NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 36 00
sss@nbb.be

2 July 2018

NBBSSS/2018/144

Information security self-certification questionnaire for NBB-SSS participants

Dear Participant,

With the present letter, the NBB-SSS is inviting you to confirm, by means of the attached **self-certification statement**, that information security measures are in place within your organisation and implemented in compliance with the requirements described in the self-certification statement, in accordance with the NBB-SSS T&C Art. 7.4.7. The current note provides guidance how the self-certification questionnaire should be completed.

The completed statement in attachment shall be signed by a senior executive from business and IT side and subsequently returned by surface mail to the NBB-SSS at the latest by Friday 31 August 2018. The NBB-SSS User Committee will be debriefed at its meeting on 3 September 2018.

Upon receipt, the self-certification statement will be reviewed by the NBB-SSS and, in the event that a case of non-compliance or partly compliance is reported, bilateral discussions will take place with a view to remedy the situation.

Should you have any further questions, please do not hesitate to contact the NBB-SSS (sss@nbb.be or tel. +32 2 221 36 00).

Kind regards,

Koen Geenen - David De Vleeschouwer
Co-Head of NBB-SSS
NBB-SSS - National Bank of Belgium
de Berlaimontlaan 14 BE-1000 Brussels
www.nbbsss.be

1. Introduction

The Principles for Financial Market Infrastructures set out certain responsibilities that must be fulfilled by Financial Market Infrastructures. More specifically, Principle 17 relates to issues concerning the security and operational reliability of Financial Market Infrastructures such as CSD/SSS.

Principle 17 states that *"…an FMI should consider establishing minimum operational requirements for its participants. For example, an FMI may want to define operational and business continuity requirements for participants in accordance with the participant's role and importance to the system."*

The NBB-SSS Terms & conditions v. 03/2018 Art. 7.4.7 impose on Participants to provide a self-certification statement upon request from the NBB-SSS in order to ensure the security and operational reliability of the participants' infrastructures and their interfaces with the NBB-SSS and with the T2S platform.

The self-certification statement assesses whether the participant has reliable and effective contingency and business continuity arrangements in place, and whether the participant has implemented reliable and effective information security measures. The self-certification template holds requirements and criteria which are based upon the ISO/IEC 27002 standard and pre-defined by the NBB-SSS.

The self-certification statement must be renewed on an annual basis and the respective form must be signed by senior executives from the business side and from the IT side.

The current note provides guidance how the self-certification questionnaire should be completed.

2. Security requirements for NBB-SSS participants

In the following the security requirements for NBB-SSS Participants are specified. Taking into account that the set-up of the internal systems used by participants for submitting transactions to NBB-SSS / T2S may vary significantly, the requirements are purposely defined at a high level. However, the security requirements are considered to be best practice and should hence be generally applicable. Eventually it is up the individual organisations to assess whether all or only subsets of the security requirements are applicable to them. In this respect, it is recalled that it is ultimately the responsibility of those signing the self-certification statement to make sure that it reflects a true and accurate picture of the security situation of their organisation.

Requirement 1: Human resources security

Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs. Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities. An adequate level of awareness should be ensured among all employees, contractors and third party users, and education and training in security procedures and the correct use of information processing facilities should be provided to them, to minimise possible security risks.

Requirement 2: Asset management

All organisational assets should be accounted for and have a nominated owner. The responsibility for the maintenance of appropriate controls should be assigned.

Requirement 3: Access control

Access to information, information processing facilities and business processes should be controlled on the basis of business and security requirements. Access control rules should take account of policies for information dissemination and authorisation.

Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final deregistration of users that no longer require access.

Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights which allow users to override system controls.

Users should be made aware of their responsibility for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

Access to both internal and external networked services should be controlled. User access to networks and network services should not compromise the security of the network services, i.e. it should be ensured that appropriate interfaces are in place between the organisation's network and networks owned by other organisations and public networks, appropriate authentication mechanisms are applied for users and equipment, and controls of user access to information services are enforced.

Security facilities should be used to restrict access to operating systems to authorised users. The facilities should be capable of authenticating authorised users, recording successful and failed system authentication attempts, recording the use of special system privileges, issuing alarms when system security policies are breached, providing appropriate means for authentication and, where appropriate, restricting users' connection times.

Logical access to application software and information should be restricted to authorised users. When mobile computing is used, the risks of working in an unprotected environment should be considered and appropriate protection applied.

In the case of teleworking the organisation should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

Requirement 4: Physical and environmental security

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference.

Requirement 5: Operations management

Responsibilities and procedures should be established for the management and operation of all information processing facilities.

As regards operating procedures, segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

The operational requirements of new systems should be established, documented and tested prior to their acceptance and use. Precautions must be taken to prevent and detect the introduction of malicious code and unauthorised mobile code. Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses and logic bombs, and users should be made aware of its dangers. Managers should, where appropriate, introduce controls to prevent, detect and remove malicious code and control mobile code.

Routine procedures should be established to implement the agreed backup policy and strategy for taking backup copies of data and rehearsing their timely restoration.

The secure management of networks, which may span organisation boundaries, requires careful consideration to be given to dataflow, legal implications, monitoring and protection. Additional controls may also be required to protect sensitive information passing over public networks. Data storage media should be controlled and physically protected.

Appropriate operating procedures should be established to protect documents, computer media, input/output data and system documentation from unauthorised disclosure, modification, removal and destruction.

Exchanges of information and software between organisations should be based on a formal exchange policy and carried out in line with exchange agreements, and should be compliant with any relevant legislation. Procedures and standards should be established to protect information and physical media containing information in transit.

Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure that information system problems are identified.

System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

Requirement 6: Information systems acquisition, development and maintenance

Information systems include operating systems, infrastructures, business applications, off-the-shelf products, services and user-developed applications. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.

Appropriate controls should be built into applications, including user-developed applications, to ensure correct processing. These controls should include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive,

valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.

A policy should be developed on the use of cryptographic controls to protect the integrity of information. Key management should be in place to support the use of cryptographic controls. Access to system files and program source code should be controlled and IT projects and support activities conducted in a secure manner.

Technical vulnerability management should be implemented in an effective, systematic and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems and any other applications in use.

Requirement 7: Information security in supplier relationships

To ensure protection of the participant's internal component system used for operating with NBB-SSS / T2S that is accessible by suppliers, information security requirements for mitigating the risks associated with supplier's access to the participant's internal component system should be agreed with the supplier and documented.

Requirement 8: Management of information security incidents and improvements

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses, management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

Requirement 9: Technical compliance review

A participant's internal component system used for operating with NBB-SSS / T2S (i.e. back office systems, internal networks and external network connectivity infrastructure) should be regularly reviewed for compliance with the organization's information security policies and standards.

3. Compliance check

For each of the requirements listed in the previous section the NBB-SSS participant shall report its level of compliance in the annex to this self-certification statement.

In the event of non-compliance at level 2 or level 3 with the above-mentioned requirements, a description of the major risks[1] should be included in the annex. Furthermore, an action plan for rectifying the situation and the planned dates for implementing each particular measure should be included. This information shall be evaluated and the implementation of risk-mitigating measures monitored by the NBB-SSS.

Contact details

In the following the name and contact details of a person to be contacted in case further information is required shall be provided.

Name of the participant	
Address	
Contact person (name) (print)	
Contact person (telephone)	
Contact person (e-mail)	

Signatory

The self-certification statement shall be signed by a senior official (i.e. at board level or equivalent) responsible for the relevant business area within the critical participant. Given the heavy reliance on information technology (IT), the self-certification statement shall, in addition, be signed by a senior official (also at board level or equivalent) responsible for the IT department within the organisation of the participant. If a senior official is responsible for both, the business area and the IT department, one signature is sufficient.

Certification

The signatories confirm that they have read and understood the requirements outlined in this self-certification statement. The statement (including the annex) is valid for one year and is due for renewal one year after the date of the first signature.

The signatories certify that the information contained in the annex represents a true and accurate picture of the current situation. They further certify that the annex has been prepared under their direction and

[1] A major risk could be, for instance, insufficient measures against denial of service attacks, uninterruptible power supply not in place, etc.

supervision and that qualified personnel properly gathered and evaluated the information provided. The submitted information is, to the best of the signatories' knowledge and belief, true, accurate and complete. The signatories are aware that the submission of this information is a material obligation and that submitting false, inaccurate or misleading information constitutes a breach of NBB-SSS Terms & conditions v.03/2018 Article 10.7 (iii) which is one of the grounds for termination of an institution's participation in NBB-SSS.

Finally, the signatories confirm that their organisation has a mechanism in place to ensure that it will remain in compliance over the coming year or, if compliance has not yet been achieved, that appropriate measures will be taken to make satisfactory progress on the work items listed in the action plan.

First signature

Name of official from the business area (print)	
Title	
Date	
Signature	

Second signature

Name of official from IT department (print)	
Title	
Date	
Signature	

This form (including the annex) shall be returned to

NBB-SSS
NBB - Payments and Securities Service
Attn. Koen Geenen – David De Vleeschouwer
boulevard de Berlaimont 14
BE-1000 Brussels

Annex to the self-certification statement for NBB-SSS participants

Your Participant BIC11: ……

If you are the service provider for other Participants, please add those BICs as well.

1. **Level of compliance**

NBB-SSS Participants are required to indicate their level of compliance with the requirements regarding information security management specified by the NBB-SSS.

The participant shall indicate its level of compliance by ticking the appropriate box.

- **Full compliance:** the participant fully complies with requirement as described in the self-certification statement.
- **Levels of non-compliance**
    - **Level 1:** no significant areas of non-compliance; reasonable assurance can be given that this does not have the potential to harm the smooth functioning of NBB-SSS / T2S and/or adversely affect other system participants.
    - **Level 2:** significant areas of non-compliance; reasonable assurance cannot be given, and an exploitation of the vulnerabilities identified could harm the smooth functioning of NBB-SSS / T2S and/or adversely affect other system participants.
    - **Level 3:** non-compliance; reasonable assurance cannot be given, and an exploitation of the vulnerabilities identified would significantly harm the smooth functioning of NBB-SSS / T2S and/or adversely affect other system participants

Information security management requirements	Full compliance	Non-compliance		
		Level 1	Level 2	Level 3
Requirement 1	☐	☐	☐	☐
Requirement 2	☐	☐	☐	☐

Requirement 3	☐	☐	☐	☐
Requirement 4	☐	☐	☐	☐
Requirement 5	☐	☐	☐	☐
Requirement 6	☐	☐	☐	☐
Requirement 7	☐	☐	☐	☐
Requirement 8	☐	☐	☐	☐
Requirement 9	☐	☐	☐	☐
Which information security standard is mainly used for security controls?				

2. Towards compliance

If any areas of non-compliance at level 2 or level 3 have been identified, the following section shall be completed.

Have any risks resulting from non-compliance at level 2 or level 3 with requirements 1 to 9 been identified? Comments:
What steps will be taken to achieve full compliance or reduce non-compliance to level 1? Comments:
By when will full compliance or non-compliance at level 1 be achieved? Comments: