2 Oversight of Payment Systems Stability

2.1 Roles and responsibilities of the BOT in supervising important payment systems

Payment systems are significantly important financial infrastructures for the country's currency circulation and economic growth given their roles in supporting financial transactions of financial institutions, the public sector, the private sector, small businesses, and the general public. Therefore, it is crucial that payment systems are supervised to ensure sound management, security, continual operation, and appropriate consumer protection to foster users' confidence.

The BOT is entrusted with the task to maintain the country's payment systems stability, ensuring that operations are conducted with efficiency, safety, consumer protection, appropriate risk management, along with compliance with the international standard — Principles for Financial Market Infrastructures (PFMIs) — issued by the Bank for International Settlements (BIS). Committees whose functionalities are involved in this supervisory role include the Payment Systems Committee (PSC) that sets policies on supervision of systemically important payment systems and oversees the country's payment systems stability, and the Electronic Transactions Commission (ETC) that sets policies on supervision of electronic payment service providers.

2.2 Important payment systems

There are two categories of important payment systems under the BOT's oversight.

1) Systemically Important Payment Systems (SIPS) are infrastructures that support interbank high-value funds transfer and payment. There is only one SIPS in Thailand, that is, the Bank of Thailand Automated High-Value Transfer Network (BAHTNET), operated by the BOT.

2) Prominently Important Retail Payment Systems (PIRPS) include the Imaged Cheque Clearing and Archive System (ICAS), operated by the BOT, and interbank retail funds transfer systems such as ATM pool and interbank retail bulk payment systems, operated by National ITMX Co. Ltd. (NITMX).

2.3 Oversight approach

The BOT prescribes an approach in oversight of important payment systems in the Oversight Policy Framework as follows.

1) Periodic analysis, monitoring, and assessment of risks in important payment systems to assess impacts of key risks such as liquidity risk, operational risk and settlement risk, which could result in potential systemic risk in the payment systems under various abnormal circumstances or crises, including impacts in case of key changes to the systems or regulations;
2) Assigning payment systems operators to undertake self-assessment against to the PFMIs; and
3) Conducting on-site assessment of service providers to assess potential risks which could arise during business processing and services.

In addition, the BOT undertakes cooperative oversight together with the Securities and Exchange Commission (SEC)[6] in relation to information sharing on oversight of Financial Market Infrastructures (FMIs), progression on oversight of interconnected systems, regulation compliance and risk management that should be aligned with PFMIs.

2.4 Ensuring stability of important payment systems

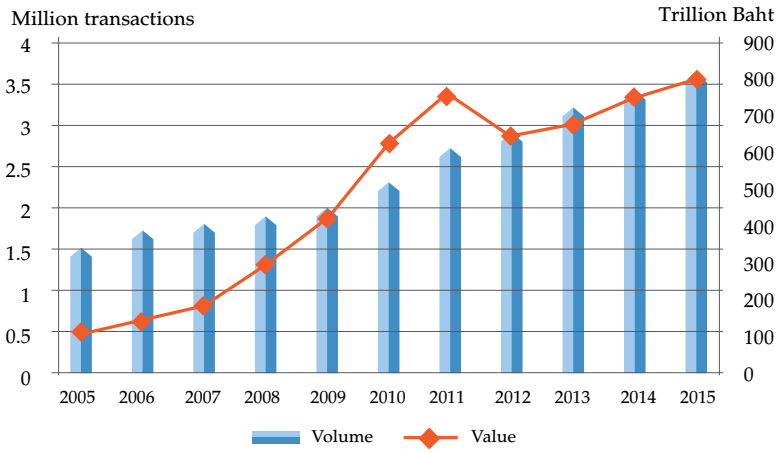
2.4.1 Bank of Thailand Automated High-Value Transfer Network (BAHTNET)

BAHTNET is an important high-value funds transfer system that caters for funds transfer between financial institutions with deposit accounts at the BOT, for example, interbank funds transfer, third-party funds transfer, funds transfer for securities settlement and multilateral funds transfer. The BOT, thus, needs to supervise BAHTNET in compliance with PFMIs so that its operation and risk management are efficient enabling it to offer services with no interruption both normal and emergency circumstances.

6 The SEC oversees the Securities Settlement System (SSS); Central Counterparties (CCP), operated by Thailand Clearing House (TCH); and Central Securities Depositories (CSD), operated by Thailand Securities Depository (TSD).

In 2015, funds transfer through BAHTNET totaled at 3.6 million transactions, equivalent to 790 trillion baht. Compared to 2014, funds transfer volume increased by 6.4 percent while funds transfer value increased by 4.3 percent. Both BAHTNET funds transfer volume and value increased steadily, averaging at 14,800 transactions and 3.3 trillion Baht per day. BAHTNET funds transfer value was 58.4 times of GDP.

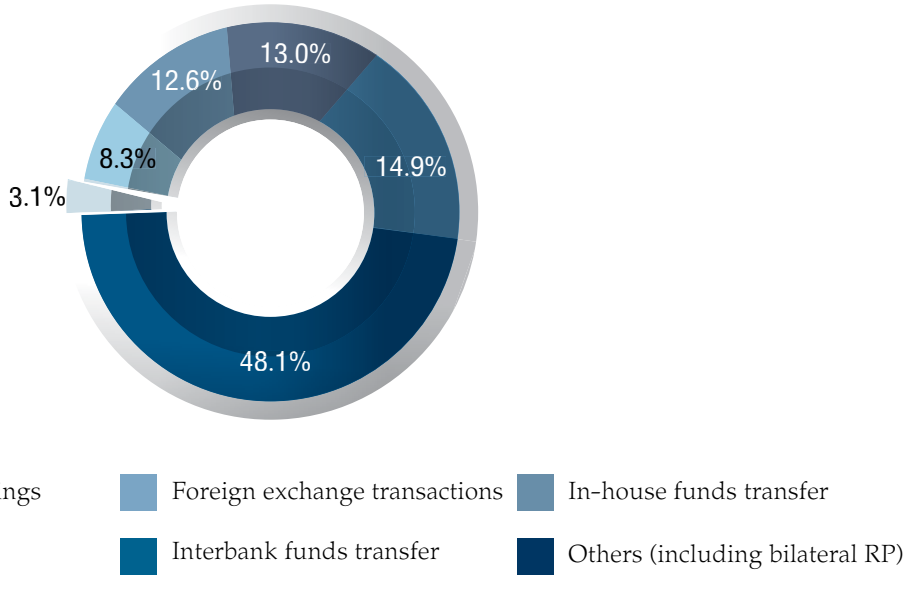
Figure 3: Volumes and values of funds transfer through BAHTNET



Source: Bank of Thailand

In transaction type categories revealed that bilateral repurchase operations (bilateral RP) was the highest proportion, reaching 48.1 percent with total value of 375.7 trillion Baht, followed by interbank funds transfer at 14.9 percent, securities trading at 13.0 percent, in-house funds transfer at 12.6 percent, foreign exchange transactions at 8.3 percent and interbank borrowing at 3.1 percent.

Figure 4: Proportion of funds transfer through BAHTNET categorized by transaction types



Source: Bank of Thailand

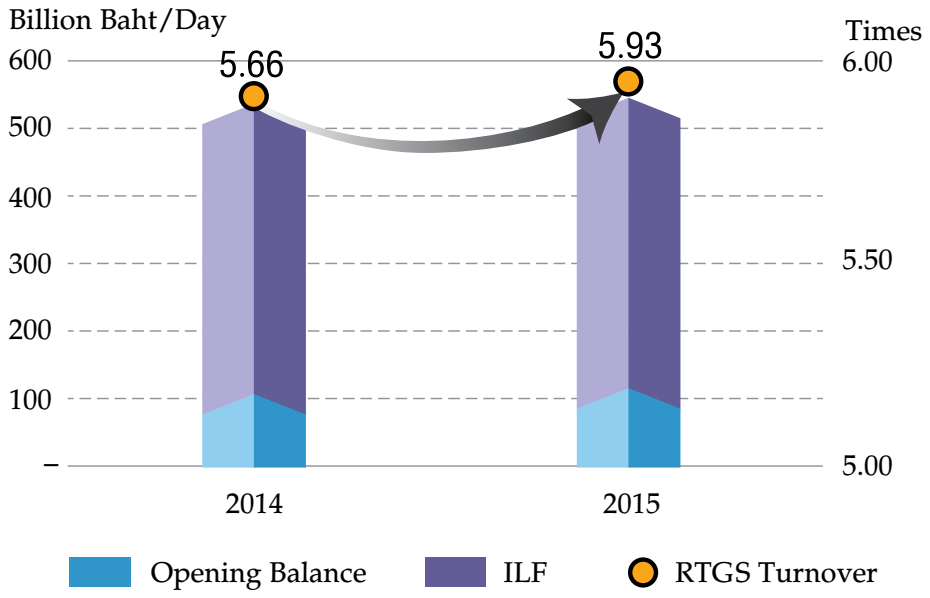
- Management of material risks in BAHTNET

(1) Liquidity risk and settlement risk

BAHTNET members had adequate liquidity to support BAHTNET funds transfer without incurring settlement risk. In 2015, intraday liquidity of members consisted of opening balances and Intraday Liquidity Facility (ILF), averaging at 548.7 billion Baht per day, increasing by 0.3 percent or 1.8 billion Baht per day from 2014. In terms of Real-time Gross Settlement (RTGS) Turnover, daily turnover was 5.7 times in 2014 and 5.9 times in 2015. In addition, fund transfer orders in queue was only at 1.5 percent of total transaction volume.

On risk management for multilateral net settlement, the BOT endorsed the measurement on Securities Requirement for Settlement (SRS) which was come into effect on 2 July 2015, requiring member banks to pledge collateral against the exposure arising from net settlement of retail payment such as cheque clearing and interbank retail funds transfer. Securities requirement shall not be less than the maximum possible negative balance. This would reduce risk in case a member bank has insufficient funds to complete settlement and might affect others in the system. At present, multilateral net settlement can be completed within prescribed timeframe without the need to enforce SRS.

Figure 5: Daily average of BAHTNET intraday liquidity



Source: Bank of Thailand

(2) Operational risk

Operational risk is a key risk in BAHTNET that the BOT should oversee to ensure a high degree of security and operational reliability in both normal and emergency circumstances. Management for continuity of BAHTNET is a crucial key to support smooth functioning of payment systems. The BOT, as an operator of BAHTNET, prescribed target system availability at 99.7 percent based on operations during past periods. In 2015, BAHTNET's system availability was 99.95 percent, higher than the target set. The BOT monitors BAHTNET's system availability periodically and reports results to concerned management and the PSC every six months.

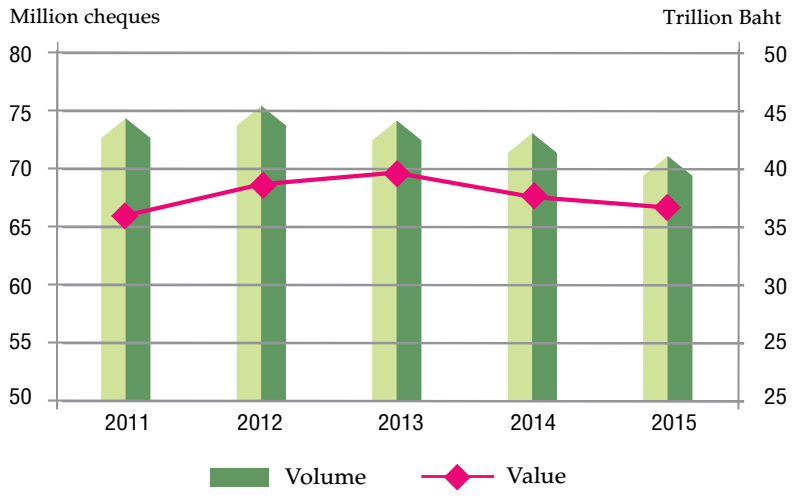
- **BAHTNET's compliance with PFMIs**

The BOT plans to join for the Financial Sector Assessment Program (FSAP) in 2018. Since 2015, the BOT has enhanced the efficiency of BAHTNET along with its compliance with international standards such as expediting the legislation of payment finality, designing default rules and procedures for BAHTNET's members in the event of default or bankruptcy (default management), and establishing a risk management framework to manage the range of risks that are borne by BAHTNET according to PFMIs.

2.4.2 Imaged Cheque Clearing and Archive System (ICAS)

ICAS is an important retail funds transfer system that caters for interbank imaged cheque clearing. The BOT has decided that 14 PFMIs, out of the 18 that are applicable to ICAS.

Figure 6: Volume and value of interbank cheques

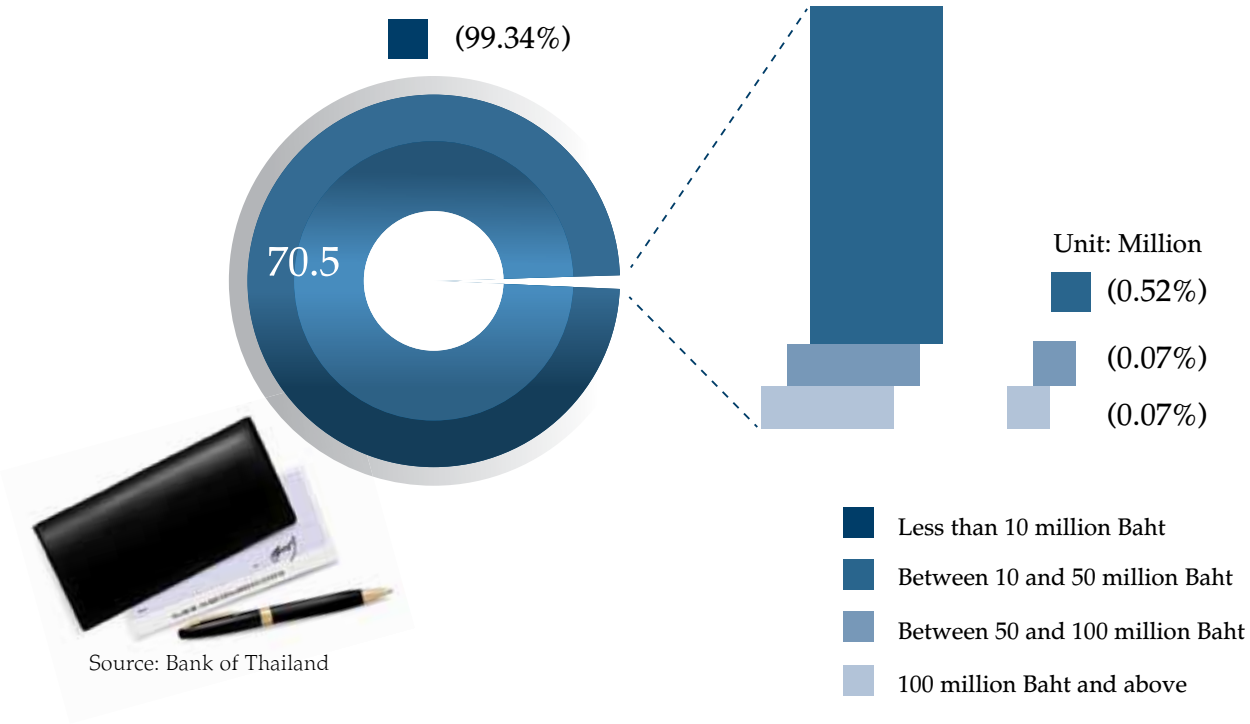


Source: Bank of Thailand

In 2015, interbank cheques nationwide totaled 71.0 million cheques, representing 37.4 trillion baht, declining from 2014 by 2.3 and 1.4 percent, respectively. The volume and value of interbank cheques averaged at 292,331 cheques and 154.1 billion baht per day, also trending downwards due to domestic economic condition coupled with increase in e-Payment during previous years.

In 2015, for Bangkok metropolitan region, interbank cheques of less than 10 million Baht in value made up the highest proportion of 99.34 percent or 70.5 million cheques, followed by interbank cheques of between 10 and 50 million Baht in value (0.52 percent), interbank cheques of between 50 and 100 million Baht in value (0.07 percent), and interbank cheques of 100 million Baht and above in value (0.07 percent).

Figure 7: Volume of interbank cheques in Bangkok metropolitan region, classified by value in 2015



Source: Bank of Thailand

- Management of material risks in ICAS

The BOT continuously managed operational risk and business continuity of ICAS whereby the target of systems availability was set at 99.7 percent. In 2015, ICAS achieved 99.99 percent systems availability, higher than the target set. The BOT monitors ICAS' system availability continually and reports results to concerned management and the PSC every six months.

- Oversight of ICAS

The BOT has adopted 14 PFMIs out of the 18 in the oversight of ICAS. In 2015, the BOT conducted an onsite examination specifically on the ICAS' operational risk (Principle 17: operational risk) in two dimensions (1) operational reliability and availability; and (2) business continuity management (BCM). The examination found that ICAS had risk management measures and procedures for operational reliability and availability and business continuity management that mostly complied with PFMIs. Any identified gaps were not issues of concern and manageable.

2.4.3 Interbank Transaction Management and Exchange (ITMX)

The BOT oversees NITMX which is an important retail funds transfer system by virtue of the provisions of the Royal Decree on Regulating Electronic Payment Services Business B.E. 2551 (2008) and applies PFMIs in the oversight of NITMX.

In 2015, the BOT conducted an onsite assessment of NITMX in compliance with PFMIs and summarized that NITMX's operation and risk management mostly complied with PFMIs on areas such as legal risk, operational risk, and settlement risk. In addition, its system development to respond to member banks' need was also carried out. The NITMX disclosed clear regulations, procedures, and access criteria as well as necessary usage information to members and stakeholders. Moreover, communication procedures for data transfer were found to meet required standards. There were no serious issues of concern that require immediate action.

2.5 International standards on key payment systems oversight

In 2015, the Working Group on Cyber Resilience under the Committee on Payments and Market Infrastructures (CPMI) and the Technical Committee of the International Organization of Securities Commission (IOSCO), referred to as CPMI – IOSCO, which is responsible for formulating international standards on oversight of efficiency and stability of payment systems and securities related systems, under the umbrella of the Bank for International Settlements (BIS), issued a consultative document titled "Guidance on Cyber Resilience for Financial Market Infrastructures" to be used as supplementary guidelines for PFMIs.

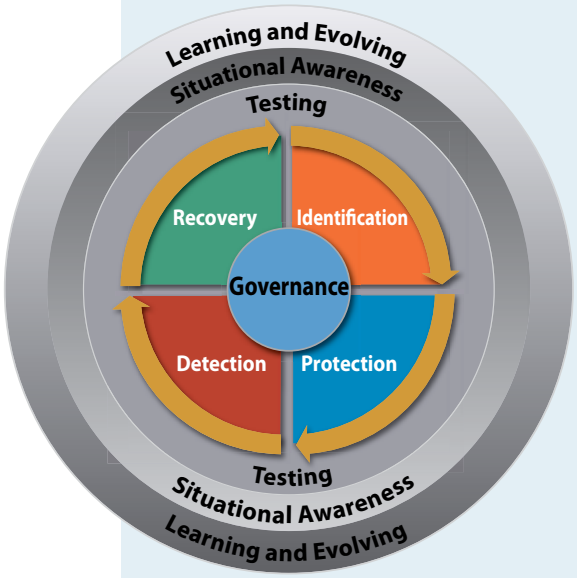
In short, the Guidance requires operators of FMIs and their regulators to adequately recognize cyber risks, including personnel in all levels of the organizations. Consideration must also be given to connectivity with FMIs that may result in interconnected risks and impacts, focusing on monitoring and collection of data on network computers for systematic analysis and interpretation in order to yield effective operation. The Guidance also focuses on subjecting designed cybersecurity measures to tests and emphasizes the importance of swift response and recovery by FMIs. The complete version of the Guidance was issued in June 2016 and the BOT would consider applying it to oversee important payment systems in the future.

Box 7: Cyber resilience for Financial Market Infrastructures

Cyber resilience refers to the ability to prepare, resist, and control the situation as well as swiftly recover the systems to normal operation after a cyber-attack.

Strengthening cyber resilience of important payment systems classified as FMIs is a crucial task that would support payment systems efficiency and compliance with PFMIs as well as allow financial transactions to be processed continuously. There must also be appropriate operational risk management and recovery procedures which allow the safe resumption of critical operations within 2 hours of a cyber disruption, and also enable itself to complete settlement by the end of the day the disruption occurred.

In order to ensure an operational framework for FMIs to strengthen cyber resilience, CPMI-IOSCO issued Guidance on Cyber Resilience for Financial Market Infrastructures to serve as guidelines for FMIs to adapt for usage. The guidance outlines 5 primary risk management categories known as GIPDR, as follow;



Governance: Ensure necessary measures, procedures and resources for cyber risk management

Identification: Identify factors that influence key operations, including procedures, systems or networks

Protection: Identify factors that influence key operations, including procedures, systems or networks

Protection: Prescribe standards for control and design procedures to protect key operations

Detection: Monitor and detect cyber threats in a quick and timely fashion

Recovery: Control the situation and minimize damage, ensuring that recovery can take place quickly and securely, thereby enabling continu ous operations of FMIs

Additionally, in order to achieve resilience objectives, there are 3 overarching components that should be factored across an FMI's cyber resilience framework. The overarching components are: testing (all elements of a cyber resilience framework should be tested to determine their overall effectiveness), situation awareness (ability to understand and pre-empt cyber events, and to effectively detect, respond to and recover from cyber attacks that are not prevented), and learning and evolving (aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evolution).

Mobile wallet
in cart 2 item(s)
1 add to cart
Your Online Shopping
cancel
next
ANALYTICS
1234 5678 9012 3456
0000
Bank Name

3 Supervision of e-Payment Service Providers

3.1 Revision of laws and regulations on supervision of service providers

In 2015, the BOT considered reviewing related laws and regulations as follows.

1) Revised rules, procedures, and conditions for supervision under the Royal Decree on Regulating Electronic Payment Services Business B.E. 2551 (2008) which is a sub-law under the Electronic Transactions Act B.E. 2544 (2001), including revision of notifications of the ETC and the BOT to be more appropriate and in line with changes in economic environment and business models. The revised notifications of the ETC and BOT were published in the Government Gazette dated 11 April 2016 and 28 April 2016 respectively with salient points as follows.
   - Revised rules on supervision of service providers' financial status to ensure soundness and continuity of business and services.
   - Prescribed additional qualifications and prohibited characteristics of executive board members.
   - Expanded the scope of e-Money services to include, for instance, foreign currency e-Money for usage abroad, undertaking of other businesses that support e-Payment operation by obtaining approval from the BOT prior to such undertaking. Moreover, the BOT also required service providers to maintain the ratio of net shareholders' equity to outstanding balance of deferred revenue to manage risks to financial status and soundness.

2) Revised rules, procedures, and conditions for supervision under the Notification of the Ministry of Finance on Business that Requires a Permit According to Section 5 of the Notification of the Revolution Council No. 58 (e-Money businesses) to be more appropriate and in line with changes in economic environment, ensure more efficient risk management by service providers, and comply with notifications of the ETC. Examples included additional qualifications and prohibited characteristics of executive board members, expansion of business scope, and reporting of open/move/close of branches. The revised notifications

of the Ministry of Finance and the BOT were published in the Government Gazette dated 28 June 2016 and 2 August 2016 respectively.

3) Drafted the Royal Decree on Regulating Electronic Payment Services Business of Specialized Financial Institutions B.E. 2559 (2016) to be a sub-law under the Electronic Transactions Act B.E. 2544 (2001) to supervise e-Payment services of Specialized Financial Institutions (SFIs) to ensure alignment of service standards to those of bank and non-bank e-Payment service providers. The draft was prepared according to instructions of the ETC. It was approved by the Cabinet and published in the Government Gazette dated 30 March 2016 and would become effective on 28 July 2016 onwards. Currently, the BOT is in the process of formulating related notifications and regulations to supervise e-Payment services of SFIs pursuant to the abovementioned Royal Decree.

3.2 Supervision and examination of e-Payment service providers

The BOT supervises e-Payment service providers to ensure sound risk management in the provision of financial transaction services, foster reliable and safe e-Payment services, and enhance the business sector's competitiveness and the public sector's services. In this regard, the BOT supervises key e-Payment service providers according to various legislations, including e-Money service providers according to the Notification of the Revolution Council No. 58 (e-Money businesses) and the Royal Decree on Regulating Electronic Payment Services B.E. 2551 (2008).

3.2.1 Supervision According to Notification of the Ministry of Finance on Business that Requires a Permit According to Section 5 of the Notification of the Revolution Council No. 58 (e-Money businesses)

The BOT supervises e-Money service providers that are non-banks as authorized by the Notification of the Ministry of Finance on Business that Requires a Permit According to Section 5 of the Notification of the Revolution Council No. 58 (e-Money businesses), dated 4 October 2004.

In 2015, there were four applications for e-Money license to offer e-Money services on mobile phone applications for payment of goods and services at participating retailers and online. At the end of 2015, there were a total of 12 e-Money service providers licensed under the Notification of the Revolution Council No. 58.

3.2.2 Supervision According to the Royal Decree on Regulating Electronic Payment Service Business, B.E. 2551 (2008)

The BOT has a legal mandate to supervise e-Payment service providers according to the Royal Decree on Regulating Electronic Payment Services Business B.E. 2551 (2008), which is a sub-law under the Electronic Transactions Act B.E. 2544 (2001). According to the Royal Decree, there are three categories of supervisory levels, namely, List A for businesses that are required to notify the BOT, List B for businesses that are required to register with the BOT, and List C for businesses that are required to acquire licenses before providing services. In 2015, the BOT supervised e-Payment service providers according to the Royal Decree as follows.

1) Considered that the applications from List A and List B applicants appropriately met the requirements as stipulated by the legislations and issued List A notifications and List B registrations. Considered the applications for List C licenses before passing recommendations to the ETC for approval. During 2015, there were issuances of one List A notification, one List B registration, and 13 List C licenses. Most of these were payment gateway service providers, e-Money service providers, and bill payment service providers. However, there were one cancellation on List B registration and three cancellations on List C license.

Figure 8: e-Payment service providers

List A — 1 Non-bank

	Bank	Non-Bank	Total
A e-Money	-	1	1
Total (notifications)	-	1	1
Total (operators)	-	1	1

List B — - Banks, 9 Non-banks

	Bank	Non-Bank	Total
B (1) Credit card network	-	-	-
B (2) EDC network	-	-	-
B (3) Switching	-	4	4
B (4) e-Money	-	5	5
Total (notifications)	-	9	9
Total (operators)	-	9	9

List C — 31 Bank, 62 Non-bank

	Bank	Non-Bank	Total
C (1) Clearing	-	3	3
C (2) Settlement	3	-	3
C (3) e-Payment	31	45	76
C (4) Switching	-	3	3
C (5) Bill Payment	19	21	40
C (6) e-Money	8	12	20
Total (notifications)	61	84	145
Total (operators)	31	62	93

Source: Bank of Thailand

As of 30 December 2015

At the end of 2015, there was one List A service provider, nine List B service providers, and 93[7] List C service providers (31 banks and 62 non-banks, representing the total number of 145 licenses issued).

2) Supervised and conducted off-site examination for compliance with the Royal Decree on Regulating Electronic Payment Services Business B.E. 2551 (2008) and related notifications, monitored users' complaints about service providers, and sought facts on other issues to

[7] List of e-Payment service providers can be found on the BOT's website (https://www.bot.or.th/English/PaymentSystems/ OversightOfEmoney/ListOfEmoney/Pages/eMoneyProvider.aspx)

ensure legal compliance. In 2015, there were reports of non-compliance with promulgated legislations but such issues did not affect the consumers' use of services. The result of oversight activities and the incidences of non-compliance by service providers were reported to the ETC. The concerned service providers were also notified and the issues were promptly addressed.

3) Conducted on-site examinations at offices of e-Payment service providers. In 2015, the BOT conducted on-site examination and observed operations of non-bank e-Payment service providers under List C. The businesses were selected for examination based on their popularity among users, extent of impact on users, financial soundness, and complaints received from users. The BOT examined and assessed service providers' operations in both management of e-Payment services and IT risks perspectives. Findings were reported to service providers to ascertain that improvements are carried out to ensure that services are sufficiently comprehensive and exhaustive, able to be offered continuously and efficiently with satisfactory IT security standards. At the same time, improvements must also address fair treatment of consumers or users and compliance with prescribed laws and regulations, thereby fostering confidence in e-Payment services.