaterina Seredkina.

Jaheed Parvez (Technical Specialist) and Eliko Boletawa (Head, Policy Programs and Regional Initiatives) from the AFI Management Unit have contributed to the development of the case study.

We would like to thank AFI member institutions, partners and donors for generously contributing to development of this publication.

1. INTRODUCTION

Twenty-first century banking is a sea change from the banking business as we used to know it. Particularly in addition to classic banking (attracting deposits and granting loans) banks started to offer broader spectrum of financial services to their clients in order to be more competitive and attractive for customers. At the same time, targeting higher efficiency and better quality for their services, banks began to delegate some functions to third-party professionals, who are more experienced and have more adequate resources to develop or deliver specific products or services.

To keep up with FinTech start-ups and innovations in DFS, banks have begun to deploy IT solutions in their internal processes, as well as in product design. As they currently lack advanced in-house expertise to develop the software, technologies and networks to offer DFS products, banks have outsourced most of these activities to specialist third-party service providers. This practice is widespread among banks worldwide for its benefits associated with cost and time savings, besides allowing banks to focus on maximizing their “core competencies”.

However, as banks become increasingly dependent on third-party service providers, this outsourcing practice raises concerns about the overall integrity of the banking business and the sharing of customer data with third-party contractors. The latter especially creates additional risks for customer data protection and the smooth performance of banking activities by bringing new actors and new relationships into the banking industry.

Previously, central banks and supervisory authorities granted licenses to banks and non-bank financial institutions to perform special financial activities that were regulated or supervised to protect depositors and other investors. However, with the development of outsourcing activities, regulators and supervisory authorities must now confront the problem of how to regulate or supervise third-party service providers that are unlicensed but are outsourced by licensed

banks and non-bank financial institutions to perform financial activities because these unlicensed third-party providers do not come under their direct purview.

Notably, third-party outsourcing by banks creates information gaps and introduces data/information access risks for supervisors that supervisory authorities must be cognizant of. Thus, supervisory authorities would need to update their technical and market expertise in order to be able to identify and evaluate the risks that arise when licensed banks outsource their activities to third-party service providers. As the trend for outsourcing becomes widespread, there is a need to explore new supervisory tools and risk-mitigation methods to address their risks.

This paper looks at issues that arise from the outsourcing of banking activities in the Eastern Europe and Central Asia (EECA) region and outlines their possible solutions. It illustrates how these issues arise with a case study of the outsourcing landscape for financial institutions in Armenia. It provides a summary of the results of a survey conducted among participating EECA jurisdictions, which illustrates the main features and differences of approach taken by the jurisdictions to regulate outsourcing risks. It then briefly surveys how developed economies regulate the outsourcing of banking activities and makes some tentative recommendations.

2. REGIONAL OVERVIEW OF THE OUTSOURCING OF BANKING ACTIVITIES AND ITS REGULATION AND SUPERVISION

In order to understand the overall context of outsourcing in the Eastern Europe and Central Asia (EECA) region and its related issues, a survey of EECA jurisdictions was conducted. (See, Appendix 3 for the questionnaire and Appendix 4 for the responses.)

While Mongolia has no specific regulations for outsourcing activities, the following four EECA countries participated in the survey:

- > Armenia
- > Belarus
- > Russia
- > Uzbekistan

2.1 OUTSOURCING OF BANKING ACTIVITIES TO THIRD PARTIES

Of the four jurisdictions that participated in the survey, Armenia, Belarus and Russia allow banks to outsource their activities to third parties, while Uzbekistan is in the process of adopting a draft law on “Banks and Banking Activities” which also allows for banks to outsource their activities to third parties. The following is the list of activities banks are allowed to outsource in the four jurisdictions:

Activities	Armenia	Belarus	Russia	Uzbekistan
Internal auditing	✓		✓	
Accounting	✓			✓
Compliance	✓		✓	
IT systems	✓	✓	✓	✓
Know-your-customer (KYC) processes	✓	✓	✓	✓
Taking deposits	✓	✓		
Lending	✓	✓		✓
Risk management	✓		✓	

Of all the activities allowed to be outsourced by banks in the four jurisdictions, KYC and IT systems are permitted by all four.

In Russia, a “credit institution” may engage a bank payment agent for the following functions:

- > Accepting and issuing cash funds from and to customers (including using payment terminals and ATMs)
- > Providing electronic payment facilities to customers
- > For KYC processes in accordance with Russian anti-money laundering legislation, perform fund transfers without opening bank accounts, including electronic money transfers, or to provide an electronic means of payment to individual customers
- > A credit institution may also engage a payment aggregator to accept electronic means of payment and for electronic money transfers (mostly via internet)

2.1.1 DEFINITION OF OUTSOURCING

Outsourcing has been broadly defined in Belarus, Russia¹ and Uzbekistan, and these definitions are generally comparable with one another. Although there is no specific definition of outsourcing in Armenia, the law on “Banks and Banking”² allows banks to outsource their core and ancillary activities fully or partially for a specified or indefinite term to a legal third-party entity. Russia and Uzbekistan distinguish between “Outsourcing” and “Purchase of Services”. With regard to the definition of “Purchase of Services”, only Russia among the four countries in the survey defines the term.³

2.1.2 THIRD-PARTY SERVICE PROVIDERS THAT QUALIFY FOR A CONTRACT FOR OUTSOURCED BANKING ACTIVITIES

The criteria for a third-party service provider (TPP) to qualify for a contract for outsourced banking activities is generally similar across all the four jurisdictions. However, there are differences in terms of the legal status of the TPP and of the activities it can be contracted by the bank to perform.

- > In Armenia and Uzbekistan, banking activities may be outsourced to any TPP that is a legal entity. However, banking activities that require a specific license or special permit may only be outsourced to a TPP with the relevant license or permit.

1 The Bank of Russia Standard STO BR IBBS-1.4-2018 on informational security in outsourcing - <http://d-russia.ru/wp-content/uploads/2018/03/ib-outsourcing-st-14-18.pdf>

2 <https://www.cba.am/EN/lalaws/banking.pdf>

3 Federal Law No. 223-FZ of July 18, 2011, “On the purchase of goods, works, services by certain types of legal entities”.

- > In Belarus, banking activities may be outsourced to any TPP that is a legal entity; or is licensed and supervised by the supervisory authority.
- > In Russia, banking activities may be outsourced to any TPP that is a legal entity or a natural entity; or is licensed and supervised by the supervisory authority.

2.1.3 AUTHORIZATION FOR THE OUTSOURCING OF BANKING ACTIVITIES

In Armenia and Uzbekistan, banks must obtain the prior consent of the supervisory authority to outsource banking activities to a third party.

In Belarus, banks are required to disclose to the supervisory authority which of their banking activities and operations are outsourced. Also, a register of outsourcing companies is maintained.

In Russia, outsourcing procedures differ according to the type of outsourced activities; the Central Bank of the Russian Federation (Bank of Russia) recommends organizations of the Russian banking system (banks and non-bank financial institutions) to notify it of any outsourcing plans but does not make it mandatory for them to do so.⁴ However, any outsourcing of internal controls must be reported within three days of a decision being taken to do so.⁵

2.1.4 AUTHORITY FOR ON-SITE INSPECTIONS AND SUPERVISION OF THIRD-PARTY CONTRACTORS

In Armenia, Uzbekistan and Belarus, supervisory authorities have the power to inspect outsourced banking activities.

In Russia, the procedure for on-site inspection and off-site supervision depends on the type of outsourcing. While banks and non-bank financial institutions are responsible for the control of their agents, the Bank of Russia supervises how they exercise such control.⁶ The Bank of Russia is mandated to conduct inspections of “credit institutions” and “banking groups”, including the inspection of a credit institution from the same banking group.⁷

4 Standard STO BR IBBS-1.4-2018

5 Regulation No. № 242-P of December 16, 2003, “On organizing internal controls in credit institutions and banking groups”: a credit organization shall send a written notice to the Bank of Russia within three days from the date of taking a decision on significant changes in the IAS, ICS and RMS (including outsourcing services).

6 Federal Law No. 161-FZ of June 27, 2011 “On the National Payment System (NPS law)”

7 Federal Law No. 86-FZ of July 10, 2002



2.1.5 INTRAGROUP OUTSOURCING

Intragroup outsourcing occurs when a bank or non-bank financial institution enters into an outsourcing contract with a party from the same banking or financial group. In Armenia, Belarus and Uzbekistan, intragroup outsourcing is subject to the same regulatory and supervisory requirements as for conventional outsourcing. In Russia, there are specific regulations for supervising banking groups and banking holdings where intragroup outsourcing is concerned.

2.1.6 REQUIREMENTS OR PROCEDURES FOR THE SHARING OF PERSONAL DATA WITH THIRD PARTIES

The sharing of personal data is subject to regulation in Armenia, Uzbekistan and Russia. In Belarus, the sharing of personal data by a bank with a third party for the purpose of outsourcing its activities is not subject to regulation but is subject to the following basic principles:

- > The confidentiality of the personal data is secured
- > The mode of data transfer is secured
- > Personal data are considered confidential customer information and are protected under banking secrecy laws
- > The sharing of personal data must be disclosed to the customer, whose written consent must be obtained for this purpose
- > The disclosure should contain details of what information will be shared, a list of parties with which such information will be shared, the purposes for which the information is being shared, and the period during which the information can be shared with third parties

In **Armenia**, the sharing of personal data is regulated under the Law of the Republic of Armenia on “Protection of personal data” (adopted on 18 May 2015).⁸

In **Uzbekistan**, personal data may be shared only with a third party that has special permission to deal with confidential personal information.

In **Russia**, the processing of personal data can only be done with the consent of their owners.⁹ In cases provided for under federal law, the processing of personal data shall be carried out only with written consent of their owners. This consent can be in the form of an electronic document signed using an electronic signature.

2.1.7 GUIDELINES FOR THE SUPERVISION OF CONTRACTS FOR OUTSOURCED BANKING ACTIVITIES

The outsourcing of banking activities must be formalized in a legally binding contract between the bank and the third party provider in Armenia, Belarus and Russia. Of the three jurisdictions, only Belarus has specific guidelines for the supervision of outsourced banking activities. Uzbekistan has not issued any guidelines related to contracts for outsourced banking activities.

2.2 MANAGING OUTSOURCING RISKS

The rising trend in the outsourcing of banking activities can be attributed to reduced costs, improved efficiency and better flexibility in operations. Outsourcing can help a bank to access new technologies, tools and services that it lacks the capacity to provide, or that require large investments. However, the outsourcing of banking activities also introduces risks for banks and customers alike. Thus, managing outsourcing risks is now an increasing priority for financial sector regulators.

The responses show that banks in surveyed jurisdictions are allowed to outsource all or some of their banking activities, as well as other operations, including ancillary activities such as internal audit, accounting and risk management. While the outsourcing of certain activities can create several benefits, improperly managed outsourcing arrangements can expose the financial institution to security risks and compromise the soundness of a financial system. Most of the trends and challenges in outsourcing of digital services faced by banks globally are similar to those faced in the region. The following table showcases the risks outlined by the Basel Committee on Banking Supervision that are equally applicable to the region.¹⁰

The results of the survey indicate that all four jurisdictions allow for the outsourcing of IT and KYC functions. This practice carries the following general risks:

> Qualifications of service provider's workers:

Outsourcing can facilitate access to experienced IT specialists which are lacking in-house. However, third-party service providers often recall their most highly qualified workers to win new clients and replace them with less qualified ones.

8 Article 26. Transfer of personal data to third parties; and Article 27. Transfer of personal data to other states) and the Law of the Republic of Armenia, adopted on 7 October 1996 “On bank secrecy”.

9 Federal Law No. 152-FZ of July 27, 2006 “On personal data”

10 <https://www.bis.org/publ/joint12.pdf>

- > **Lack of compliance:** The service provider might not carry out the task as expected or monitor the process less closely than the principal would have done.
- > **Loss of technical capacity:** Outsourcing can gradually result in a loss of in-house expertise and capacity to provide a service over time because much of the new knowledge required to deliver innovative services remains with the third-party provider. The innovation capability of the firm may also be reduced, since this requires sufficient in-house technical and economic resources.
- > **Hidden costs:** Of all the perceived or real hidden costs related to outsourcing of banking activities, the following risks stand out:
 - a. **Search and hiring costs:** The costs associated with identifying, evaluating, negotiating and onboarding a third-party service provider are often not well understood or overlooked. It is difficult to assess search and hiring costs, as most of these costs are fixed and do not depend on the value of the contract; for example, whether the contract is valued at USD 10 million or USD 500 million. This limited range of information makes it difficult to identify the service provider that offers the most competitive contracting costs.
 - b. **Transition costs:** The cost estimates for a full transition from in-house IT to a third-party managed service can be widely divergent and depend on how long it takes for the provider to completely understand the service required by the bank.

TABLE 1: SOME KEY RISKS IN OUTSOURCING

RISK	MAJOR CONCERNS
STRATEGIC RISK	<ul style="list-style-type: none"> > The third party may conduct activities on its own behalf, which are inconsistent with the overall strategic goals of the regulated entity. > Failure to implement appropriate oversight of the third-party service provider. > Inadequate expertise to oversee the third-party service provider.
REPUTATION RISK	<ul style="list-style-type: none"> > Poor service from third-party service provider. > Customer interaction is inconsistent with the overall standards of the regulated entity. > Third-party practices not aligned with stated practices (ethical or otherwise) of regulated entity.
COMPLIANCE RISK	<ul style="list-style-type: none"> > Non-compliance with privacy laws. > Inadequate compliance with consumer and prudential laws. > Third-party service provider has inadequate compliance systems and controls.
OPERATIONAL RISK	<ul style="list-style-type: none"> > Technology failure. > Inadequate financial capacity to fulfill obligations and/or provide remedies. > Fraud or error. > Risk that banks find it difficult/costly to undertake inspections of the third-party service provider.
EXIT STRATEGY RISK	<ul style="list-style-type: none"> > The risk that appropriate exit strategies are not in place. This could arise from over-reliance on one firm, the loss of relevant skills in the bank itself that prevent it bringing the activity back in-house, and contracts that make a speedy exit prohibitively expensive. > Limited ability to return services to home country due to lack of staff or loss of intellectual history.
COUNTERPARTY RISK	<ul style="list-style-type: none"> > Inappropriate underwriting or credit assessments. > Quality of receivables may diminish.
COUNTRY RISK	<ul style="list-style-type: none"> > Political, social and legal climate may create added risk. > Business continuity planning is more complex.
CONTRACTUAL RISK	<ul style="list-style-type: none"> > Enforceability of contract. > For offshore contracts, choice of governing law is important.
ACCESS RISK	<ul style="list-style-type: none"> > Outsourcing arrangement hinders ability of regulated entity to provide timely data and other information to regulators. > Additional layer of difficulty for regulator in understanding activities of the service provider.
CONCENTRATION AND SYSTEMIC RISK	<p>Overall industry has significant exposure to third-party service provider. This concentration risk has a number of facets, including:</p> <ul style="list-style-type: none"> > Lack of control of individual firms over provider > Systemic risk to industry as a whole

c. Service provider management costs: The costs associated with managing a service provider are entirely internal to the bank and not part of the contract. Service provider management probably represents the largest category of hidden costs because it covers three areas: monitoring of the provider's contractual obligations, bargaining with the provider (and sanctioning it if necessary), and negotiating any contractual changes that may be needed. Banks often do not take such costs into consideration when outsourcing a service until it becomes apparent.

d. Switching costs: This generally refers to transitioning back to in-house services or switching service providers upon the expiry of an outsourcing contract. When services are redirected to a new provider, the cost involves the search for a suitable candidate, drafting a new contract and transitioning resources. Similarly, when services are reintegrated in-house, the cost involves rebuilding the activity from scratch.

> **Unclear cost-benefit relationship:** It is difficult to account for all relevant outsourcing factors in order to put a figure on their costs. For example, as in how to value the potentially better service delivered by the provider over an in-house department, or how to measure the consequences of a provider's poor quality of service.

> **Security and confidentiality concerns:** These are especially important when a provider also attends to several direct competitors and require strict confidentiality and non-disclosure clauses in the contract.

Outsourcing may seem to be a cost-effective and efficient way of managing KYC processes, but it can result in great setbacks if inadequately monitored. For banks and non-bank financial institutions, there are several important differences to note between KYC outsourcing and more commonly outsourced activities. KYC processes require a higher level of training compared with standard outsourced processes. Legally, a financial institution is ultimately responsible for the quality of work executed by a third-party service provider.

The survey shows that although there are some similarities in outsourcing regulation and supervision frameworks of the four jurisdictions, there are also many differences in approach, implementation and interpretation. Analysis of international practices shows even more broadly divergent regulatory approaches and supervisory practices.

As the outsourcing of banking activities is yet to have a standard process, it comes with various risks and cross-border issues. It is imperative to provide guidelines and principles to harmonize the following concepts and relationships in widely different jurisdictions across the world, to reduce regulatory arbitrage:

- > A clear segregation of the concepts of "outsourcing" and "purchase of services"
- > A descriptive list of "banking activities" that may be outsourced to a third-party provider
- > Clarification of a supervisory authority's role in overseeing outsourced banking activities (whether its prior consent must be obtained, or if it can be notified ex-post)
- > An elaboration of a supervisory authority's right to access data collected and used by a third-party provider for its services as well as its operational data, and to access its premises for inspection
- > Ensuring minimum security standards are met for the sharing of private data
- > Providing guidelines for qualifying criteria for third-party providers for outsourcing contracts
- > The harmonization and facilitation of cross-border issues
- > Providing guidelines for intragroup outsourcing contracts

These are the broad areas that need to be clarified, defined and somehow standardized across different jurisdictions to facilitate robust working relationships for outsourced banking activities. This is particularly so for the jurisdictions that take a totally unregulated approach and others where over-regulation is evident.

3. CASE STUDY: THE MAIN CHALLENGES ARISING FROM THE OUTSOURCING OF BANKING ACTIVITIES IN THE REPUBLIC OF ARMENIA

Financial institutions are constantly being pushed to assess the effectiveness of their core functions in order to deliver better value for investors. This constant drive to re-evaluate business models and become more flexible has inevitably led to an erosion of the distinction between core and non-core functions, paving the way for a range of new outsourcing opportunities along the way.

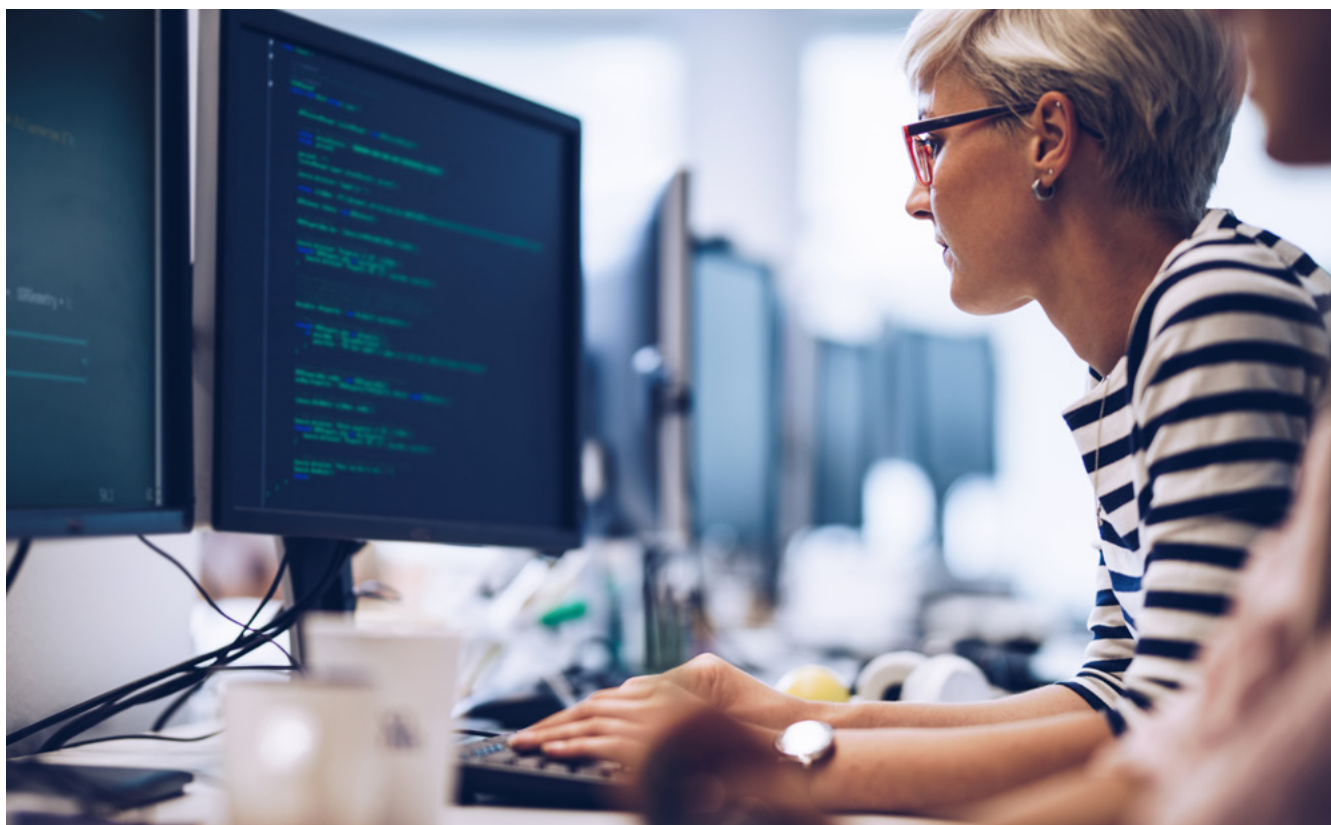
Outsourcing enables a bank to greatly expedite delivery, reduce operational costs and enhance efficiency by consolidating and centralizing its core activities. Banks that strive to keep everything in-house typically end up

developing a series of vertically integrated silos that result in extensive duplication and redundancy across businesses and markets.

Not only do these duplicated structures and inflexible services generate needlessly high costs, they also damage service quality. This is why banks are keen to outsource certain in-house functions that comprise part of their banking activities.

Several types of outsourcing have become increasingly common, such as IT outsourcing (ITO), which involves a third-party service provider being contracted to manage specific applications for a financial institution. Server management and infrastructure solutions, network administration, isolated cloud centers and software development are the most common functions to be outsourced. ITO is typically implemented to save banks time and money while introducing flexibility in terms of data storage, product offerings and speed of service.

It is also important to understand that by importing efficiency from third-party service providers, companies are also importing risks. In this context, it is important for supervisors to establish a mechanism by which banks can reduce their outsourcing risks.



To mitigate such risks, banks must perform due diligence with extra care before entering into any sort of outsourcing arrangement with a third-party service provider. Extensive research is needed to select the right partner, negotiate terms and change management, consider time frames and organize adequate exit and contingency policies in order to mitigate unforeseeable risks. A well thought out outsourcing strategy combined with careful due diligence can set a bank apart from its competitors.

This section details the regulatory framework and challenges related to supervising the outsourcing of banking activities in Armenia.

In 2018, the Central Bank of Armenia (CBA) introduced a new regulation on the outsourcing of banking activities, “CBA preliminary consent for outsourcing activities”.¹¹ The regulation sets out the main principles governing such outsourcing as follows:

- > The bank shall remain entirely responsible for the functions/activities outsourced to third parties
- > CBA has the right to conduct on-site inspections of the functions/activities outsourced at the service provider’s premises
- > Upon a request by CBA, the bank is obliged to amend/terminate the outsourcing contract signed with the service provider

Banks may legally outsource their activities to third-party providers only with the preliminary consent of CBA. Any outsourcing agreement signed without the preliminary consent of CBA is considered void.

In addition, CBA Regulation 4 on “Minimum requirements of internal control for banks” specifies that internal audits should include at least an assessment of the effectiveness of the activities outsourced by the bank.

The regulation sets out three types of outsourcing activities: highly relevant, relevant and non-relevant. Preliminary consent for each type is given based on its complexity and whether it meets a set of minimum requirements for third-party outsourcing contracts.

In particular, to obtain the preliminary consent of CBA for highly relevant activities, a bank must submit:

- 1) Information on the third-party service provider as required by CBA. (This information does not need to be provided if the provider is already an entity supervised by CBA.)
- 2) The draft contract for outsourcing activities.

- 3) Justification of the need for outsourcing, as well as an analysis of the risks arising from the outsourcing arrangement and the possible ways of mitigating them.
- 4) The applicant bank's internal rules that are relevant to the relationships created by the outsourcing arrangement, including its contractual relationship with the third-party service provider.
- 5) The applicant bank's contingency plans for its outsourced activities.
- 6) The applicant bank's assessment of the capacity of the third-party service provider's human resources, technical expertise, and other resources to perform the outsourced activities better than the outsourcing bank based on the requirements of Armenian law and existing international standards.
- 7) The service provider's contingency plans in the event of a failure to provide the outsourced activities as set out in the contract with the applicant bank.

The following are the detailed criteria that should be met in order to obtain CBA's preliminary consent for the outsourcing of banking activities:

- 1) The application should clearly show that the result of the outsourcing will significantly increase the efficiency of the bank's use of resources, reduce costs and increase efficiency, as well as improve the quality of service provided.
- 2) The draft contract should clearly describe the rights, obligations and responsibilities of the parties, and should contain provisions on:
 - a. the bank's right to monitor the service provider's performance of the outsourced activities;
 - b. the bank's authority to call for an external audit of the service provider on its own, as well as at the request of the CBA;
 - c. a description of the actions of the parties at the termination of the outsourcing contract, to ensure smooth continuity of operations;
 - d. a dispute resolution mechanism, in particular, whether the service provider continues to provide services pending the resolution of a dispute;
 - e. the protection of confidential information by the service provider; and,
 - f. procedures to facilitate supervision, inspection, auditing and research on the service provider's operations by CBA.

11 Article 34, Law on Banks and Banking, Republic of Armenia.

- 3) The applicant bank's contingency plan should set out the process for bringing the outsourced activities in-house, including how the bank's operations will be handled, the responsible parties and line of reporting, to ensure continuity of operations.
- 4) The applicant bank's internal rules on its relationship with third-party service providers should contain provisions on how to manage risks that arise in the selection process of a third-party service provider and its operations.

The criteria above are less stringent for outsourcing activities classified as "relevant". For outsourcing activities classified as "non-relevant", an annual notification requirement applies instead of the preliminary consent granted by CBA. The regulations on "CBA preliminary consent for outsourcing activities" also specify that:

- > Banking activities may not be subcontracted by a third-party service provider except for IT services.
- > In respect of outsourced banking activities that involve consumer or retail services, the bank shall notify a customer with whom it has an existing contract at least 10 days in advance of any change in the counterparty (i.e. the third-party service provider) by means of communication chosen by the customer.

- > When establishing a new relationship, in respect of transactions and relationships affected by the outsourcing contract between the bank and its retail customer, the bank shall inform the customer verbally that the servicing of interest is outsourced to the third-party service provider and furnish the customer with information about the provider, such as in a fact sheet and contract note.

However, despite the regulation of Armenia's financial services outsourcing relationships being in line with international best practices to mitigate major risks and to equip CBA with proper supervisory tools, challenges continue to arise in the following situations.

3.1. DETERMINING WHAT OUTSOURCED ACTIVITIES SHOULD BE REGULATED

Most supervisory authorities distinguish between material and non-material outsourcing, and issue guidance only for the former category. Although definitions of materiality are country-specific, the general idea is to concentrate on outsourcing relationships, which, if disrupted, would have significant negative impact on the bank's operations and its ability to perform as usual.



But sometimes the boundary between material and non-material outsourcing is unclear and this may cause disagreement between the bank and the supervisory authority. The same activity may be considered material for one institution but non-material for another. This requires subjective judgments on case-by-case basis. Hence to be on the safe side and to reduce subjective case-by-case judgments, CBA has defined as material all activities that require special licenses, as well as accounting, internal audit, compliance, risk management and IT services, all of which require substantial due diligence to be performed by banks in order to be outsourced. This creates additional paperwork for banks and increases the supervisory burden. However, it guarantees more resilient and justified outsourcing relationships.

3.2. DETERMINING IF A NEW REGULATION SHOULD APPLY TO EXISTING CONTRACTS

From a supervisory authority's point of view, regulation is intended to mitigate risk. Hence to ensure the financial system's resilience, it is only logical to apply new regulations to both existing and new contracts.

From a bank's point of view, applying new regulations to existing contracts can be a very costly exercise due to the need to renegotiate them, and there is no guarantee that its third-party service providers will agree to amend a contract to bring it into line with new regulations.

However, if new regulations apply to existing contracts, changes to their provisions are inevitable, and this places an onus on the bank and its third-party service provider to cooperate with each other. In extreme cases, it may be necessary for a bank to replace an existing service provider if it cannot meet the criteria set out in the new regulations. This might create business continuity issues, especially for contracts of outsourced banking activities that are categorized as relevant activities.

3.3. OUTSOURCING TO NON-RESIDENT COMPANIES

Outsourcing to non-resident service providers can be more cost-effective than outsourcing to resident service providers or in-house operations but it comes with certain risks.

The main risk is related to the different legal jurisdictions of the bank and the service provider. For example, CBA regulations give a supervisory authority the right to conduct on-site inspections of outsourced activities at the service provider's premises. But if the

service provider is non-resident, this legal right may not exist or be exercisable.

Another related risk is in the legal interpretation of the term "banking secrecy" which is particularly important in the sharing of personal data. In this case, it is crucial to provide clear definitions in the contract in order to ensure the security of personal data in compliance with the legal requirements of the jurisdiction from which it is being shared.

3.4. OUTSOURCING TO BIG TECH

With global third-party service providers such as Amazon or Google, on-site inspection will likely be costly, if at all possible. They may disallow a supervisory authority of a small jurisdiction, such as Armenia, from conducting on-site inspections. Similarly, they may disregard a request to report on the outsourced activities by a national supervisory authority and be unwilling to amend their standard contractual terms to comply with national regulations. Thus, a national supervisory authority has to weigh the benefits of allowing a bank under its watch to outsource its activities to world-class companies with good ratings, implied low risk and high security standards against the exploitation of personal data and possible non-compliance with national standards. The alternative is to allow banks to contract with only third-party service providers that will fully comply with national regulations but are less effective and recognized.

3.5. OUTSOURCING TO SMALL COMPANIES

The main disadvantage of such organizations is their small staff size. However, they usually lack dedicated legal, advisory or accounting departments which makes it unlikely that they can respond quickly and provide professional solutions to problems that arise.

3.6. IT OUTSOURCING

Compared with an in-house IT team, the main challenges with IT outsourcing (ITO) are as follows:

RAMP-UP PERIOD

A third-party service provider will likely need a long period of familiarization with a bank's working environment before achieving an acceptable level of efficiency. Depending upon how frequently the third-party service provider is on-site, it may be weeks or months before it acquires adequate knowledge of a bank's culture and IT systems to start offering it guidance and making recommendations for improvement.

TIMEFRAMES

Beyond the initial ramp-up period, a third-party service provider works to a schedule and will not always be on-site or provide support on demand. Because it has to prioritize the work of a number of different types of clients, it can only implement a bank's larger-scale initiatives in weeks rather than days.

SPECIALIZATION

If a bank uses non-standard applications, a third-party service provider may not be well-positioned to support them. In particular, while third-party IT service providers are generally very adept at supporting mainstream technologies and applications, they do not always have specialized knowledge of local or fully-customized software applications.

CULTURE

At best, a third-party service provider will become an accepted part of a bank but can never be fully immersed in its culture like an in-house department. However, a good firm will have systems in place to help bridge the gap.

Key to a successful contract for ITO is the choice of a provider prepared for the challenges inherent to outsourcing as detailed above, and has developed systems to compensate for them and prevent lapses in service. It will assess a project to accelerate ramp-up, and dedicate a team to working with a bank in real-time and that will be accountable for any delays. It will fathom a bank's IT capacity and capabilities, make contingency plans, and budget far in advance for upcoming projects. Finally, it will have the resources to provide a bank with prompt and reliable support. It will, of course, take some effort to identify firms that abide by these criteria.¹²

3.7. PROTECTION OF PERSONAL DATA

The outsourcing of banking activities is very risky for the protection of the personal data of a bank's customers because the third-party service provider will often have access to such data. It is incumbent upon a bank to notify its customers that their personal data will be shared with the third-party service provider, and to obtain their consent for it. Thus, a bank runs the risk of losing its customers from notifying them. However, non-compliance with disclosure regulations would be untenable for being unlawful and unethical, besides its obvious risks to a bank's reputation.

3.8. SUPERVISORY AUTHORITY STAFF

The staff of a supervisory authority must have a professional knowledge and experience to understand all the specifics of banking activities that can be outsourced, such as IT systems, and business processes. However, it may sometimes need expertise in very specific fields to bridge gaps in its knowledge. To build its in-house expertise, a supervisory authority would need to embark on a costly training program for its staff.

Summarizing, we may conclude that the prerequisite for effective and smooth outsourcing processes is a well-defined legal framework that provides the supervisory authority with all the required tools for effective supervision and the comprehensive information to be so effective. However, in addition to an effective regulatory framework, there should also be a well-performing, strong supervisory mechanism to address issues and challenges that arise in practice and that require ad-hoc approaches or case by case solutions.

¹² <https://resource.optimalnetworks.com/blog/2015/05/21/what-are-the-problems-with-outsourcing-it>

4. OUTSOURCING OF FINANCIAL SERVICES: INTERNATIONAL PRACTICES

In most jurisdictions, banks and non-bank financial institutions (NBFIs) are governed under a licensing regime. Because of the growing trend for banks and NBFIs to outsource their banking activities to third-party service providers, alternative ways of supervising their attendant risks have been developed.

There are two main models of supervision:

1. **Direct**, in which supervisory authorities directly organize or participate in on-site inspections of third-party service provider firms;¹³ and,
2. **Indirect**, which is more common among bank regulators around the world and by which regulators stipulate special provisions to be included in contracts between banks and third-party service providers.¹⁴

In recognition of concerns about the legal and systemic implications of the outsourcing of banking activities, a consultative paper outlining nine high-level principles of outsourcing was issued by the Joint Forum, a financial services policy group established by the Basel Committee on Banking Supervision, the International Organization of Securities Commissions, and the International Association of Insurance Supervisors. The principles can be grouped into three broad categories.¹⁵

The first category refers to the policies that regulated financial institutions should have in place even before entering into an outsourcing agreement. For example, the financial institution should establish a comprehensive policy for assessing whether and how certain activities can be outsourced, and its board of directors should retain direct responsibility for that policy. In addition, the financial institution should establish a comprehensive outsourcing-risk management program to monitor and address risks arising from the outsourced activities and relationships with service providers.

The second category addresses concerns around specific outsourcing arrangements. Outsourcing relationships should be governed by written contracts that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of all parties. The financial institution should also maintain adequate contingency plans and take appropriate steps to ensure that service provider protects the confidential information of both itself and that of its clients from intentional or inadvertent disclosure.

The third category addresses concerns specific to supervisory authorities which need to take into account outsourcing activities as an integral part of their monitoring responsibilities. They should assure themselves that the financial institution's outsourcing arrangements do not hamper its ability to meet its supervisory requirements; that is, supervisory authorities should be able to obtain promptly any relevant materials on the outsourced activities.

This section presents a brief overview of some characteristics of the outsourcing of banking activities in selected jurisdictions and is based on a thorough survey of international practices. It highlights some of the approaches taken by supervisory authorities to identify and mitigate the risks typical in outsourcing arrangements which might be instructive for jurisdictions in the EECA region for developing and enhancing their own frameworks.

For example, the US context illustrates the wide range of tools available to supervisory authorities in their oversight of third-party service-providers, and how these tools are extensively deployed in practice. The experience of Luxembourg shows how a well-established regulatory framework must be put into effect by a well-designed program for the supervision of third-party service providers. The example of Singapore shows the importance of manuals for financial institutions to effectively manage outsourcing risks.

13 Examples of supervisory authorities with such statutory powers include the Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg, the Saudi Arabian Monetary Authority (SAMA), and the Federal Reserve Bank, Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC) in the United States.

14 For examples, please kindly refer to Annex 2 - Indirect supervision of third-party service providers.

15 <https://www.frbsf.org/economic-research/publications/economic-letter/2004/november/outsourcing-by-financial-services-firms-the-supervisory-response/#conc>

4.1. EUROPEAN UNION



Competent authorities from the European Union have the authority to supervise the operational functions and activities outsourced by credit institutions to third parties. This includes the right to require all information that is necessary in order to carry out those tasks directly from the service provider, including for off-site inspections, as well as to perform inspections at their business premises. The supervisory guidance recommends that supervisory access should be guaranteed via a specific clause in the outsourcing contract.

Supervisory powers are encoded in the Capital Requirements Directive (CRD4), and have been adopted into law by EU member countries, as well as into the regulation of the European Central Bank's Single Supervisory Mechanism. Although CRD4 sets out minimum requirements, the process of adopting the directive into law by different jurisdictions may result in variations across the region. The European Banking Authority (EBA) periodically issues updated guidelines and recommendations to achieve a high-level of harmonization.¹⁶

The EBA's revised guidelines on outsourcing were published on 25 February, 2019. These address the

outsourcing of cloud data storage services, and oblige the cloud service provider to undertake in writing:

- > to provide to the competent authority supervising the outsourcing institution (or any third party appointed for that purpose by that authority) full access to the cloud service provider's business premises (head offices and operations centers), including the full range of devices, systems, networks and data used for providing the services to the outsourcing institution (right of access); and,
- > to confer to the competent authority supervising the outsourcing institution (or any third party appointed for that purpose by that authority) unrestricted rights of inspection and auditing related to the outsourced services (right of audit).¹⁷

Taking into account the emerging risk of transferring a huge range of banking data and processes to unregulated third party service providers, the guidelines help to ensure that supervisory authorities have full access to the data held by third-party service providers.

¹⁶ <https://www.bis.org/bcbs/publ/d431.pdf>

¹⁷ https://eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf



4.2. UNITED STATES



In the US, the Bank Service Company Act (BSCA), 12 USC §1867(c)¹⁸ provides the federal banking agencies with the authority to regulate and examine the performance of certain services by a third-party service provider for a depository institution “to the same extent as if such services were being performed by the depository institution itself on its own premises”. Other sources of statutory authority may also be relevant in specific situations, such as the enforcement authority over third-party service providers that meet the definition of “institution-affiliated party” (IAP) in the Federal Deposit Insurance Act (FDI Act), 12 USC §1813(u).¹⁹

Federal banking agencies have used this authority to conduct individual examinations of service providers; moreover, they have developed a formal supervisory program for significant technology service providers (TSPs) for the US banking industry. These examinations focus primarily on technology and operational risk. However, where appropriate, the inter-agency examination team may expand the scope of review for product-specific risks or other risk areas that can affect the services provided to the client of the depository institutions. In addition to the federal banking agencies, other financial supervisors, such as the Consumer Financial Protection Bureau (CFPB) and several state banking agencies have varying levels of authority to conduct examinations of third-party service providers.²⁰

In comparison with other jurisdictions, US supervisory bodies have extensive powers over third-party service providers which they often use. This is in contrast with some other jurisdictions where supervisory authorities can find it hard to access third-party service providers despite being empowered to do so under their respective regulatory frameworks. This problem is especially significant in jurisdictions with local, small-scale financial institutions that outsource their banking activities to Big Tech companies such as Google and Amazon. The latter are unlikely to respond to requests for information from supervisory authorities of minor clients, simply because it is not worth their while to deal with the red tape involved. Hence, the relationship between supervisory authorities in significant financial markets with third-party service providers is quite different to jurisdictions with a small financial market.

4.3. UNITED KINGDOM



In the UK, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) are empowered under the Financial Services and Markets Act to make rules and issue guidance. The PRA has

responsibility for prudential supervision of banks, insurance companies, building societies, credit unions and certain large investment firms, including the responsibility for supervising these firms' outsourcing arrangements. The FCA is responsible for supervising the business activities of all financial institutions (including those prudentially supervised by the PRA, which are therefore “dual-regulated”). The FCA is also responsible for supervising the outsourcing arrangements entered into by financial institutions not prudentially supervised by the PRA. A regulated firm cannot delegate or contract out of its regulatory obligations when outsourcing. It must give advance notice to the FCA or PRA (as applicable) of any proposal to enter into a material outsourcing arrangement and of any material changes to arrangements.

Financial institutions regulated only by the FCA must give notice to the FCA before entering into, or significantly changing, a material outsourcing arrangement. Firms that are also regulated by the PRA must also notify the PRA. Although no period of notice is specified, the appropriate regulator expects the financial institution to discuss matters with it at an early stage, before making any internal or external commitments.

Failure to give notice to the appropriate regulator is likely to amount to a breach of the rule requiring a financial institution to be open and co-operative with its regulator. Both the FCA and the PRA have various enforcement powers at their disposal, including the power to impose an unlimited fine.²¹

4.4. LUXEMBOURG

Luxembourg has developed a formal program for the supervision of third-party service providers of operational functions, which are registered as such (“professionnel du secteur financier de support”) by the Commission de Surveillance du Secteur Financier, Luxembourg's financial regulator. A formal program is important because it makes the supervision of outsourcing risks more organized and transparent, and allows for their identification and mitigation at an early stage. It also means a supervisory authority becomes more informed and involved in the outsourcing processes and builds communication channels with third-party service providers.

¹⁸ https://ithandbook.ffiec.gov/media/27536/con-12usc1861_1867c_bank_service_company_act.pdf

¹⁹ <https://www.fdic.gov/regulations/laws/rules/1000-400.html>

²⁰ <https://www.bis.org/bcbs/publ/d431.pdf>

²¹ <https://uk.practicallaw.thomsonreuters.com/>

4.5. ITALY



In addition to requirements under EU law, banks in Italy must comply with stringent requirements when outsourcing internal functions.²² Accordingly, when outsourcing internal functions, banks must:

- > set up protections against the possible risks arising from external choices
- > retain control over the outsourced activities
- > remain responsible for the outsourced activities
- > retain the essential competencies to re-insource the outsourced activities, if and when necessary

The last point is extremely important from the viewpoint of business continuity of the bank, but might prove too costly to do because of the very specific skills or technologies required.

Banks must implement adequate policies to meet the obligations above, and these must meet minimum requirements on details of the decision-making process for the outsourcing of internal functions, for example.

Banks that plan to outsource, even partially, the performance of important operational or control functions must submit a notification to the Bank of Italy or to the ECB, as the case may be. For a 60-day period following such notification, the Bank of Italy may initiate a procedure to prohibit the outsourcing. Additionally, sector-specific rules may apply depending on the specific features of the outsourcing agreement.²³

4.6. GERMANY



Financial institutions that outsource their activities must meet the requirements of the Banking Act (Kreditwesengesetz) (KWG) (section 25b, KWG).²⁴ They must take reasonable precautions to avoid excessive additional risks when outsourcing their activities and must ensure the German Federal Financial Supervisory Authority (BaFin) is not prevented from performing its duties, such that there is no negative impact from the outsourcing on its right to information, inspection and control.

BaFin has issued administrative guidelines for "minimum requirements on risk management" (MaRisk).²⁵ Article 9 of MaRisk contains important guidance on outsourcing. According to this guidance, as a general rule, all activities may be outsourced when this does not impair proper business organization. The financial institution determines on its own which of its activities are material with regard to outsourcing risks ("material outsourcings"). The following terms must be defined and agreed upon in a contract for material outsourcings:

- a) the specifications and, if necessary, description of services to be performed by the third-party service provider;
- b) stipulation on information that must be provided to the supervisory authority; and the obligation to comply with the supervisory authority's call for an internal and/or external audit;
- c) provision to ensure BaFin's access to information and ability to provide effective supervision;
- d) stipulation to comply with the supervisory authority's directives to minimize outsourcing risks;
- e) provisions for ensuring compliance with data protection regulations;
- f) appropriate periods of notice;
- g) provisions for various possible modalities of sub-outsourcing which guarantee that the contracting parties continue to comply with the banking supervisory requirements; and,
- h) the commitment of the third-party service provider to inform the financial institution of material developments affecting its performance of the contract.

In brief, the requirements above are to ensure that the directive powers, control and audit rights of the financial institution and the supervisory authority are written into the contract.

4.7. SINGAPORE



The Monetary Authority of Singapore (MAS)' Guidelines on Outsourcing²⁶ sets out its expectations of a financial institution that has entered into any outsourcing arrangement or is planning to outsource its business activities to a third-party service provider.

²² Bank of Italy, Circular No 285 of 19 December 2013, under Title IV, Chapter 3, Section IV (19th revision of 2 November 2016)

²³ <https://uk.practicallaw.thomsonreuters.com/3-501-4571?transitionType=Default&contextData=%28sc.Default%29>

²⁴ <https://www.cftc.gov/sites/default/files/idc/groups/public/@otherif/documents/ifdocs/eurexmcobankingact.pdf>

²⁵ <https://www.bundesbank.de/resource/blob/623102/bca5bafd72a669115b15c4125e063feb/mL/minimum-requirements-for-risk-management-mindestanforderungen-an-das-risikomanagement-marisk-data.pdf>

²⁶ <https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing>

The guidelines cover:

- > Engagement with MAS on outsourcing.
- > Sound practices of risk management of outsourcing arrangements.
- > Cloud computing.

In supervising an institution, MAS will review its implementation of the guidelines, the quality of its board and senior management oversight and governance, internal controls and risk management with regard to managing outsourcing risks.

MAS has removed the expectation for institutions to notify it before making any material outsourcing commitment. Institutions are expected to exercise appropriate due diligence on their outsourcing arrangements and be ready to demonstrate their observance of the guidelines, including submitting the outsourcing register to MAS at least annually or upon request.

Institutions are no longer expected to consult and submit the completed MAS Technology Questionnaire for Outsourcing to MAS before making any significant IT outsourcing commitment.²⁷

An institution should notify MAS as soon as possible of any adverse development arising from its outsourcing arrangements that could affect the institution. Such adverse developments include any event that could potentially lead to prolonged service failure or disruption in the outsourcing arrangement, or any breach of security and confidentiality of the institution's customer information. An institution should also notify MAS of such adverse developments encountered within the institution's group.

An institution should assess all relevant aspects of the service provider, including its capability to employ a high standard of care in the performance of the outsourcing arrangement as if the service is performed by the institution to meet its obligations as a regulated entity. The due diligence should also take into account the physical and IT security controls the service provider has in place, the business reputation and financial strength of the service provider, including the ethical and professional standards held by the service provider, and its ability to meet obligations under the outsourcing arrangement. On-site visits to the service provider, and where possible, independent reviews and market feedback on the service provider, should also be obtained to supplement the institution's assessment.

On-site visits should be conducted by persons who possess the requisite knowledge and skills to conduct the assessment.²⁸

4.8. JAPAN



The Financial Services Agency (FSA), which regulates the financial services industry, regularly conducts inspections of financial institutions and publishes manuals that are publicly available in relation to such inspections. In relation to outsourcing, the following points should be noted:

- > how the financial institution plans and implements outsourcing;
- > how the financial institution controls risks related to outsourcing; and,
- > how the financial institution resolves problematic issues.

However, even if the FSA identifies concerns in relation to the above, there are no penalties, although it may take these points into consideration when deciding whether to make an order, including for the business to submit a business improvement plan.

The manuals published by FSA cover security standards for computer systems that financial institutions must comply with, and ensure that third-party service providers comply with them as well.²⁹

While the Bank of Japan (BoJ) does not have a similar level of supervisory authority, the BoJ can conduct on-site inspections of third-party service providers (and re-assignees) with their consent, as well as consent by the assignor bank and initially assigned service providers.³⁰ In 2001, BoJ published a paper on risk control for the outsourcing of financial institution activities, which includes suggestions on how to carry out outsourcing for financial institutions. It does not prescribe penalties. The BoJ takes this paper into consideration when overseeing banking operations.³¹

In addition to onsite inspections, the BoJ conducts day-to-day off-site monitoring of these activities.

27 https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Outsourcing-Guidelines-Jul-2016_FAQ.pdf

28 <https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing>

29 <https://iclg.com/practice-areas/outourcing-laws-and-regulations/japan>

30 <https://www.bis.org/bcbs/publ/d431.pdf>

31 <https://iclg.com/practice-areas/outourcing-laws-and-regulations/japan>

4.9. CANADA



Federally regulated entities (FREs) such as financial institutions that outsource, or contemplate outsourcing, one or more of their business activities to a third-party service provider are expected to follow specific guidelines (B-10 Outsourcing of Business Activities, Functions and Processes Guideline (Guideline B-10)),³² published by the Office of the Superintendent of Financial Institutions (OSFI)). Although Guideline B-10 is not legally binding, the introduction states that its expectations should be considered prudent practices, procedures or standards that should be applied according to the characteristics of the outsourcing arrangement and the circumstances of the FRE. FREs are required to ensure their material outsourcing arrangements and service providers comply with Guideline B-10.

Guideline B-10 states that OSFI expects FREs to assess the materiality of all outsourcing arrangements and to follow risk management protocols for all outsourcing arrangements, except those that are deemed clearly immaterial. The materiality of an outsourcing arrangement depends on the extent to which it could have an important influence on a significant line of business of the FRE's consolidated operations, or the Canadian operations of a foreign branch or subsidiary.

OSFI has supplemented Guideline B-10 with a Memorandum (on) New technology-based outsourcing arrangements (dated 29 February 2012), which is intended to address issues raised by cloud computing. The memo states that FREs should recognize the unique features of new technology-based services such as cloud computing and duly consider the associated risks. The expectations contained in Guideline B-10 apply in respect of such services.

No formal regulatory notifications or approvals are required prior to outsourcing in the financial sector. However, Guideline B-10 requires an outsourcing FRE to notify OSFI in case of substantial security or data breaches. Also, FREs must ensure that the supplier regularly tests its business recovery system as it pertains to the outsourced activity and are expected to provide a summary of the test results to OSFI on reasonable notice.³³

Established international practice reveals significant differences in the range of powers available to supervisory authorities and the extent to which they use these powers.

An important component of outsourcing regulation is the notification and approval process for outsourcing activities. This notification can be required before the initiation of outsourcing, or after the fact. Mostly, it is the former, with varying notification periods of four days to three months prior the outsourcing contract entering into force. These procedures give a supervisory authority an opportunity to assess the risks associated with the outsourcing of specific activities and in case of concerns, to prohibit or prevent the outsourcing.

The table in Annex 1 summarizes the requirements for regulatory notification and approval of outsourcing transactions in key jurisdictions across the globe.

The other important component in the supervision of outsourcing risks is the power of the supervisory authority to access the premises of third-party service providers, which is provided in law or written into the outsourcing contract. The table in Annex 2 summarizes the rights to supervise or examine third-party service providers, regulatory requirements for contracts to allow supervisory access and the availability of formal processes to supervise service provider activities.

32 <http://www.osfi-bsif.gc.ca/eng/fi-if/rg-ro/gdn-ort/gl-ld/pages/b10.aspx>

33 <https://content.next.westlaw.com/Document/l2ef1288e1ed511e38578f7ccc38dcbee/View/FullText.html?navigationPath=Search%2Fv1%2FResults%2Fnavigation%2Fi0ad62aee0000016cbe4304a8454a72b8%3FNav%3DKNOWHOW%26fragmentIdenti>

5. CONCLUSION

The outsourcing of banking activities has grown rapidly in recent years due to continuous advancements in IT, and forecasts suggest that this trend towards outsourcing is likely to continue in the near future.

Although there are challenges associated with outsourcing for financial institutions and regulators, two issues deserve special highlight. The first involves concerns about maintaining the privacy of customers' financial information; the other involves maintaining the required level of control by supervisory bodies over the risks related to outsourcing.










The first issue becomes more vulnerable and less controllable when outsourcing process happens across borders; different legal frameworks and privacy standards make it more complicated to assure data security and soundness. Bearing in mind that customer data security and customer trust are a bank's most valuable assets, there is a need for universal privacy standards and internationally accepted processes to address issues raised by cross-border transactions. As the sharing of customers' private data involves not only regulated financial institutions but also unregulated companies from outside the financial sector, a comprehensive approach should be taken at the international level to cover all the parties involved in the outsourcing of banking activities. The responsibilities of each party should be set out, and a proper level of safeguards for customers of financial institutions should be prescribed.











International practice shows that many jurisdictions have outsourcing guidelines in place that describe the risk-evaluation processes for financial institutions, the assessment of service providers, outsourcing agreement policies, and so on. However, few jurisdictions have financial supervisory authorities with direct oversight of third-party service providers. In most of the cases, regulators impose requirements on banks to include specific provisions in the outsourcing contract. All these are different types of prudential measures to mitigate the risk, some of which put more responsibility and risk-preventing function on regulating entity; some leave the final decision after the regulatory body. However, no matter which option is chosen, the monitoring and supervising role of the supervisory authority should




be crucial in all cases. Regulators and supervisory authorities have the mandate to license, regulate and oversee financial markets and their participants in order to protect depositors and investors and to ensure financial stability. In this regard, they are responsible for assessing and regulating all the risks associated with banking activities. To fulfill their mandate, supervisory authorities should be extensively involved in the assessment and mitigation of material risks associated with the outsourcing of banking activities. They must ensure that regulatory arbitrage is not created and that the risks involved are disclosed to all parties and well-understood.

6. ANNEX 1: NOTIFICATIONS VS APPROVALS³⁴

³⁴ <https://uk.practicallaw.thomsonreuters.com/1-5182551?transition-Type=Default&contextData=%28sc.Default%29>

JURISDICTION		Which industry sectors require regulatory notification or approval of outsourcing transactions?	What are the time limits for notification/applications for approval?
AUSTRALIA		The financial services industry needs approval from the Australian Prudential Regulation Authority.	Notification is required within 20 business days of the execution of the outsourcing agreement.
BRAZIL		None.	None.
BULGARIA		<ul style="list-style-type: none"> > Financial services. > Telecommunications. > Personal data processing. > Others 	<ul style="list-style-type: none"> > There are no explicitly stipulated time limits. > The approval/notification should be sought in a timely manner prior to the date of commencement of the outsourcing.
CANADA		Financial services. An FRE that outsources, or contemplates the outsourcing of, one or more business activities must ensure that the key stakeholders within the FRE receive sufficient information to enable the FRE to discharge its duties and obligations under OSFI's Guideline B-10. While regulatory notification or approval is not required, some FREs may ask OSFI for guidance on material outsourcing arrangements in certain circumstances.	Not applicable. As noted in the left column, notification to OSFI is voluntary (that is, an FRE has no affirmative obligation to notify).
CHINA		Banks must notify CBRC of the outsourcing of certain types of activities.	<ul style="list-style-type: none"> > No statutory time limits. > Generally, notification should be made before entering into a binding outsourcing agreement.
DENMARK		Undertakings conducting financial services must give notice to the Danish Financial Services Authority (FSA) before entering into, or significantly changing, a material outsourcing arrangement.	The notice must be given within 8 days from the day the outsourcing contract has been entered into.
FRANCE		Any sector outsourcing personal data collection: approval must be sent to the French Data Protection Authority (CNIL).	Any data processing must be subject to a declaration with the CNIL prior to its implementation.
GERMANY		There are no regulatory notifications or approvals needed from officials for outsourcing transactions. As an exception, a stock exchange carrier must immediately notify the supervisory authority about its intention to outsource and the execution of the outsourcing transaction.	Not applicable.
HONG KONG		Monetary Authority: an authorized institution under the regulation of the Hong Kong Monetary Authority.	Discuss outsourcing plan with Monetary Authority in advance.

JURISDICTION		Which industry sectors require regulatory notification or approval of outsourcing transactions?	What are the time limits for notification/applications for approval?
INDIA		Generally, there is no specific notification required for conducting an outsourcing transaction.	Generally, there is no specific notification required for conducting an outsourcing transaction.
IRELAND		Notice of outsourcing by regulated financial services entities must be sent to and cleared by the Central Bank of Ireland.	The outsourcing must be notified in sufficient time to enable it to be cleared by the Central Bank of Ireland prior to the outsourcing becoming effective. Specific timelines may be mandated for specific financial services.
ITALY		Banking.	At least 60 days before the contract is performed. The supervising authority can commence a proceeding to prohibit the outsourcing within this term.
JAPAN		There are no industry sectors that require regulatory notifications or approvals for the outsourcing of transactions.	Not applicable.
LUXEMBURG		In the financial sector, the project must be notified to, or obtain authorization from, the CSSF, depending on the outsourcing scheme. Any credit institution, payment institution, e-money institution and investment fund manager, which intends to carry out an outsourcing relying on a cloud computing infrastructure shall keep a register and obtain prior authorization from CSSF in case of material outsourcing.	Not applicable.
MEXICO		There are no specific outsourcing regulations.	Not applicable.
THE NETHERLANDS		Financial sector: depending on the scope and type of activities, an outsourcing may cause a change within the financial undertaking that must be notified to the Dutch supervisor the Dutch National Bank or the Authority for the Financial Markets.	At least 14 days before the change.
SINGAPORE		Financial services: Monetary Authority of Singapore (MAS).	Except as specifically stated, notifications are pre-event or post-event, as appropriate.
SPAIN		Financial services: Bank of Spain (BdE) and/or the Spanish Securities Market Commission (CNMV). Personal data: Spanish Data Protection Agency (AEPD).	Financial institutions must notify any agreements outsourcing essential services or functions to the Bank of Spain and/or the Spanish Securities Market Commission (CNMV) one month in advance. Prior the authorization from the Director of the Data Protection Agency (transfers of personal data to third countries which do not ensure an adequate level of protection).
SWEDEN		Financial sector. An outsourcing requires notification to the Financial Services Authorities (FSA). The outsourcing agreement must be in writing and submitted to the FSA. No formal approval of the contract is required.	FSA. Notification to the FSA must be made at least 1 month before the execution of the agreement.

JURISDICTION	Which industry sectors require regulatory notification or approval of outsourcing transactions?	What are the time limits for notification/applications for approval?
SWITZERLAND 	Financial services. For an outsourcing transaction by a bank or securities dealer, no notification required if compliant with Outsourcing Circular of the Swiss Financial Market Supervisory Authority (FINMA) and the Data Protection Act.	Courtesy notifications should be considered for material outsourcing transactions. No specific time limits in this respect.
UK (ENGLAND & WALES) 	Financial Services. Regulated firms must give advance notification to the PRA and/or FCA (as appropriate) before entering into, or significantly changing, a material outsourcing arrangement.	No notice period is specified, but notification must be done promptly, prior to making any internal or external commitments.
UNITED STATES 	<p>The Securities and Exchange Act requires notification in a filing with the Securities Exchange Commission upon a US public company entering into a "material definitive agreement" not made in the ordinary course of business, as well as a material amendment to such agreements and early termination of an agreement if the early termination has a material effect on the public company.</p> <p>Under the Bank Service Company Act and the Home Owner's Loan Act, covered financial institutions under these Acts must notify their primary federal regulator if they enter into an agreement with a third party service provider.</p>	<p>Notice must be made within 4 business days of the execution of the agreement.</p> <p>Notice must be made within 30 days of entering into an agreement with a third-party service provider.</p>

7. ANNEX 2: INDIRECT SUPERVISION OF THIRD-PARTY SERVICE PROVIDERS³⁵

35 <https://www.bis.org/bcbs/publ/d431.pdf>

36 For European jurisdictions, the authority to supervise third-party service providers is usually limited to activities and services provided to the bank, with the aim to inspect if the proper business organization of the bank is ensured and not compromised. If deficiencies are identified, further regulatory action can be taken against the bank, not the third-party service provider.

JURISDICTION	Authority to supervise or examine third-party service providers ³⁶	Regulatory requirement for contracts to allow supervisory access	Program/process to supervise service provider activities
ARGENTINA - BCRA	Yes	Yes	Depends
AUSTRALIA - APRA	No	Yes	Depends
AUSTRALIA - RBA	No	Yes	No
AUSTRALIA - ASIC	No	No	No
BELGIUM - NBB	Yes	Yes	Yes
BRAZIL - CBB	No	Yes	Depends
CANADA - OSFI	No	Yes	No
CHINA - CBRC	Depends	Yes	Depends
EUROPEAN CENTRAL BANK	Yes	Yes	Yes
FRANCE - ACPR	Yes	Yes	No
GERMANY - BUBA	Yes	Yes	Yes
GERMANY - BAFIN	Yes	Yes	Yes
HONG-KONG SAR - HKMA	No	Yes	No
INDIA - RBI	Depends	Yes	Depends
ITALY - BOL	Yes	Yes	Depends
JAPAN - FSA	Yes	Yes	Depends
JAPAN - BOJ	No	No	Depends
KOREA - BOK	No	No	No
KOREA - FSS	No	Yes	No
LUXEMBOURG - CSSF	Yes	Yes	Yes
MEXICO - BOM	No	Yes	No
MEXICO - CNBV	Depends	Yes	Yes
NETHERLANDS - DNB	Yes	Yes	Depends
RUSSIA - CBR	No	Yes	Yes
SAUDI ARABIA - SAMA	Yes	Yes	Yes
SINGAPORE - MAS	No	Yes	No
SOUTH AFRICA - SARB	No	Yes	No
SPAIN - BOS	Yes	Yes	Yes
SWEDEN - FINANSINSPEKTIONEN	Yes	Yes	No
SWITZERLAND - SNB AND FINMA	Depends	Depends	No
TURKEY - BRSA	Yes	Yes	Depends
UNITED KINGDOM - BOE AND FCA	Yes	Yes	No
UNITED STATES - FRB	Yes	No	Yes
UNITED STATES - FDIC	Yes	No	Yes
UNITED STATES - OCC	Yes	No	Yes

8. ANNEX 3: QUESTIONNAIRE ON OUTSOURCING

1. Is it allowed in your jurisdiction to outsource activities from banks to third parties (hereinafter referred to as a “counterparty”)

☐ Yes ☐ No ☐ Other

If “Other” is selected, please specify

2. Is there a definition of “outsourcing” in your jurisdiction?

☐ Yes ☐ No ☐ Other

If “Yes” is selected, please provide
If “Other” is selected, please specify

3. Is there segregation between “outsourcing” and “purchase of services” in your jurisdiction?

☐ Yes ☐ No ☐ Other

If “Other” is selected, please specify

4. Is there a definition of “purchase of services” in your jurisdiction?

☐ Yes ☐ No ☐ Other

If “Yes” is selected, please provide
If “Other” is selected, please specify

5. Which banking activities/operations/functions are allowed to be outsourced by a bank to a counterparty? (multiple options are available)

☐ Attracting deposits ☐ providing loans
☐ internal audit ☐ accounting ☐ IT systems
☐ risk management ☐ compliance ☐ KYC

Others

Comments, if any

6. Who can act as a counterparty when outsourcing banking activities/operations? (multiple options are available)

☐ organizations, licensed and supervised by the supervisory authority
☐ any legal entity ☐ any natural entity ☐ other

If “Other” is selected, please specify

7. What is the procedure of outsourcing banking activities/operations to a counterparty?

☐ It is necessary to get the prior consent of the supervisory authority
☐ It is necessary to inform the supervisory authority ____ days **before** outsourcing
☐ It is necessary to inform the supervisory authority ____ days **after** outsourcing
☐ other

If “Other” is selected, please specify

8. Does the supervisory authority have a power to proceed inspections/supervision at the counterparty’s premises?

☐ Yes ☐ No ☐ Other

If “Other” is selected, please specify

9. Is the intragroup outsourcing (when the bank and the counterparty ARE members of the same banking/financial group) subject to the same regulatory and supervisory requirements as the ordinary outsourcing (when the bank and the counterparty ARE NOT members of the same banking/financial group)?

☐ Yes ☐ No ☐ Other

If “No” or “Other” is selected, please specify

10. Does the legislation define special requirements/procedures while transferring personal data (data containing secrecy) to the counterparty?

☐ Yes, the data may be transferred only within the same jurisdiction
☐ Yes, the data may be transferred only to a counterparty, licensed by the regulatory authority
☐ Yes, the data may be transferred only to a counterparty, having a special permission to deal

with personal data (data containing secrecy)

☐ Yes, the data may be transferred to any legal entity

☐ No

☐ Other

If “Other” is selected, please specify

11. Does the legislation explicitly define the requirements on the outsourcing contracts, signed between the bank and the counterparty?

☐ Yes ☐ No ☐ Other

If “Yes” or “Other” is selected, please specify

12. Does the supervisory authority have special guidelines for the supervision of outsourcing activities?

☐ Yes ☐ No ☐ Other

If “Other” is selected, please specify

9. ANNEX 4: SUMMARY OF RESPONSES

37 Uzbekistan's responses are based on provisions of its draft law.

38 If the outsourcing company is a bank or on-bank organization, then it can. If not a bank, then there are many conventions, there is no direct indication of outsourcing, but in principle, legislation allows for cross-checks.

39 Following the adoption of the law "On banks and banking activities" by the Parliament of Uzbekistan, the Central Bank of Uzbekistan will issue special guidelines for supervising the outsourcing of banking activities.

COUNTRY	Armenia	Belarus	Russia	Uzbekistan ³⁷
Banks are allowed to outsource activities to third parties	YES	YES	YES	YES
There is a definition of "outsourcing"	NO	YES	YES	YES
There is a segregation between "outsourcing" and "purchase of services"	NO	NO	YES	YES
There is a definition of "purchase of services"	NO	NO	YES	NO
Banking activities/ operations/functions, that are allowed to be outsourced	<ul style="list-style-type: none"> > all banking activities, > internal audit, > accounting, > risk management, > compliance, > IT systems, > KYC 	<ul style="list-style-type: none"> > attracting deposits, > providing loans, > IT systems, > KYC 	<ul style="list-style-type: none"> > internal audit, > risk management, > compliance, > IT systems, > KYC 	<ul style="list-style-type: none"> > providing loans, > accounting, > IT systems, > KYC
When outsourcing, as a counterparty can act	<ul style="list-style-type: none"> > organizations, licensed and supervised by the supervisory authority > any legal entity 	<ul style="list-style-type: none"> > organizations, licensed and supervised by the supervisory authority > any legal entity 	<ul style="list-style-type: none"> > organizations, licensed and supervised by the supervisory authority > any legal entity > any natural person 	organizations with corresponding license, in case of outsourcing of certain types of banking services and operations
Procedure of outsourcing banking activities/operations is	to get the prior consent of the supervisory authority	to disclose it, maintaining a register of outsourcing companies	N/A It depends on the type of outsourced function	to get the prior consent of the supervisory authority
The supervisory authority have a power to proceed inspections/supervision at the counterparty's premises	YES	YES ³⁸	depends on the type of outsourcing	YES
The intragroup outsourcing is subject to the same regulatory and supervisory requirements as the ordinary outsourcing	YES	YES	NO (There is a specific regulation)	YES
There is a special requirements/ procedure while transferring personal data	YES	N/A	YES	YES
The legislation explicitly defines the requirements on the outsourcing contracts, signed between the bank and the counterparty	YES	YES	YES	NO
Supervisory authority has special guidelines for the supervision of outsourcing activities	NO	YES	NO	NO ³⁹

Alliance for Financial Inclusion

AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia

t +60 3 2776 9000 e info@afi-global.org www.afi-global.org

 Alliance for Financial Inclusion  AFI.History  @NewsAFI  @afinetwork