Unofficial Translation
with courtesy of the Association of International Banks
This translation is for convenience of those unfamiliar with Thai language.
Please refer to the Thai text for the official version.

BANK OF THAILAND

26 May 2017 (B.E.2560)

To Manager
BAHTNET user institutions
Member banks of the Electronic Clearing House

No. ThorPorTor. ForChorPor. (31) Wor. 794/2560 Re: Dispatch of the BOT Notification Re: Standard on IT Security Management System for BAHTNET and ICAS Client Computers

Currently risks from cyber threats has gradually increased and may incur losses to financial institutions, either in form of financial losses or loss of reputation, which may, as a result, constitute an impact on people and the overall economy as well as the credibility of settlement system, the Bank of Thailand (BOT) hereby prescribed measures to enhance information security management for important settlement infrastructures, namely BAHTNET and ICAS to be in accordance with international standards. While, formerly in 2015 (B.E.2558), the BOT has arranged for the servers of those systems to be certified to ISO/IEC 27001, and, as that certification is being maintained, the BOT is intended to extend the scope of certification to cover the client computers,

In order to prevent the system from cyber threats in a more comprehensive manner, the BOT thereby requires BAHTNET and ICAS client computers to be certified to ISO/IEC 27001 for information security management within 2018 (B.E.2561), and that certification must be continuously maintained. And, as the BOT has consulted and periodically held meetings with member institutions, this requirement is thereby prescribed, as detailed in 2 BOT Notifications, namely Re: Requirements on Information Security Management System for BAHTNET Client Computers and the Requirements for ICAS Client Computers, as attached herewith.

Please be informed and comply with accordingly.

Best Regards,

(Mr. Permsuk Sutthinoon)
Assistant Governor, Information Technology Group
For Governor

Enclosure 1. The Bank of Thailand Notification No. SorRorKhor. 4/2560 Re: Requirements on Information Security Management System for BAHTNET Client Computers dated 23 May 2017 (B.E.2560)
2. The Bank of Thailand Notification No. SorRorKhor. 5/2560 Re: Requirements on Information Security Management System for ICAS Client Computers dated 23 May 2017 (B.E.2560)

Payment and Bond Department
Tel. 0 2283 5056, 0 2283 5034

Bank of Thailand Notification
No. SorRorKhor. 4/2560
Re: Requirements on Information Security Management System for BAHTNET Client Computers

---

1. Rationale

The Bank of Thailand (BOT) stresses the importance of security risks of data, systems and networks involving funds transfer through the BAHTNET system, which is one of the important payment infrastructure of the country, and deems that ISO/IEC 27001 is the standard that emphasizes on maintaining and promoting security of the IT system of the organization and can be applied as the guidelines for auditing and maintaining information system security.

The BOT hereby issues this Notification to require BAHTNET client computers to be certified to ISO/IEC 27001, which will enhance the security of BAHTNET client computers to ensure the integrity and availability of the service in accordance with international standards.

2. Statutory Power

By virtue of Clause 15 of the Bank of Thailand Regulation Re: BAHTNET Services B.E.2549 (2006)

3. Scope of Application

This Notification shall apply to BAHTNET users according to the Bank of Thailand Regulation Re: BAHTNET Services

4. Contents

Clause 1 In this Notification

"Client computer" refers to the computer system of a BAHTNET user, either used for day-to-day operations or used as a backup system, that is connected to the BOT's BAHTNET system, namely the computer system for electronic financial services (EFS) or the computer system for sending/receiving data directly to/from the BOT's Server (Host-to-host connection), excluding the SWIFT computer system.

"Independent auditor" refers to an auditor for IT works, which may be an internal auditor who is independent from a unit responsible for IT works (IT unit) and a unit responsible for IT risk management (IT risk management unit), or external auditor with capability to perform an audit of information security management system according to ISO/IEC 27001 (Information security management) and is certified or receives a certificate in information security that is internationally accepted, such as Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Security Professional (CISSP).

"Certification body" refers to an organization that performs an assessment of information security management system according to ISO/IEC 27001.

"Assessment" refers to an assessment of information security management system according to ISO/IEC 27001 by an independent auditor.

"Certification" refers to the certification of information security management system according to ISO/IEC 27001 by a certification body.

Clause 2 BAHTNET users must manage to have their BAHTNET client computers certified under any of the following approaches:

(1) certified within 2017 (B.E.2060)

(2) assessed within 2017 (B.E.2560) and certified within 2018 (B.E.2561)

For institutions participating in the BAHTNET system after the effective date of this Notification, those institutions must manage to have their client computers assessed within 180 days from the date of participation in the BAHTNET system, and those client computers must be certified within 1 year from the assessment date.

On this, when BAHTNET users have carried out those as specified in the first paragraph or the second paragraph, as the case may be, they shall submit the assessment/certification documents to the BOT promptly.

Clause 3 BAHTNET users must continuously maintain the ISO/IEC 27001 certification for information security management system for their client computers, which has been granted by the certification body according to Clause 2.

On this, the certification documents as specified in the first paragraph must be submitted to the BOT promptly.

Clause 4 If any BAHTNET user cannot carry out those as specified in Clause 2 or Clause 3, that BAHTNET user shall submit a request for relaxation of requirements, by specifying reasons and details of necessity, resolution frameworks and timeframe, to the BOT promptly. The BOT reserves the right to extend/not to extend the specified time limit as deemed appropriate.

5. Effective Date

This Notification shall come into effect from the announcement date onwards.

Announced on 23 May 2017 (B.E.2560)

(Mr. Veerathai Santipraphob)
Governor
Bank of Thailand

Payment and Bond Development Team 1
Payment and Bond Department
Tel. 0 2283 5056

Bank of Thailand Notification
No. SorRorKhor. 5/2560
Re: Requirements on Information Security Management System for ICAS Client Computers

---

1. Rationale

The Bank of Thailand (BOT) stresses the importance of security risks of data, systems and networks involving the Imaged Cheque Clearing and Archive System (ICAS), which is one of the important payment infrastructure of the country, and deems that ISO/IEC 27001 is the standard that emphasizes on maintaining and promoting security of the IT system of the organization and can be applied as the guidelines for auditing and maintaining information system security.

The BOT hereby issues this Notification to require ICAS client computers to be certified to ISO/IEC 27001, which will enhance the security of ICAS client computers to ensure the integrity and availability of the service in accordance with international standards.

2. Statutory Power

By virtue of Clause 1 of the Bank of Thailand Regulation No. SorRorKhor. 1/2554 Re: Imaged Cheque Clearing and Archive System

3. Scope of Application

This Notification shall apply to member banks according to the Bank of Thailand Regulation Re: Imaged Cheque Clearing and Archive System

4. Contents

Clause 1 In this Notification

"Client computer" refers to the computer system with installed equipment and software for the use of ICAS and electronic financial services of a member bank, either used for day-to-day operations or used as a backup system, that is connected to the BOT's ICAS system, namely the Imaged Cheque Member Gateway (ICMG) and the computer system for the use of ICAS through electronic financial services (EFS).

"Independent auditor" refers to an auditor for IT works, which may be an internal auditor who is independent from a unit responsible for IT works (IT unit) and a unit responsible for IT risk management (IT risk management unit), or external auditor with capability to perform an audit of information security management system according to ISO/IEC 27001 (Information security management) and is certified or receives a certificate in information security that is internationally accepted, such as Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Security Professional (CISSP).

"Certification body" refers to an organization that performs an assessment of information security management system according to ISO/IEC 27001.

"Assessment" refers to an assessment of information security management system according to ISO/IEC 27001 by an independent auditor.

"Certification" refers to the certification of information security management system according to ISO/IEC 27001 by a certification body.

Clause 2 Member banks must manage to have their ICAS client computers certified under any of the following approaches:

(1) certified within 2017 (B.E.2060)

(2) assessed within 2017 (B.E.2560) and certified within 2018 (B.E.2561)

For institutions participating in the ICAS system after the effective date of this Notification, those institutions must manage to have their client computers assessed within 180 days from the date of participation in the ICAS system, and those client computers must be certified within 1 year from the assessment date.

On this, when member banks have carried out those as specified in the first paragraph or the second paragraph, as the case may be, they shall submit the assessment/certification documents to the BOT promptly.

Clause 3 Member banks must continuously maintain the ISO/IEC 27001 certification for information security management system for their client computers, which has been granted by the certification body according to Clause 2.

On this, the certification documents as specified in the first paragraph must be submitted to the BOT promptly.

Clause 4 If any member bank cannot carry out those as specified in Clause 2 or Clause 3, that member bank shall submit a request for relaxation of requirements, by specifying reasons and details of necessity, resolution frameworks and timeframe, to the BOT promptly. The BOT reserves the right to extend/not to extend the specified time limit as deemed appropriate.

5. Effective Date

This Notification shall come into effect from the announcement date onwards.

Announced on 23 May 2017 (B.E.2560)

(Mr. Veerathai Santipraphob)
Governor
Bank of Thailand

Payment and Bond Development Team 1
Payment and Bond Department
Tel. 0 2283 5056