BANK OF RUSSIA STANDARD

STO BR IBBS-1.2-2014

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

ASSESSMENT METHOD FOR COMPLIANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS WITH REQUIREMENTS OF STO BR IBBS-1.0-2014*

Date enacted: 1 June 2014

Official publication

Moscow
2014

Foreword

- ADOPTED AND ENACTED by the Bank of Russia Directive No. P-399, dated 17 May 2014.

- REPLACES STO BR IBBS-1.2-2010.

*In case of any translation ambiguity the Russian version shall prevail.

Table of Contents

Introduction

To check the level of information security (IS) both in the Bank of Russia and the organisations of the banking system (BS) of the Russian Federation (RF), the Bank of Russia standard STO BR IBBS-1.0-2014 'Maintenance of Information Security of the Russian Banking System Organisations. General Provisions' defines the requirements for regular IS audit and IS self-assessment.

This standard establishes the methods for determining the degree of compliance with the requirements of the Bank of Russia standard STO BR IBBS-1.0-2014 'Maintenance of Information Security of the Russian Banking System Organisations. General Provisions', as well as the final level of IS conformity to the requirements of the Bank of Russia standard STO BR IBBS-1.0-2014 ' Maintenance of Information Security of Organisations of the Russian Banking System Organisations. General Provisions' during the IS audit and IS self-assessment.

BANK OF RUSSIA STANDARD

MAINTENANCE OF

INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

ASSESSMENT METHOD FOR COMPLIANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS WITH REQUIREMENTS OF STO BR IBBS-1.0-2014

Date enacted: 1 June 2014

1. Scope of Application

This standard applies to RF BS organisations as well as to organisations assessing IS conformity of a RF BS organisation to the requirements of Bank of Russia standard STO BR IBBS-1.0-2014 'Maintenance of Information Security of the Russian Banking System Organisations. General Provisions' (hereinafter referred to as STO BR IBBS-1.0).

This standard is recommended to be used by including references to it and/or direct use of its provisions in the internal documents of RF BS organisations, as well as in the contract documents that establish the relationship of the parties in conducting external assessments of IS compliance.

The provisions of this standard shall apply on a voluntary basis, unless some specific provisions are made binding by the applicable laws of the Russian Federation, regulatory acts of the Bank of Russia or the terms of contracts.

2. Regulatory References

This standard uses the regulatory references to STO BR IBBS-1.0.

3. Terms and Definitions

This document uses the terms in accordance with STO BR IBBS-1.0, Bank of Russia standard STO BR IBBS-1.1-2007 'Maintenance of Information Security of the Russian Banking System Organisations. Information Security Audit', as well as the following terms with their corresponding definitions:

3.1. **"Information security indicator"** means a measure or characteristic for assessing information security.

3.2. **"Auditing organisation"** means the organisation assessing IS conformity in a RF BS organisation to the requirements of STO BR IBBS-1.0.

3.3. **"Audited organisation"** means a RF BS organisation whose IS is being assessed for conformity to the requirements of STO BR IBBS-1.0.

4. Symbols and Abbreviations

ABS – automated banking system;
BS – banking system;
LC – life cycle;
IS –information security;
ISPD –information system of personal data;

UA – unauthorised access;
URA – unregulated activities within the delegated authority;
RF – the Russian Federation;
DET –data encryption tool;
IS Management System – information security management system;
ISS – information security system;
IS Maintenance System – information security maintenance system;
ECM – computer;
ES – electronic signature;
EV_1 – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 in the area "current IS level in the organisation";
EV_2 – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 in the area "IS management in the organisation";
EV_3 – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 in the area "IS awareness level in the organisation";
$EV_{OPDProc}$ – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 regulating personal data processing;
$EV'_{OPDProt}$ – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 regulating personal data protection without considering the degree of compliance with STO BR IBBS-1.0 in ensuring information security when using data encryption tools;
$EV^2_{OPDProt}$ – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 regulating personal data protection including the degree of compliance with STO BR IBBS-1.0 in ensuring information security when using data encryption tools;
EV_{BITP} – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 regulating bank information process;
EV_{BPTP} – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 regulating bank payment process;
EV_{Mi} – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 for group indicator;
EV_{Mij} – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 for individual indicator;
i – number of group indicator;
j – number of individual indicator;
M_{ij} – symbol of individual indicator;
R – total level of conformity of IS in a RF BS organisation to the requirements of STO BR IBBS-1.0.

5. General provisions

5.1. The purpose of this procedure is standardisation of approaches and methods used for assessing IS conformity in a RF BS organisation to requirements of STO BR IBBS-1.0 in the following assessment areas:

- Current IS level in the organisation;
- IS Management in the organisation;
- IS awareness level in the organisation.

5.2. The objectives of this procedure are as follows:

- To determine IS indicators and the methods for their assessment;
- To determine the method for assessing the current IS level in an organisation by determining the degree of compliance with the requirements specified in section 7 of STO BR IBBS-1.0;
- To determine the method for assessing IS management in and organisation and IS awareness level of an organisation by determining the degree of compliance with the requirements specified in section 8 of STO BR IBBS-1.0;
- To determine the total level of IS conformity in an organisation to the requirements of STO BR IBBS-1.0.

6. Information Security Indicators. Methods for Assessing the Indicators

6.1. The group and private IS indicators are used to assess the degree of IS conformity in a RF BS organisation to the requirements of STO BR IBBS-1.0. IS group indicators form the structure of assessment areas by providing the details on the assessment of the current IS level in an organisation, IS management and level of IS awareness. The assessments of group indicators *(EV_{Mi})* are used to obtain the assessments by areas *(EV_1, EV_2 и EV_3).* The individual IS indicators are part of the group indicators and are presented in the form of questions, the answers to which make it possible to determine the assessments (EV_{Mij}), which then form the assessments *EV_{Mi}* of the group indicators.

Annex A includes the forms to be completed during assessment. Each form includes a IS group indicator and IS private indicators included in the group indicator.

6.2. Individual indicators are divided into two types. The first type includes individual indicators reflecting the requirements of STO BR IBBS-1.0, which are mandatory for compliance in the organisation. The second type includes individual indicators reflecting the requirements of STO BR IBBS-1.0, which are recommended for compliance in the organisation. Information on inclusion of individual indicators into these types is defined in the forms of Annex A.

6.3. The method used for assessing the individual indicator depends on its inclusion into one of the types defined in clause 6.2 of this methodology.

6.4. The assessment of individual indicator *EV_{Mij}* is based on the degree of compliance with the requirements identified by the auditing group through expert assessment.

The assessment of the individual indicator shall be accompanied by entering a symbol, such as "X" in the appropriate box of the forms provided in Annex A.

6.5. The following scale of compliance is established for individual indicators, which are mandatory for compliance (first type):

- “No” – the assessment is assigned with the value equal to zero;
- “Partially” – the assessment is assigned with value of either 0.25, 0.5 or 0.75;
- “Yes” – the assessment is assigned with the value equal to one;

If the individual indicator is designed for assessing requirements that do not apply to the activities of the organisation or are not relevant for the organisation at the time of assessment, which is recorded in the documents of the organisation, then this individual indicator is defined as non-assessed (please mark the box "N/A" – no assessment) and is not considered in further assessment results.

6.6. The following scale of compliance is established for individual indicators which are recommended for compliance (second type):

- “Yes” – the assessment is assigned with the value equal to one;
- “No” – the individual indicator is defined as non-assessed (please mark the box "N/A" – no assessment) and is not considered in further assessment results.

6.7. The following general approach is used when assessing the individual indicators which are evaluated both for degree of their establishment (determination) in the RF BS organisation and the degree of compliance (individual indicator of audit category 1):

Table 1. Recommended criteria for assessing individual IS indicators that evaluate both the degree of documentation and the degree of compliance with IS requirements

Assessment of individual IS indicator	Criteria for assessing the individual IS indicator
0	Requirements for individual IS indicator are not established (determined) in the internal documents of the audited organisation
0.25	Requirements for individual IS indicator are established (determined) in the internal documents of the audited organisation but are not complied with
0.5	Requirements for individual IS indicator are established (determined) in the internal documents of the audited organisation but are not fully complied with

Assessment of individual IS indicator	Criteria for assessing the individual IS indicator
0.75	Requirements for individual IS indicator are established (determined) in the internal documents of the audited organisation and are almost fully complied with
1	Requirements for individual IS indicator are established (determined) in the internal documents of the audited organisation and are fully complied with

6.8. The following general approach is used when assessing the individual indicators that evaluate only the degree of documentation (individual indicator of audit category 2):

Table 2. Recommended criteria for assessing the individual IS indicators that evaluate only the degree of documentation of IS requirements

Assessment of individual IS indicator	Criteria for assessing the individual IS indicator
0	Requirements for individual IS indicator are not established in the internal documents of the audited organisation
1	Requirements for individual IS indicator are fully established in the internal documents of the audited organisation

6.9. The following general approach is used when assessing the individual indicators that evaluate only the degree of compliance (individual indicator of audit category 3):

Table 3. Recommended criteria for assessing the individual IS indicators that evaluate only the degree of compliance of IS requirements

Assessment of individual IS indicator	Criteria for assessing the individual IS indicator
0	Requirements of the individual IS indicator are not complied with
0.5	Requirements of the individual IS indicator are not fully complied with
1	Requirements of the individual IS indicator are fully complied with

6.10. In cases where a limited set of objects included in the area selected for IS assessment is used in the assessment of the individual indicator (e.g., limited ABS sample), and the assessment of the individual indicator produces results indicating full compliance or complete non-compliance/full documentation or absence of documentation of the relevant IS requirements, it is recommended to expand the set of these objects (sample) to confirm or correct the obtained results.

6.11. The assessment of the individual IS indicator shall be based on evidence. It is recommended to use the following as the main source of evidence:

- Documents of the audited organisation and, when necessary, the documents of third parties related to ensuring IS of the organisation;
- Verbal statements from employees of the audited organisation made during interviews;
- Results of observations on the activities of employees of the audited organisation made by the members of the audit team.

During the verbal interviews of employees of the audited organisation and observations on the activities of these employees, the members of the audit team shall reach a conclusion on the degree of conformity of the assessed activities to the requirements of internal documents of the audited organisation.

The evidence obtained for the assessment of IS conformity and its sources shall be documented by preparing the sheets for collecting evidence for assessment of IS conformity, an example of which is provided in Annex B. When completing the sheets for collecting evidence for

assessment of IS conformity, specify the references to relevant internal documents of the audited organisation, the results of interviews conducted with the employees of the audited organisation, as well as the results of observations made by members of the audit team. The results of interviews and observations shall be confirmed by the signature of the interviewed employee of the organisation and the member of the audit team, respectively.

6.12. The assessment of the group indicator (EV_{Mi}) is calculated from the assessments of individual indicators (EV_{Mij}) included in this group indicator:

$$EV_{Mi} = \frac{\sum_{j} EV_{Mij}}{j}.$$

6.13. If all individual indicators within a group indicator are defined as non-assessed, the specified group indicator is also defined as non-assessed and not considered in preparing any further results of assessment. In this case, the group indicator is not considered in the calculation formulas used for EV_{BITP}, EV_{BPTP}, $EV_{OPDProc}$, $EV_{OPDProt}$, $EV_{OPDProt}$, EV_1, EV_2 and EV_3 (see sections 7, 8, 9) with a corresponding correction in the formulas used for calculating the number of assessed group indicators. The assessments for such group indicators are not shown in the circular diagram (see. section 11).

7. Assessing the Current Level of Information Security of Organisations of the Banking System of the Russian Federation

7.1. The assessment of the current IS level in an organisation is determined by IS group and individual indicators that make it possible to evaluate the degree of compliance with IS requirements of STO BR IBBS-1.0 in the following areas:

- Ensuring IS in assigning and allocating roles and ensuring confidence in personnel;
- Ensuring IS at the stages of ABS life cycle;
- Ensuring IS in access control and registration;
- Ensuring IS by antivirus protection tools;
- Ensuring IS when using Internet resources;
- Ensuring IS when using data encryption tools;
- Ensuring IS of bank payment technological processes;
- Ensuring IS of bank information processes;
- Personal data processing in a RF BS organisation;
- Ensuring IS of banking processes used for personal data processing.

7.2. The group indicators used for the assessment area "current IS level in the organisation" reflect the aggregate of IS requirements for the areas defined in section 7 of STO BR IBBS-1.0. Table 4 shows the conformity between the structural elements of STO BR IBBS-1.0 containing IS requirements and IS group indicators designed to audit the implementation of these requirements.

Table 4. Conformity of IS group indicators to the aggregate of IS requirements for the areas defined in section 7 of STO BR IBBS-1.0

IS group indicator	IS group indicator name	Structural element of STO BR IBBS-1.0
M1	- Ensuring IS in assigning and allocating roles and ensuring confidence in personnel	Clause 7.2
M2	Ensuring IS at the stages of ABS life cycle	Clause 7.3
M3	Ensuring IS in access control and registration	Clause 7.4
M4	Ensuring IS by antivirus protection tools	Clause 7.5
M5	Ensuring IS when using Internet resources	Clause 7.6

IS group indicator	IS group indicator name	Structural element of STO BR IBBS-1.0
M6	Ensuring IS when using data encryption tools	Clause 7.7
M7	Ensuring IS of bank payment processes	Clause 7.8
M8	Ensuring IS of bank information processes	Clause 7.9
M9	General requirements for personal data processing in a RF BS organisation;	Clause 7.10
M10	General requirements for ensuring information security of banking processes used for personal data processing	Clause 7.11

7.3. The individual indicators used for the assessment area "current IS level in the organisation" reflect specific IS requirements of STO BR IBBS-1.0 in each area. The individual indicators for assessment area "current IS level in the organisation" (indicators M1 ÷ M10) in Annex A.

7.4. The individual indicators within the group indicators M1 ÷ M6 must be assessed separately based on the analysis of compliance with the relevant requirements of STO BR IBBS-1.0 in the following areas:

- Bank payment process (M7);
- Bank information process (M8);
- Banking process used for personal data processing (M10).

7.5 The assessments EV_{Mij} and EV_{Mi} obtained following the assessment of group indicators of IS M1 ÷ M10 are entered in corresponding boxes of forms provided in Annex A.

7.6. The individual indicators within the group indicators M1-M7 for the bank payment process shall be assessed by considering the up-to-date results of the last assessment for compliance of the organisation with the requirements to ensure data protection for money transfers established by the Regulations of the Bank of Russia No. 382-P 'On the Requirements for the Protection of Money Transfer Data and the Procedure for the Bank of Russia to Exercise Control over Compliance with the Requirements for the Protection of Money Transfer Data' of 9 June 2012 (hereinafter, the "Regulations of the Bank of Russia No. 382-P of 9 June 2012") and used to calculate the total indicator $EV1_{PS}$ established by the Regulations of the Bank of Russia No. 382-P of 9 June 2012.

The table of conformity of individual indicators and requirements for data protection of money transfers specified in Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012 and considered in the assessment of individual indicators is provided in Annex B.

To assess the individual indicators by considering the results of assessing the compliance of an organisation with the requirements for data protection for money transfers established by the Regulations of the Bank of Russia No. 382-P of 9 June 2012 , use the approach established in clauses 6.7, 6.8 and 6.9 hereof while taking into account that the assessment of an individual indicator may not exceed the minimum assessment of compliance with the requirements established by the Regulations of the Bank of Russia No. 382-P of 9 June 2012 corresponding to the assessed individual indicator.

7.7. Final assessment EV_1 reflecting the degree of compliance with the requirements of STO BR IBBS-1.0 in the area "current IS level in an organisation" is calculated in accordance with the following formula:

$$EV_1 = \min(EV_{БИТП}, EV_{БПТП}, EV^2_{ОЗПД}, EV_{ООПД}), \text{ где:}$$

EV_{BITP} – degree of compliance with the requirements of STO BR IBBS-1.0 regulating the bank information process;

EV_{BPTP} – degree of compliance with the requirements of STO BR IBBS-1.0 regulating the bank payment process;

$EV_{OPDProt}$ – degree of compliance with the requirements of STO BR IBBS-1.0 regulating personal data protection in personal data information systems including the assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 for information security while using data encryption tools;

$EM_{OPDProc}$ – degree of compliance with the requirements of STO BR IBBS-1.0 regulating personal data processing.

7.8. The degree of compliance with the requirements of STO BR IBBS-1.0 regulating the bank payment process is assessed by calculation as per a formula where the assessments of group indicators M1 ÷ M6 are selected based on the results of their evaluation relative to the bank payment process and by considering the results of assessing the compliance of the organisation with the requirements for data protection for money transfers by the Regulations of the Bank of Russia No. 382-P of 9 June 2012:

$$EV_{БПТП} = k^1_{БПТП} \frac{\sum_i EV_{Mi} + EV_{M7}}{7}, \; i = 1 \div 6,$$

where k^1_{BPTP} is the correction factor determined in accordance with the rules established in section 10.

The degree of compliance with the requirements of STO BR IBBS-1.0 regulating bank information process is assessed by calculation as per a formula where the assessments of group indicators M1 ÷ M6 are selected based on the results of their evaluation relative to the bank information process:

$$EV_{БИТП} = k^1_{БИТП} \frac{\sum_i EV_{Mi} + EV_{M8}}{7}, \; i = 1 \div 6,$$

where k^1_{BPTP} is the correction factor determined in accordance with the rules established in section 10.

The degree of compliance with the requirements of STO BR IBBS-1.0 regulating personal data protection without considering the assessment of compliance with the requirements of STO BR IBBS-1.0 for ensuring IS in using data encryption tools (DETs) is assessed by calculation as per a formula where the assessments of group indicators M1 ÷ M5 are selected based on the results of their evaluation relative to the banking process used to process personal data in ISPD:

$$EV^1_{ОЗПД} = k^1_{ОЗПД_1} \frac{\sum_i EV_{Mi} + EV_{M8} + EV_{M10}}{7}, \; i = 1 \div 5,$$

where $k^1_{OPDProt}$ is the correction factor determined in accordance with the rules established in section 10.

The degree of compliance with the requirements of STO BR IBBS-1.0 regulating personal data protection while considering the assessment of compliance with the requirements of STO BR IBBS-1.0 for ensuring IS in using DET is assessed by calculation as per a formula where the assessments of group indicators M1 ÷ M6 are selected based on the results of their evaluation relative to the banking process used to process personal data in ISPD:

$$EV^2_{ОЗПД} = k^1_{ОЗПД_2} \frac{\sum_i EV_{Mi} + EV_{M8} + EV_{M10}}{8}, \; i = 1 \div 6,$$

where $k^1_{OPDProt}$ is the correction factor determined in accordance with the rules established in section 10.

The degree of compliance with the requirements of STO BR IBBS-1.0 regulating the personal data processing is assessed by calculation as per the formula:

$$EV_{ООПД} = k^1_{ООПД} \cdot EV_{M9},$$

where k_{PDProc} is the correction factor determined in accordance with the rules established in section 10.

7.9. The assessments EV_{Mi} obtained as a result of assessing the group indicators of IS M1 ÷ M10 are shown in the circular diagram (see. section 11) in sectors 1 to 10 by arcs removed from the centre of the circular diagram by a value corresponding to the value of these assessments.

7.10 The assessment is shown in the circular diagram (see section 11) in sectors 1 to 10 by an arc removed from the centre of the circular diagram by the value corresponding to the value of EV_1

8. Assessing the Information Security Management of Organisations of the Banking System of the Russian Federation

8.2. The assessment of IS management in an organisation is determined by IS group and individual indicators that make it possible to evaluate the degree of compliance with IS requirements of STO BR IBBS-1.0 in the following areas:

- Arranging and functioning of IS services in a RF BS organisation;
- Defining/adjusting IS Maintenance System scope;
- Selecting/adjusting the approach to assessing the risks of IS breaches and conducting risk assessments of IS breaches;
- Developing the processing plans for the risks of IS breaches;
- Developing/adjusting the internal documents regulating activities in IS area;
- Adopting by the management of the RF BS organisation the decisions on implementing and operating IS Maintenance System;
- Arranging the implementation processing plans for the risks of IS breaches;
- Developing and arranging the implementation of programmes for training and raising awareness in the area of IS;
- Arranging the detection and response to IS incidents;
- Arranging business continuity and its restoration after interruptions;
- IS monitoring and control of safeguards;
- Conducting IS self-assessment;

Conducting an IS external audit;

- Analysing IS Maintenance System functioning;
- Analysing IS Maintenance System by the management of the RF BS organisation;
- Adopting decisions on tactical improvements of IS Maintenance System;
- Adopting decisions on strategic improvements of IS Maintenance System.

8.2. The group indicators used for the assessment area "IS management in the organisation" reflect the aggregate of IS requirements for the areas defined in section 8 of STO BR IBBS-1.0. Table 5 shows the conformity between the structural elements of STO BR IBBS-1.0 containing IS requirements and IS group indicators designed to audit the implementation of these requirements.

Table 5. Conformity of IS group indicators to IS Management System requirements provided in section 8 of STO BR IBBS-1.0

IS group indicator	IS group indicator name	Structural element of STO BR IBBS-1.0
M11	Arranging and functioning of IS services in a RF BS organisation	Clause 8.2
M12	Defining/adjusting IS Maintenance System scope	Clause 8.3
M13	Selecting/adjusting the approach to assessing the risks of IS breaches and conducting risk assessments of IS breaches	Clause 8.4
M14	Developing the processing plans for the risks of IS breaches	Clause 8.5
M15	Developing/adjusting the internal documents regulating the activities in IS area	Clause 8.6
M16	Adopting by the management of the RF BS organisation the decisions on implementing and operating IS Maintenance System	Clause 8.7
M17	Arranging the implementation of IS Maintenance System deployment plans	Clause 8.8
M18	Developing and arranging the implementation of programmes for training and raising awareness in the area of IS	Clause 8.9
M19	Arranging the detection and response to IS incidents	Clause 8.10
M20	Arranging business continuity and its restoration after interruptions	Clause 8.11

IS group indicator	IS group indicator name	Structural element of STO BR IBBS-1.0
M21	IS monitoring and control of safeguards	Clause 8.12
M22	Conducting IS self-assessment	Clause 8.13
M23	Conducting IS audit	Clause 8.14
M24	Analysing IS Maintenance System functioning	Clause 8.15
M25	Analysing IS Maintenance System by the management of the RF BS organisation	Clause 8.16
M26	Adopting decisions on tactical improvements of IS Maintenance System	Clause 8.17
M27	Adopting decisions on strategic improvements of IS Maintenance System	Clause 8.18

8.3. The individual indicators used for the assessment area "IS management in the organisation" reflect specific IS requirements of STO BR IBBS-1.0 in each area. The individual indicators for assessment area "IS management in the organisation" (indicators M11 ÷ M27) are provided in Annex A.

8.4. The assessments EV_{Mij} and EV_{Mi} obtained following the assessment of group indicators of IS M11 ÷ M27 are entered in corresponding boxes of forms provided in Annex A.

8.5. The individual indicators within the group indicators M11 ÷ M27 shall be assessed by considering the results of assessing the compliance of the organisation with the requirements ensuring data protection for money transfers established by the Regulations of the Bank of Russia No. 382-P of June 9, 2012 and used to calculate the total indicator $EV2_{PS}$ established by the Regulations of the Bank of Russia No. 382-P of 9 June 2012.

The table of conformity of individual indicators and requirements for data protection of money transfers specified in Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012 and considered in the assessment of individual indicators is provided in Annex B.

To assess the individual indicators by considering the results of assessing the compliance of an organisation with the requirements for data protection for money transfers established by the Regulations of the Bank of Russia No. 382-P of 9 June 2012, use the approach established in clauses 6.7, 6.8 and 6.9 hereof while taking into account that the assessment of an individual indicator may not exceed the minimum assessment of compliance with the requirements established by the Regulations of the Bank of Russia No. 382-P of 9 June 2012 corresponding to the assessed individual indicator.

8.6. Final assessment EV_2 reflecting the degree of compliance with the requirements of STO BR IBBS-1.0 in the area "IS management in the organisation" is calculated in accordance with the following formula:

$$EV_2 = k_2 \frac{\sum_{i=11}^{27} EV_{Mi}}{17},$$

where k_2 is the correction factor determined in accordance with the rules established in section 10.

8.7. The assessments EV_{Mi} obtained as a result of assessing the group indicators of IS M11 ÷ M27 are shown in the circular diagram (see. section 11) in sectors 11 - 27 by arcs removed from the centre of the circular diagram by a value corresponding to the value of these assessments.

8.8. The assessment EV_2 is shown in the circular diagram (see section 11) in sectors 11 - 27 by an arc removed from the centre of the circular diagram by the value corresponding to the value of EV_2.

9. Assessing the Level of Information Security Awareness of an Organisation of the Banking System of the Russian Federation

9.1. The assessment of IS awareness in the organisation is determined by IS group and individual indicators of IS that make it possible to evaluate the degree of compliance with IS requirements of STO BR IBBS-1.0 in the following areas:

- Activities of the management of a RF BS organisation aimed at supporting the functioning of the IS service in the organisation;
- Activities of the management of a RF BS organisation aimed at adopting the decisions on implementing and operating IS Maintenance System;
- Activities of the management of a RF BS organisation aimed at supporting IS Maintenance System planning;
- Activities of the management of a RF BS organisation aimed at supporting IS Maintenance System implementation;
- Activities of the management of a RF BS organisation aimed at supporting the IS Maintenance System audit;
- Activities of the management of a RF BS organisation aimed at supporting IS Maintenance System analysis;
- Activities of the management of a RF BS organisation aimed at supporting IS Maintenance System improvement.

9.2. The group indicators used for the assessment area "IS awareness level in the organisation" reflect the aggregate of IS requirements for the areas defined in section 8 of STO BR IBBS-1.0. Table 6 shows the conformity between the structural elements of STO BR IBBS-1.0 containing IS requirements and IS group indicators designed to audit the implementation of these requirements.

Table 6. Conformity of group indicators of IS to requirements provided in section 8 of STO BR IBBS-1.0

IS group indicator	IS group indicator name	Structural element of STO BR IBBS-1.0
M28	Assessment of activities of the management of a RF BS organisation aimed at supporting the functioning of the IS service	Clause 8.2
M29	Assessment of the activities of the management of a RF BS organisation aimed at adopting the decisions on implementing and operating IS Maintenance System	Clause 8.7
M30	Assessment of the activities of the management of a RF BS organisation aimed at supporting IS Maintenance System planning	Clauses 8.3, 8.4, 8.5, 8.6, 8.8
M31	Assessment of the activities of the management of a RF BS organisation aimed at supporting IS Maintenance System implementation	Clauses 8.9, 8.10, 8.11
M32	Assessment of the activities of the management of a RF BS organisation aimed at supporting IS Maintenance System audit	Clauses 8.12, 8.13, 8.14, 8.15
M33	Assessment of the activities of the management of a RF BS organisation aimed at IS Maintenance System analysis	Clause 8.16
M34	Assessment of the activities of the management of a RF BS organisation aimed at IS Maintenance System improvement	Clauses 8.17, 8.18

9.3. The individual indicators used for the assessment area "IS awareness level in the organisation" reflect the specific requirements of STO BR IBBS-1.0 for IS Maintenance System of an organisation related to activities of the organisation's management. The individual indicators for

assessment area "IS awareness level in the organisation" (indicators M28 ÷ M34) are provided in Annex A.

The individual indicators for assessment area "IS awareness level in the organisation" are assessed by considering the results of assessing the compliance of the organisation with the requirements for ensuring data protection for money transfers established by the Regulations of the Bank of Russia No. 382-P of 9 June 2012 and used to calculate the total indicator $EV2_{PS}$ established by the Regulations of the Bank of Russia No. 382-P of 9 June 2012.

9.4. The assessments EV_{Mij} and EV_{Mi} obtained following the assessment of group indicators of IS M28 ÷ M34 are entered in corresponding boxes of forms provided in Annex A.

9.5. Final assessment EV_3 reflecting the degree of compliance with the requirements of STO BR IBBS-1.0 in the area "IS awareness level in the organisation" is calculated in accordance with the following formula:

$$EV_3 = k_3 \frac{\sum_{i=28}^{34} EV_{Mi}}{7},$$

where k_3 is the correction factor determined in accordance with the rules established in section 10.

9.6. The assessments EV_{Mi} obtained as a result of assessing the group indicators of IS M28 ÷ M34 are shown in the circular diagram (see. section 11) in sectors 28 - 34 by arcs removed from the centre of the circular diagram by the value corresponding to the value of these assessments.

9.7. The assessment EV_3 is shown in the circular diagram (see section 11) in sectors 28 - 34 by an arc removed from the centre of the circular diagram by the value corresponding to the value of EV_3.

10. Rules for Determining Correction Factors

Correction factors k^1_{BPTP}, k^1_{BITP}, $k'_{OPDProt}$, $k^1_{OPDProt2}$, k^1_{PDProc}, k_2 and k_3 are determined depending on the number of individual indicators involved in the calculation of assessments EV_{BITP}, EV_{BPTP}, EV_{PDProc}, $EV^1_{OPDProt}$, $EV^2_{OPDProt}$ and EV_2, respectively, the assessments of which are equal to 0 (not complied with fully) in accordance with the rules established in table 7.

Table 7. Rules for Determining Correction Factors

Correction factor	Number of individual indicators the assessments of which are equal to zero (not complied with fully)		
k^1_{BPTP}	0	1-20	More than 20
k^1_{BITP}	0	1-20	More than 20
$k'_{OPDProt}$	0	1-20	More than 20
$k^1_{OPDProt2}$	0	1-20	More than 20
k^1_{PDProc}	0	1-8	More than 8
k_2	0	1-25	More than 25
k_3	0	1-10	More than 10
Value of the correction factor	1	0.85	0.7

11. Determining the Conformity of Information Security of an Organisation of the Banking System of the Russian Federation to the Requirements of STO BR IBBS-1.0-2014 Displaying the Assessments

11.1. If the assessment of EV_1, EV_2 or EV_3 lies within the range from 0 to 0.25, then this assessment area is assigned the level 0 of IS compliance to the requirements of STO BR IBBS-1.0.

If the assessment of EV_1, EV_2 or EV_3 lies within the range from 0.25 to 0.5, then this assessment area is assigned level 1 of IS compliance to the requirements of STO BR IBBS-1.0.

If the assessment of EV_1, EV_2 or EV_3 lies within the range from 0.5 to 0.7, then this assessment area is assigned level 2 of IS compliance to the requirements of STO BR IBBS-1.0.

If the assessment of EV_1, EV_2 or EV_3 lies within the range from 0.7 to 0.85, then this assessment area is assigned level 3 of IS compliance to the requirements of STO BR IBBS-1.0.

If the assessment of EV_1, EV_2 or EV_3 lies within the range from 0.85 to 0.95, then this assessment area is assigned level 4 of IS compliance to the requirements of STO BR IBBS-1.0.

If the assessment of EV_1, EV_2 or EV_3 lies within the range from 0.95 to 1, then this assessment area is assigned level 5 of IS compliance to the requirements of STO BR IBBS-1.0.

11.2. The value of R is determined by the lowest value among three assessments in the following assessment areas:

- Assessment of IS awareness level in the organisation (EV_3);
- Assessment of IS management in the organisation (EV_2);
- Assessment of the current IS level in the organisation (EV_1);

11.3. The R value obtained following the assessment of conformity of IS in the organisation to the requirements of STO BR IBBs-1.0 is the basis for preparing an opinion on the results of assessing IS conformity.

11.4. R values corresponding to levels 4 and 5 are recommended by the Bank of Russia.

R values corresponding to levels 0 - 3 are not recommended by the Bank of Russia.

11.5. Figure 1 represents a circular diagram for displaying the assessment results.

Sectors 1 - 10 are used to display the assessment of the current IS level in the organisation.

Sectors 11 - 27 are used to display the assessment of IS management processes in the organisation.

Sectors 28 - 34 are used to display the assessment of the IS awareness level in the organisation.

Level 5 corresponds to the circumference with a radius of 0.95 and a ring extending to the circumference with a radius of 1.

Level 4 corresponds to the circumference with a radius of 0.85 and a ring extending to the circumference with a radius of 0.95.

Level 3 corresponds to the circumference with a radius of 0.7 and a ring extending to the circumference with a radius of 0.85.

Level 2 corresponds to the circumference with a radius of 0.5 and a ring extending to the circumference with a radius of 0.7.

Level 1 corresponds to the circumference with a radius of 0.25 and a ring extending to the circumference with a radius of 0.5.

Level 0 corresponds to the circle extending to the circumference with a radius of 0.25.

11.6. A document entitled ‘Acknowledgement of Conformity of the RF BS Organisation to STO BR IBBS-1.0-2014 of the Bank of Russia’ shall be prepared following the conformity assessment.

Acknowledgement of Conformity of the RF BS Organisation to the Bank of Russia standard STO BR IBBS-1.0-2014 is based on:

- The auditor’s opinion, if the conformity was assessed by an external organisation;
- A self-assessment report, if the conformity was assessed by a RF BS organisation.

Acknowledgement of Conformity of the RF BS Organisation to the Bank of Russia standard STO BR IBBS-1.0-2014 shall include at least the following assessments:

$EV_{OPDProc}$ – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 regulating personal data processing;

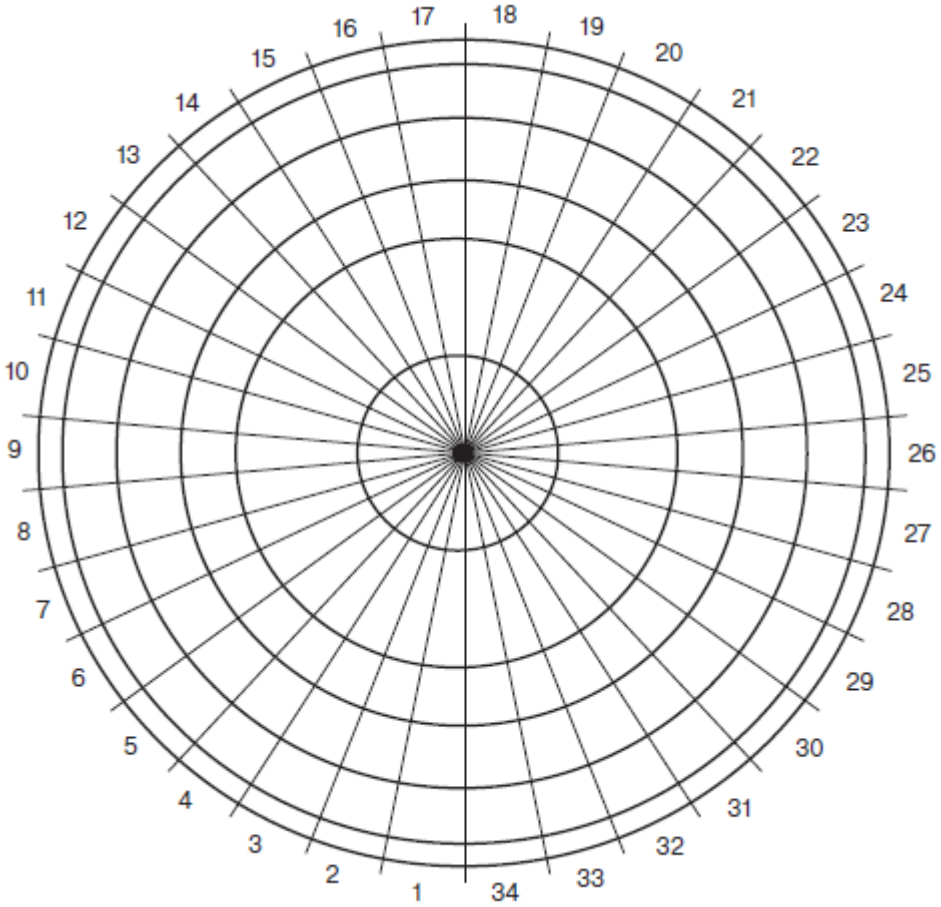
$EV^{1}_{OPDProt}$ – assessment of the degree of compliance with the requirements of STO BR IBBS-1.0 regulating personal data protection without considering the degree of compliance with STO BR IBBS-1.0 in ensuring information security when using data encryption tools;

EV_{M6} – assessment of M6 group indicator 'Ensuring information security when using data encryption tools' relative to the banking process used for personal data processing (assessment of compliance with the requirements of STO BR IBBS-1.0 regulating personal data protection when using data encryption tools);

R – total level of conformity of IS in a RF BS organisation to the requirements of STO BR IBBS-1.0.

In order to submit the Acknowledgement of Conformity of the RF BS Organisation to STO BR IBBS-1.0-2014 to the regulators responsible for overseeing the compliance with the laws in the area of personal data, this document shall be prepared in five copies, one of which is intended for use in the RF BS organisation.

Figure 1. Circular diagram for displaying assessment results



*In case of any translation ambiguity the Russian version shall prevail.

Annex A
(Mandatory)

Information Security Indicators

Group indicator M1 'Ensuring IS in assigning and allocating roles and ensuring confidence in personnel'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M1.1	Did the RF BS organisation the roles for its employees?	Required	Category 1						
M1.2	Have the roles associated with the performance of activities to ensure IS been based on requirements of sections 7 and 8 of STO BR IBBS-1.0?	Recommended	Category 1						
M1.3	Have the roles been created and assigned to employees of the RF BS organisation in compliance with the principle of providing the minimum rights and authority necessary to perform official duties?	Required	Category 1						
M1.4	Have the roles in the RF BS organisation been personalised together with the establishment of responsibility for their performance?	Required	Category 2						
M1.5	Do the official instructions or regulatory and administrative documents of the RF BS organisation establish the responsibility for performing the roles?	Required	Category 2						
M1.6	Does the RF BS organisation lack roles combining the functions of development and maintenance of ABS/software?	Required	Category 1						
M1.7	Does the RF BS organisation lack the roles combining the functions of development and operation of ABS/software?	Required	Category 1						
M1.8	Does the RF BS organisation lack the roles combining the functions of maintenance and operation of ABS/software?	Required	Category 1						
M1.9	Does the RF BS organisation lack the roles combining the functions of administrator and information security administrator?	Required	Category 1						
M1.10	Does the RF BS organisation lack the roles combining the functions for performing the operations in ABS and controlling their performance?	Required	Category 1						
M1.11	Does the RF BS organisation define, comply with and record the procedures aimed at monitoring the activities of employees possessing the aggregate of authority defined by their roles and allowing them to gain control over protected information assets of the RF BS organisation?	Required	Category 1						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M1.12	Does the RF BS organisation define, comply with and record the procedures used for hiring to positions that affect information security, including: - Checking the authenticity of submitted documents, stated qualifications, accuracy and completeness of biographic events; - Checking professional skills and assessing professional competence?	Required	Category 1						
M1.13	Do the procedures specified in individual indicator M1.12 provide for recording the results of checks?	Required	Category 2						
M1.14	Does the RF BS organisation define, comply with and record the procedures used to regularly check the professional skills and assess professional competence of employees?	Recommended	Category 1						
M1.15	Do the procedures specified in individual indicator M1.14 provide for recording the results of checks?	Recommended	Category 2						
M1.16	Does the RF BS organisation define, comply with and record the procedures for unscheduled checks of employees to establish the facts of their non-standard conduct, involvement in IS incidents or suspicion of such conduct or involvement?	Recommended	Category 1						
M1.17	Do the procedures specified in individual indicator M1.16 provide for recording the results of checks?	Recommended	Category 2						
M1.18	Have all employees of the RF BS organisation been required to undertake a written commitment to confidentiality, corporate ethics, including the requirements to prevent a conflict of interest?	Required	Category 3						
M1.19	Have IS requirements regulated by provisions been included in contracts (agreements) with external organisations and customers?	Required	Category 2						
M1.20	Do the labour contracts (agreements) and/or job descriptions define the duties of personnel to comply with IS requirements?	Required	Category 2						
M1.21	Has the non-compliance of employees of the RF BS organisation with IS requirements been considered as equivalent to the non-compliance with official duties and does it result in disciplinary action as a minimum?	Required	Category 1						
Final assessment of group indicator M1									

*In case of any translation ambiguity the Russian version shall prevail.

Group indicator M2 'Ensuring information security of automated banking at various stages of the life cycle'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M2.1	Have the following stages of the ABS LC model been considered for IS issues: – Developing requirement specifications; – Designing; – Creating and testing; – Accepting and commissioning; – Operation; – Maintenance and upgrade; – Decommissioning?	Required	Category 1						
M2.2	Have the works on IS at all stages of the ABS life cycle been performed in agreement and under control of the IS service?	Required	Category 1						
M2.3	Do the organisations engaged on a contractual basis to ensure IS at the various stages of the ABS LC have the licenses for technical protection of confidential information in accordance with the laws of the Russian Federation?	Required	Category 3						
M2.4	Have requirements for information security, established and used by the RF BS organisation to ensure IS within the processes of the RF BS organisation, been included in the requirement specifications for developing and upgrading ABS?	Required	Category 3						
M2.5	Does the RF BS organisation implement the ban on using protected information as test data, data anonymity and control over the adequacy of access provision and access isolation at the stage of creating and testing ABS and/or its components?	Required	Category 1						
M2.6	Have the operated ABS and/or their components been provided with documentation containing the description of safeguards implemented in ABS, including the description of organisational safeguards and requirements for their implementation, technical safeguards and requirements for their operation?	Required	Category 2						
M2.7	Does the RF BS organisation analyse safeguards adopted by the ABS developer aimed at ensuring the security of ABS development and security of its delivery?	Recommended	Category 1						
M2.8	Has either of the following three options been implemented in interactions of the RF BS organisation with the ABS developer: 1) Contract on ABS development or delivery of ready-made ABS and their components includes the provisions for maintenance of delivered products throughout their life; 2) The RF BS organisation acquires complete documentation which allows to maintain ABS and its components without the participation of the developer; 3) The management of the RF BS organisation assesses and records the risk of IS breach arising without the possibility of maintaining the ABS and its components?	Required	Category 3						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M2.9	Does the development of the specifications for remote banking systems consider the need to ensure data protection in the following conditions: - Attempts at unauthorised access to information by anonymous, unauthenticated attackers using public networks; - Possibility of errors by authorised users of the systems; - Possibility of unintentional or improper use of protected information by authorised users?	Required	Category 3						
M2.10	Does the RF BS organisation define, comply with and record the following procedures at the stage of operating the ABS: - Monitoring the operability (functioning, efficiency) of safeguards implemented in the ABS, including implementation of organisational safeguards, applicable technical safeguards and configuration parameters; - Monitoring the absence of vulnerabilities in ABS hardware and software; - Monitoring the changes made to ABS configuration parameters and applicable technical safeguards; - Monitoring the necessary ABS software updates, including software for technical safeguards?	Required	Category 1						
M2.11	Have the procedures needed to ensure the recovery of all implemented IS functions been defined, performed and recorded at the stage of operating the ABS?	Required	Category 1						
M2.12	Have the procedures for monitoring the components of installed and/or used ABS software been defined, performed and recorded at the stage of operating the ABS?	Required	Category 1						
M2.13	Have the roles associated with the operation and control over ABS operation and the applicable technical safeguards, including changes to their configuration settings been selected and assigned?	Required	Category 3						
M2.14	Have the procedures for monitoring the operation of all ABSs been defined and performed by the IS service, are the process and results of their performance recorded?	Required	Category 1						
M2.15	Have the procedures needed to ensure the safety of protected information media been defined, performed and recorded at the stage of operating the ABS?	Required	Category 1						
M2.16	Did the RF BS organisation define, perform and register the monitoring procedures at the stage of maintaining (upgrading) ABS to ensure protection from the following: - Intentional unauthorised disclosure, modification or destruction of information; - Unintentional modification, disclosure or destruction of information; - Denial of service or degradation of service?	Required	Category 1						
M2.17	Have the procedures for recording the changes been defined, performed and recorded at the stage of maintaining (upgrading) the ABS, related to the decision of the RF BS organisation regarding critical systems, including ABS involved in implementing the bank payment process and in ISPD?	Required	Category 1						
M2.18	Have the procedures for checking ABS functionality, including the applicable safeguards, after implementing the changes, been defined, performed and recorded at the stage of	Required	Category 1						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
	maintaining (upgrading) the ABSs, related to the decision of the RF BS organisation regarding critical systems, including ABSs involved in implementing the bank payment process and in ISPD?								
M2.19	Have the procedures ensuring the removal of information by using algorithms and/or methods preventing the recovery of deleted information, the unauthorised use of which may cause damage to the business activities of the organisation, and information used by technical safeguards, from non-volatile memory of ABS and external media (except for archives of electronic documents and electronic interaction protocols, the maintenance and preservation of which is required by the laws of the Russian Federation for as specific period, regulatory acts of the Bank of Russia and/or contractual documents), been defined, complied with, regulated and performed at the stage of decommissioning?	Required	Category 1						
Final assessment of group indicator M2									

Group indicator M3 ‘Ensuring information security in access control and registration’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M3.1	Have the procedures for identifying, recording and categorising (assigning to one of the types) the information assets been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M3.2	Have the access rights of employees and customers of the RF BS organisation to information assets and/or their types been recorded and documented?	Required	Category 1						
M3.3	Does the ABS use integrated safeguards against UA and URA?	Required	Category 1						
M3.4	Does the ABS use data encryption tools certified in accordance with the requirements of information security?	Recommended	Category 3						
M3.5	Do the safeguards against UA ensure concealment of authentication data entered by accessing parties on devices used for displaying the information?	Required	Category 3						
M3.6	Does the placement of ABS devices used for displaying information prevent unauthorised viewing?	Required	Category 3						
M3.7	Have the rules and procedures used for identification, authentication, authorisation of accessing parties, including external accessing parties that are not employees of the RF BS organisation, and software processes (services) been defined, complied with, recorded and monitored?	Required	Category 1						
M3.8	Have the rules and procedures used for limiting access to information assets through the role-based method, along with the definition of authority to access the information assets for each role, been defined, complied with, recorded and monitored?	Required	Category 1						
M3.9	Have the rules and procedures used for managing the provision/withdrawal and blocking of access, including access through external information and telecommunication networks, been defined, complied with, recorded and monitored?	Required	Category 1						
M3.10	Have the rules and procedures used for registering the actions of accessing parties, while ensuring the control of integrity and protection of registration data, been defined, complied with, recorded and monitored?	Required	Category 1						
M3.11	Have the rules and procedures used for managing the identification data, authentication data and authentication tools been defined, complied with, recorded and monitored?	Required	Category 1						
M3.12	Have the rules and procedures used for managing the accounts of accessing parties been defined, complied with, recorded and monitored?	Required	Category 1						
M3.13	Have the rules and procedures used for detecting and blocking unsuccessful access attempts been defined, complied with, recorded and monitored?	Required	Category 1						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M3.14	Have the rules and procedures used for blocking access sessions after a specified idle time or at the request of the accessing party, which requires re-authentication and re-authorisation procedures to continue the work, been defined, complied with, recorded and monitored?	Required	Category 1						
M3.15	Have the rules and procedures used for restricting user actions aimed at changing the settings of their automated workstations (restrictions to change BIOS) been defined, complied with, recorded and monitored?	Required	Category 1						
M3.16	Have the rules and procedures used for managing the set of actions allowed for identification and authentication been defined, complied with, recorded and monitored?	Required	Category 1						
M3.17	Have the rules and procedures used for restricting user actions aimed at changing the settings of the ABS and implementing control over the actions of operating personnel aimed at changing ABS configuration parameters been defined, complied with, recorded and monitored?	Required	Category 1						
M3.18	Have the rules and procedures used for identifying and blocking unauthorised transfer (copying) of information, including databases, file resources, virtual machines been defined, complied with, recorded and monitored?	Required	Category 1						
M3.19	Have the rules and procedures for the use of wireless technology, if any, to access to information and protection of internal wireless connections been defined, complied with, recorded and monitored?	Required	Category 1						
M3.20	Have the rules and procedures for the use of mobile devices, if any, to access to information been defined, complied with, recorded and monitored?	Required	Category 1						
M3.21	Do the procedures used for access control exclude the possibility of "self-authorisation"?	Required	Category 1						
M3.22	Have the rules and procedures used for monitoring IS, analysing and storing data on actions and operations and allowing the detection of illegal or suspicious operations and transactions been defined, complied with, recorded and monitored?	Required	Category 1						
M3.23	Have the actions and operations requiring registration been defined?	Required	Category 2						
M3.24	Have the structure and content of data on actions and transactions requiring registration and the period of their storage been defined?	Required	Category 2						
M3.25	Has the necessary amount of memory been reserved for recording the data?	Required	Category 3						
M3.26	Has the response to failure during the registration of actions and operations, including hardware and software errors and failures in data collection equipment, been ensured?	Required	Category 1						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M3.27	Has the generation of timestamps for registered actions and operations and synchronisation of system time on hardware used for monitoring IS, analysis and data storage, been ensured?	Required	Category 3						
M3.28	Has the RF BS organisation implemented the logging of actions and operations of automated workstations, servers and network equipment, firewalls and ABS in order to use them in response to IS incidents?	Required	Category 1						
M3.29	Has the storage of data on actions and operations been ensured for no less than three years (unless a different storage period is established by the laws of the Russian Federation, regulatory acts of the Bank of Russia)?	Recommended	Category 3						
M3.3O	Has the storage of data obtained as a result of the bank payment process been ensured for no less than five years (unless a different storage period is established by the laws of the Russian Federation, regulatory acts of the Bank of Russia)?	Recommended	Category 3						
M3.31	Has specialised software and/or hardware been used for procedures aimed at monitoring IS and analysing data on actions and operations?	Required	Category 3						
M3.32	Have the criteria aimed at identifying illegal or suspicious actions and operations and used in procedures for monitoring IS and analysing actions and operations been recorded?	Required	Category 2						
M3.33	Are the procedures aimed at monitoring IS and analysing data on actions and operations and using recorded criteria for identifying illegal or suspicious actions and operations applied on a regular basis, such as daily, to all performed operations (transactions)?	Required	Category 3						
M3.34	Has the compliance with the following requirements been defined and monitored in the RF BS organisation: - Separation of computer network segments, including those created by using virtualisation technology; - Firewalling; - Information interaction between computer network segments?	Required	Category 1						
M3.35	Has the separation of computer network segments aimed at ensuring the independent performance of bank payment processes in the RF BS organisation, as well as the performance of bank information processes with varying degree of importance in the RF BS organisation, including bank information processes used for personal data processing in the ISPD, been ensured?	Required	Category 1						
M3.36	Have the procedures used for making changes to network equipment configuration which provide approval of changes from the IS service been regulated and monitored?	Required	Category 2						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M3.37	Have the IS service employees been provided with access to network equipment configuration without the ability to make changes?	Recommended	Category 3						
M3.38	Has the procedure for accessing the information asset environment objects, including the premises hosting the information asset environment objects been defined, complied with, recorded and monitored?	Required	Category 1						
M3.39	Do the ABSs used in the RF BS organisation, including remote banking systems, allow the following to be registered: - Operations with customer account data, including operations aimed at opening, modifying and closing customer accounts; - Transactions with financial implications; - Operations associated with assigning and allocating user rights?	Required	Category 3						
M3.40	Has the procedure for using removable media in the RF BS organisation been defined, complied with and monitored?	Required	Category 1						
M3.41	Have the safeguards preventing the rejection of ownership of operation and transactions conducted by the customers been implemented in remote banking systems used in the RF BS organisation?	Required	Category 3						
M3.42	Have the protocols of operations performed through remote banking been provided with legal significance, for example, by introducing the appropriate provisions to remote banking contracts?	Required	Category 1						
M3.43	Does the conclusion of contracts with third party organisations include legal arrangements defining the necessary level of interaction if an IS incident goes beyond the individual organisation?	Recommended	Category 2						
M3.44	Has the RF BS organisation defined the procedures regulating the actions of employees and customers of the RF BS organisation if the information necessary for their identification, authentication, and/or authorisation is compromised, including through their own fault, including methods used for recognising such cases?	Required	Category 2						
M3.45	Have the procedures specified in individual indicator M3.44 been communicated to employees and customers of the RF BS organisation?	Required	Category 3						
M3.46	Do the procedures specified in individual indicator M3.44 provide for registration by employees and customers of all their actions and their results?	Required	Category 3						
M3.47	Have the mechanisms (regular, continuous or on-demand) for informing customers about all operations performed on their behalf been implemented in remote banking systems?	Required	Category 3						
M3.48	Does the RF BS organisation apply measures aimed at protecting against UA, damaging or breaching the integrity of data on actions and operations, as well as measures to protect the information necessary for identification, authentication and/or the authorisation of customers and employees of the RF BS organisation?	Required	Category 1						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M3.49	Are all attempts of UA to information needed for identification, authentication and/or authorisation of customers and employees of the RF BS organisation registered?	Required	Category 1						
M3.50	Is access to data on actions and operations provided only to perform official duties?	Required	Category 1						
M3.51	Are the regulated procedures used for the appropriate review of access rights in the event of the dismissal or change of official duties of employees of the RF BS organisation who had access to data on actions and operations, complied with?	Required	Category 1						
M3.52	Is there any usage of network protocols providing network connection protection, control over the integrity of networking interaction and implementation of two-way authentication technology for access in telecommunication channels and communication lines, including wireless lines, not controlled by the RF BS organisation?	Required	Category 3						
M3.53	Is the transmission of protected data over communication channels extending beyond the area controlled by the RF BS organisation provided only if it is secured against disclosure and modification?	Required	Category 3						
M3.54	Is the work of all employees of the RF BS organisation performed using unique and personalised accounts?	Required	Category 3						
Final assessment of group indicator M3									

Group indicator M4 ‘Ensuring information security by antivirus protection’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M4.1	Are antivirus protection tools used on all automated workstations and ABS servers of the RF BS organisation, unless otherwise provided by the process?	Required	Category 1						
M4.2	Have the procedures for installation and regular updating of antivirus tools (versions and databases) been defined, complied with, recorded and monitored on automated workstations and ABS servers?	Required	Category 1						
M4.3	Has ongoing antivirus protection in automatic mode and automatic installation of updates of antivirus software and its databases been arranged?	Recommended	Category 1						
M4.4	Is the antivirus scan of removable media performed on dedicated stand-alone computer equipment before connecting such media to computer equipment involved in banking processes?	Recommended	Category 1						
M4.5	Have the guidelines and recommendations for antivirus protection, that take into account the specific aspects of banking processes, been developed and enacted?	Required	Category 2						
M4.6	Has antivirus filtering of all e-mail traffic been arranged in the RF BS organisation?	Required	Category 3						
M4.7	Has the RF BS organisation made arrangements for a layered centralised antivirus protection system that provides for the use of antivirus tools from different vendors on: - Workstations; - Server equipment, including e-mail servers; - Firewalling hardware?	Required	Category 1						
M4.8	Have the procedures for preliminary antivirus scan of installed or modified software been defined, complied with, recorded and monitored?	Required	Category 1						
M4.9	Is an antivirus scan performed after installing or modifying software?	Required	Category 3						

M4.10	Have the procedures, performed in the event that a computer viruses is detected, which, in particular, must include the following measures, been defined, complied with, recorded and monitored: - Measures necessary to repel and eliminate the effects of a virus attack; - Procedure for officially informing the management; - Procedure for suspending work if necessary (for the period required to eliminate the effects of a virus attack)?	Required	Category 1						
M4.11	Have the procedures used for disabling and updating antivirus tools on all ABS hardware been defined, complied with and recorded?	Required	Category 1						
M4.12	Has the duty to implement the prescribed antivirus safeguards been assigned to each employee of the RF BS organisation with access to a computer and/or ABS, and has the responsibility for compliance with the requirements for antivirus protection been assigned to the heads of the functional units of the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M4									

Group indicator M5 'Ensuring information security when using Internet resources'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M5.1	Has the management of the RF BS organisation adopted a documented decision on the use of the Internet for operating and/or their own business activities, which clearly lists and records the purpose of using the Internet?	Required	Category 2						
M5.2	Is it forbidden to use Internet resources for unauthorised purposes?	Required	Category 2						
M5.3	Has the RF BS organisation allocated a limited number of packages containing the list of Internet services and resources available to users?	Required	Category 3						
M5.4	Are the employees of the RF BS organisation provided with user rights, included in the specific package containing the list of Internet services and resources, in accordance with their official duties, in particular, in accordance with their assigned roles?	Required	Category 3						
M5.5	Is there any registration for provision of employees of the RF BS organisation with user rights, included in the specific package containing the list of Internet services and resources, in accordance with their official duties, in particular, in accordance with their assigned roles?	Required	Category 3						
M5.6	Have the procedures for connecting to and using Internet resources been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M5.7	Is protected data transmitted via the Internet only when protected from disclosure and modification?	Required	Category 1						
M5.8	Does the RF BS organisation apply the safeguards in connection with the increased risk of IS breaches during interactions with the Internet, including firewalls, antivirus tools, intrusion detection tools, data encryption tools, that ensure, among other things, the reception and transmission of information only in the established format and only in accordance with a particular technology?	Required	Category 1						
M5.9	Have the guidelines and recommendations for Internet use that take into account the specific aspects of banking processes, been developed and enacted?	Required	Category 1						
M5.10	Have the procedures for logging the visits of Internet resources by the employees of the RF BS organisation been defined and complied with?	Required	Category 1						
M5.11	Is information on Internet resources visited by employees of the RF BS organisation available to employees of the IS service?	Required	Category 3						
M5.12	Have the computers used for direct interaction with the Internet been allocated and physically isolated from internal networks?	Recommended	Category 1						

M5.13	Are there any safeguards aimed at preventing the possibility of substituting the authorised customer by a hacker within a session and applied during the remote banking?	Required	Category 3							
M5.14	Are the attempts to substitute the authorised customer by a hacker within a session registered in a regulated way?	Required	Category 1							
M5.15	Are all customer operations within a session in remote banking systems, including money transfer operations, performed only after complying with the procedures for identification, authentication and authorisation?	Required	Category 3							
M5.16	Is closing of the current session and repeated performance of the procedures for identification, authentication and authorisation provided in the event of a disrupted or broken connection in remote banking systems?	Required	Category 3							
M5.17	Is there any specialised client software used to provide user access to remote banking systems?	Recommended	Category 3							
M5.18	Have the set and application procedure of safeguards used for e-mail exchange over the Internet been defined?	Required	Category 2							
M5.19	Has e-mail exchange over the Internet been arranged through a limited number of points, consisting of external (connected to the Internet) and internal (connected to internal networks of the RF BS organisation) mail servers with a secure mail message replication system installed between them (Internet kiosks)?	Recommended	Category 3							
M5.20	Is e-mail archiving performed in order to: - Control information flows, including to prevent information leaks; - Use the archives in investigations of information leaks?	Required	Category 3							
M5.21	Have the rules and procedures for access to archive information and changes to it, that allow the employees of the IS service to access the archive information, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1							
M5.22	Does the RF BS organisation allow storage and processing of bank information (including public information) on a computer used for direct interaction with the Internet?	Recommended	Category 3							
M5.23	Is the availability of bank information on computers used for direct interaction with the Internet always determined by the business goals of the RF BS organisation and authorised by its management?	Required	Category 3							
M5.24	Have the set and application procedure of safeguards used for interaction with the Internet and allowing for countermeasures to hacker attacks and spam distribution been determined?	Required	Category 1							
Final assessment of group indicator M5										

Group indicator M6 ‘Ensuring information security when using data encryption tools’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M6.1	Are DETs used in the RF BS organisation in accordance with the model of IS threats and the model of IS violator adopted by the RF BS organisation?	Required	Category 1						
M6.2	Do DETs used to protect personal data have a class not lower than KS2?	Required	Category 3						
M6.3	Are the works on ensuring the security of information by using DETs conducted in accordance with applicable laws, regulatory acts governing the operation of DET, technical documentation for DET and licensing requirements of the Federal Security Service (FSB) of Russia?	Required	Category 1						
M6.4	Does the RF BS organisation have an approved individual policy on the use of DETs in the RF BS organisation?	Recommended	Category 2						
M6.5	Do DETs allow to embed electronic messages into processes?	Required	Category 3						
M6.6	Do DETs allow interaction with application software at the cryptographic transformation query processing and reporting level?	Required	Category 3						
M6.7	Do DETs have the full set of operating documentation provided by the developer, including the description of the key system, rules for working with it and the rationale for the necessary organisational and staffing provision?	Required	Category 3						
M6.8	Have DETs been certified by the authorised government authority or do DETs have the authorisation of FSB of Russia?	Required	Category 3						
M6.9	Are the installation and commissioning as well as operation of DETs carried out in accordance with operating and technical documentation to such tools?	Required	Category 3						
M6.10	Is the logging process continuity of DET operation during the use of DETs maintained in accordance with the technical documentation for DETs?	Required	Category 3						
M6.11	Is continuity maintained for the processes to ensure the integrity of the software for DET functioning environment, which represents the aggregate of hardware and software that together provide the operation of DET and that can affect the implementation requirements established for DET?	Required	Category 3						

M6.12	Is the IS of processes used for generating cryptographic keys of DET supported by a comprehensive set of technological, organisational, technical and software measures and protection tools provided by the technical documentation for DET?	Required	Category 3						
M6.13	Have the IS monitoring procedures aimed at registering all significant events occurring in the exchange of cryptographically protected data and all IS incidents been implemented?	Recommended	Category 1						
M6.14	Has the management defined the procedure for using DETs based on the documents specified in section 7.7 of STO BR IBBS-1.0 and including the following: - Procedure for commissioning, including the procedures for embedding DET in ABS; - Procedure for operation; - Procedure for restoring operability in emergencies; - Procedure for making changes; - Procedure for decommissioning; - Procedure for key system management; - Procedure for handling key media, including the actions in case of change and compromise of keys?	Required	Category 1						
M6.15	Do the RF BS organisation and/or customer generate their DET keys independently?	Recommended	Category 3						
M6.16	Are the relations arising between organisations and their customers regulated by the concluded contracts?	Required	Category 2						
Final assessment of group indicator M6									

Group indicator M7 ‘Ensuring information security of bank payment processes’,

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M7.1	Has the RF BS organisation regulated (described) its bank payment process?	Required	Category 2						
M7.2	Has the procedure for exchanging payment information been documented in the contracts between the parties to such exchange?	Required	Category 2						
M7.3	Does the RF BS organisation prevent its employees from having the authority for uncontrolled creation, authorisation, destruction and change of payment information, as well as performance of unauthorised operations to change the status of bank accounts?	Required	Category 1						
M7.4	Are the results of operations on handling payment information by persons/automated processes monitored (checked)?	Required	Category 3						
M7.5	Is the handling of payment information and monitoring (checking) of such handling results performed by different employees/automated processes?	Recommended	Category 3						
M7.6	Does the comprehensive set of safeguards used for the bank payment process provide for the protection of payment information from distortion, tampering, redirection, unauthorised destruction, false authorisation of electronic payment messages?	Required	Category 1						
M7.7	Does the comprehensive set of safeguards used for the bank payment process provide for the access of an employee of the RF BS organisation only to those resources of the bank payment process that are necessary for the performance of their official duties or exercise of rights granted by payment information processing technology?	Required	Category 1						
M7.8	Does the comprehensive set of safeguards used for the bank payment process provide for control (monitoring) of compliance with the technology established for preparation, processing, transfer and storage of payment information?	Required	Category 1						
M7.9	Does the comprehensive set of safeguards used for the bank payment process provide for authentication of incoming electronic payment messages?	Required	Category 1						
M7.10	Does the comprehensive set of safeguards used for the bank payment process provide for two-way authentication of automated workstations (workstations and servers), participants in the exchange of electronic payment messages?	Required	Category 1						

M7.11	Does the comprehensive set of safeguards used for the bank payment process allow only authorised users to enter the payment information in the ABS?	Required	Category 1						
M7.12	Does the comprehensive set of safeguards used for the bank payment process provide for controls aimed at excluding the possibility of malicious acts, in particular, double entry, verification, restrictions depending on the amount of operations?	Required	Category 1						
M7.13	Does the comprehensive set of safeguards used for the bank payment process provide for the recovery of payment information in the event of its intentional (accidental) destruction (distortion) or failure of computer equipment?	Required	Category 1						
M7.14	Does the comprehensive set of safeguards used for the bank payment process provide for reconciliation of outgoing electronic payment messages with corresponding incoming and processes electronic payment messages during interbank settlements?	Required	Category 1						
M7.15	Does the comprehensive set of safeguards provide for blocking the acceptance of instructions from the customers?	Required	Category 1						
M7.16	Does the comprehensive set of safeguards used for the bank payment process provide for the delivery of electronic payment messages to participants in the exchange of such messages?	Required	Category 1						
M7.17	Has the RF BS organisation made arrangements for authorised entering of payment information in the ABS by two employees with subsequent application-based reconciliation of input results for matching (‘dual control’)?	Recommended	Category 3						
M7.18	Do the remote banking systems use procedures that implement the following: - Reducing the likelihood of unintentional or accidental operations or transactions by authorised customers; - Communicating to customers information on possible risks associated with operations or transactions?	Required	Category 3						
M7.19	Have the customers of remote banking systems been provided with detailed instructions describing the procedures for operations or transactions?	Required	Category 3						
M7.20	Have the procedures for maintaining the computer equipment used in the bank payment process, including the replacement of its software and/or hardware parts, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						

M7.21	Have the procedures for periodic control of all functions (requirements) aimed at ensuring IS of payment information and implemented by software and hardware been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M7.22	Have the procedures for controlling the absence of specialised tools used for unauthorised information retrieval and placed on devices involved in the bank payment process that are located in public places outside the area of continuous monitoring, including ATMs and payment terminals, been defined, complied with, recorded and monitored in RF BS organisation?	Required	Category 1						
M7.23	Have the procedures for restoring all functions (requirements) aimed at ensuring IS of payment information and implemented by software and hardware been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
Final assessment of group indicator M7									

Group indicator M8 'Ensuring information security of bank information processes',

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M8.1	Has the RF BS organisation classified non-payment information?	Required	Category 2						
M8.2	Is the classification of non-payment information performed in accordance with the severity of the consequences arising from the loss of IS properties, in particular, such properties as availability, integrity and confidentiality?	Required	Category 3						
M8.3	Has the set of requirements for protecting each type of non-payment information resulting from classification been defined?	Required	Category 2						
M8.4	Has the RF BS organisation regulated (described) its bank information processes?	Required	Category 1						
M8.5	Have the bank information processes been implemented within ABSs established for that purpose?	Required	Category 3						
M8.6	Have the servers, office computers and other equipment, not included in ABSs implementing bank information processes, been isolated from these ABSs at the level of local area networks by using a method agreed with the IS service?	Recommended	Category 3						
M8.7	Have the requirements for ABS interaction of in RF BS organisations with third-party information systems (external information systems) been defined, complied with and monitored?	Required	Category 1						
Final assessment of group indicator M8									

*In case of any translation ambiguity the Russian version shall prevail.

Group indicator M9 'General requirements for personal data processing in a RF BS organisation'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M9.1	Has the management of the RF BS organisation set the goals of personal data processing (hereinafter, the 'PD')?	Required	Category 2						
M9.2	Has the RF BS organisation established the requirement to notify the authorised body for protection of PD entities on PD processing?	Required	Category 2						
M9.3	Is there any activity arranged for timely provision of such notice in accordance with the requirements of the Federal Law 'On Personal Data' in the event of such need?	Required	Category 3						
M9.4	Has the RF BS organisation established the criteria for referring ABS to ISPD?	Required	Category 2						
M9.5	Have the procedures for recording PD resources, including ISPD, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M9.6	Has each PD resource been provided with a goal of PD processing?	Required	Category 2						
M9.7	Have the personal data storage periods and the terms for terminating their processing been established and complied with for each PD resource?	Required	Category 1						
M9.8	Has the list and categories of processed PD (special categories of PD, biometric PD, PD obtained from publicly available sources or other PD) been defined for each PD resource?	Required	Category 2						
M9.9	Has the compliance with procedures established for recording the number of PD entities, including PD entities that are not employees of the RF BS organisation been ensured for each PD resource?	Required	Category 1						
M9.10	Has the restriction on processing the PD resource by the goal of PD processing been complied with for each PD resource?	Required	Category 3						
M9.11	Has the conformity of the content and amount of processed PD to established goals of processing been established for each PD resource?	Required	Category 3						
M9.12	Has the accuracy, adequacy and relevance of PD, including the objectives of PD processing, been ensured for each PD resource?	Required	Category 3						
M9.13	Has the compliance with established procedures for obtaining consent of PD entities (their legal representatives) to processing their PD been ensured for each PD resource, if such consent is necessary in accordance with the requirements of the Federal Law 'On Personal Data'?	Required	Category 3						
M9.14	Has the compliance with established procedures for obtaining consent of PD entities to transfer the processing of their PD to third parties been ensured for each PD resource, if such consent is necessary in accordance with the requirements of the Federal Law 'On Personal Data'?	Required	Category 3						
M9.15	Has the termination of PD processing and destruction or depersonalisation of PD at the request of the PD entity after achieving the objectives of processing been ensured for each PD resource in cases stipulated by the Federal Law 'On Personal Data', including when the PD entity withdraws its consent for processing its PD?	Required	Category 3						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M9.16	Have the procedures for terminating PD processing and their destruction or depersonalisation within the periods established by the Federal Law 'On Personal Data', after achieving the objective of PD processing, been defined, complied with, recorded and monitored in the RF BS organisation (unless otherwise provided by the contract, a party, beneficiary or guarantor of which is the PD entity, other agreement between the RF BS organisation and the PD entity)?	Required	Category 1						
M9.17	Have the procedures for terminating PD processing and their destruction or depersonalisation within the periods established by the Federal Law 'On Personal Data', if the PD entity withdraws its consent for PD processing, or if PS storage is no longer required for PD processing purposes, been defined, complied with, recorded and monitored in the RF BS organisation (unless otherwise provided by the contract, a party, beneficiary or guarantor of which is the PD entity, other agreement between the RF BS organisation and the PD entity)?	Required	Category 1						
M9.18	Have the procedures for terminating PD processing and their destruction or depersonalisation within the periods established by the Federal Law 'On Personal Data', if PD are obtained illegally or are not required for the stated purpose of processing, been defined, complied with, recorded and monitored in RF BS organisation?	Required	Category 1						
M9.19	Have the procedures for terminating PD processing and their destruction or depersonalisation within the periods established by the Federal Law 'On Personal Data', in the event of illegal PD processing performed by the RF BS organisation or processing handler instructed by the RF BS organisation, if it is impossible to ensure the legality of PD processing, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M9.20	Have the procedures for terminating PD processing and their destruction or depersonalisation within the periods established by the Federal Law 'On Personal Data', in case of illegal PD processing without the consent of the PD entity, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M9.21	Does the RF BS organisation ensure blocking of PD with their subsequent destruction no later than within six months from the day of blocking, if there is no possibility to destroy or depersonalise PD within the periods established by the Federal Law 'On Personal Data'?	Required	Category 1						
M9.22	Has the RF BS organisation defined, complied with and monitored its PD processing policy, and has it established, if necessary, any procedures for PD processing of individual PD resources?	Required	Category 1						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M9.23	Is the PD processing procedure for PD resources processed in the ABS of the RF BS organisation, including ISPD, a part of operating documentation for the ABS and is it developed at the stage of ABS creation or upgrading?	Recommended	Category 2						
M9.24	Does the PD processing policy define the procedures for granting access to PD?	Required	Category 2						
M9.25	Does the PD processing policy define the procedures for changing PD in order to ensure their accuracy, reliability and relevance, including in relation to the objectives of PD processing?	Required	Category 2						
M9.26	Does the PD processing policy define the procedures for destruction, depersonalisation or blocking of PD in the event of the need for such procedures?	Required	Category 2						
M9.27	Does the PD processing policy define the procedures for requests by PD entities (their legal representatives) in cases stipulated by the Federal Law 'On Personal Data', in particular, the procedure for preparing information on the availability of PD related to the specific PD entity, information necessary for enabling the review by PD entity (their legal representatives) of its PD, as well as procedures for processing the requests for clarification of PD, their blocking or destruction if PD are incomplete, outdated, inaccurate, illegally obtained or are not necessary for the stated purpose of their processing?	Required	Category 2						
M9.28	Does the PD processing policy define the procedures for processing the request of the body authorised to protect the rights of PD entities?	Required	Category 2						
M9.29	Does the PD processing policy define the procedures for obtaining consent of the PD entity for processing its PD or transferring its PD processing to third parties?	Required	Category 2						
M9.30	Does the PD processing policy define the procedures for transferring PD between the users of the PD resource and providing for the transfer of PD only between employees of the RF BS organisation granted with PD access?	Required	Category 2						
M9.31	Does the PD processing policy define the procedures for transferring PD to third parties?	Required	Category 2						
M9.32	Does the PD processing policy define the procedures for handling physical media with PD?	Required	Category 2						
M9.33	Does the PD processing policy define the procedures necessary for notifying the body authorised to protect the rights of PD entities on PD processing within the periods established by the Federal Law 'On Personal Data'?	Required	Category 2						
M9.34	Does the PD processing policy define the need to use standard documents forms for PD processing and procedures for working with them (standard document form means a template, document form or other unified form of document used by the RF BS organisation to collect PD)?	Required	Category 2						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M9.35	Has the RF BS organisation ensured unrestricted access to the document defining its policy with regard to PD processing, as well as to details on implemented requirements for ensuring the security of personal data?	Required	Category 3						
M9.36	Has the RF BS organisation established in which cases it is necessary to obtain the consent of PD entities?	Required	Category 2						
M9.37	Have the form and procedure for obtaining the consent of entities been regulated?	Required	Category 2						
M9.38	Have the procedures for maintaining the records of persons with access to PD been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M9.39	Has the head of the RF BS organisation approved the document defining the list of persons with access to PD?	Required	Category 2						
M9.40	Do the employees of the RF BS organisation process PD only for performing their official duties?	Required	Category 3						
M9.41	Have the procedures for familiarising the employees of the RF BS organisation directly involved in PD processing with the provision of the laws of the Russian Federation and internal documents of the RF BS organisation containing the requirements for PD processing and security regarding their official duties, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M9.42	Does the RF BS organisation familiarise the employees of the RF BS organisation directly involved in PD processing with the provision of the laws of the Russian Federation and internal documents of the RF BS organisation containing the requirements for PD processing and security regarding their official duties during the activities aimed at their training or awareness?	Required	Category 3						
M9.43	Have the procedures for maintaining the records of premises used for PD processing, as well as the access of employees of the RF BS organisation and other persons to the premises used for PD processing been defined?	Required	Category 1						
M9.44	Has the separation of PD been ensured from other information, in particular, by recording PD on separate removable media with PD, in special sections or fields of document forms (when processing PD on paper)?	Required	Category 3						
M9.45	Have the records of removable media with PD been maintained when working with removable media containing PD?	Required	Category 1						
M9.46	Have the establishment, compliance and monitoring of the procedure for storing removable media with PD, including machine-readable media, and access to such media been ensured when working with removable media containing PD?	Required	Category 1						
M9.47	Has the storage on separate removable media with PD with processing purposes, which are clearly incompatible, been ensured when working with removable media containing PD?	Required	Category 3						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M9.48	Have the registration and records of storage locations for physical media with PD along with indication of categories of processed personal data (special categories of PD, biometric PD, PD obtained from public sources, or any other PD), including the separate storage of PD resources processed for different purposes, been ensured when working with removable media containing PD?	Required	Category 3						
M9.49	Has the appointment of employees responsible for storage of removable media with PD been ensured when working with removable media containing PD?	Required	Category 3						
M9.50	Has the establishment and compliance with the procedure for destruction (erasure) of information recorded on removable media containing PD been ensured when working with removable media containing PD?	Required	Category 3						
M9.51	Are PD stored in a form allowing to determine the PD entity no longer than required by the purpose of PD processing, if the period for PD storage is not established by federal law, contract, where the party, beneficiary or guarantor is the PD entity?	Required	Category 3						
M9.52	Does the RF BS organisation create and publish publicly available sources of PD only for meeting the requirements of the laws of the Russian Federation?	Required	Category 3						
M9.53	Have the procedures for publishing PD in the publicly available sources of PD been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M9.54	Is the assignment of PD processing to a third party (hereinafter, the "handler") based on the contract?	Required	Category 2						
M9.55	Does this contract define a list of actions (operations) with PD to be performed by the handler and the purpose of such processing?	Required	Category 2						
M9.56	Does this contract establish the obligation of the handler to ensure the security of PD (including by complying with PD confidentiality) during their processing, not to disclose or not to distribute PD without the consent of the PD entity, unless otherwise provided by federal law, and specify the requirements for security of PD?	Required	Category 2						
M9.57	Has the RF BS organisation obtained the consent of the PD entity when assigning the processing of personal data to the handler, unless otherwise provided by federal law?	Required	Category 3						
M9.58	Have the procedures performed when necessary to make a cross-border transfer of PD been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M9.59	Has the RF BS organisation appointed a person responsible for arranging PD processing?	Required	Category 3						
M9.60	Has the management of the RF BS organisation established the authority of the person responsible for arranging PD processing, as well as their rights and obligations?	Required	Category 2						
Final assessment of group indicator M9									

Group indicator M10 'General requirements for ensuring information security of banking processes used for personal data processing'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M10.1	Does the RF BS organisation define, comply with and record the procedures for monitoring the integrity of and ensuring trusted software downloads, including software for technical safeguards, for computing equipment included in ISPD to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 1						
M10.2	Does the RF BS organisation define, comply with and record the procedures for access to operating documentation and archive files containing the settings parameters for ISPD, including the settings for applicable technical safeguards to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 1						
M10.3	Does the RF BS organisation define, comply with and record the procedures for backup and recovery of PD to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 1						
M10.4	Does the RF BS organisation define, comply with and record the procedures for backup and recovery of software, including software for technical safeguards included in ISPD, to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 1						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M10.5	Does the RF BS organisation identify and authenticate devices used for providing access as part of ensuring IS in access control and registration to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 3						
M10.6	Does the RF BS organisation host hardware intended for administering ISPD, automated user stations and server components of ISPD in separate, dedicated segments of computer networks as part of ensuring IS in access control and registration to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 3						
M10.7	Does the RF BS organisation monitor network traffic, detect intrusions and network attacks and respond to them as part of ensuring IS in access control and registration to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 1						
M10.8	Does the RF BS organisation define, comply with, record and monitor the procedures for updating the signature databases for technical safeguards, monitor as part of ensuring IS in access control and registration to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 1						
M10.9	Does the RF BS organisation define, comply with, record and monitor the procedures for using communication ports, I/O devices, removable computer media and external data storage devices as part of ensuring IS of bank information processes to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 1						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M10.10	Does the RF BS organisation define, comply with, record and monitor the procedures for accessing PD archives as part of ensuring IS of bank information processes to meet the requirements for personal data protection for second level PD protection during the processing in ISPD as established by the Decree of the Government of the Russian Federation No. 1119 'On approval of requirements for protection of personal data during their processing in personal data information systems' of 1 November 2012?	Required	Category 1						
M10.11	Has the RF BS organisation implemented protection for perimeters of computer network segments that host ISPD and control of information interaction between the segments of computer networks?	Required	Category 3						
M10.12	Does the RF BS organisation define and monitor the rules of information interaction between ISPD with other ABSs?	Required	Category 1						
M10.13	Does the RF BS organisation use in its ISPD the data protection tools certified in accordance with the requirements of the Order of the Federal Service for Technical and Export Control No. 21 'On approval of composition and content of organisational and technical measures for protection of personal data during their processing in personal data information systems' of 18 February 2013?	Required	Category 3						
M10.14	Has an employee of the RF BS organisation responsible for security of personal data in ISPD been designated for each ISPD?	Required	Category 2						
Final assessment of group indicator M10									

Group indicator M11 'Arrangement and functioning of the IS service in a RF BS organisation'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M11.1	Has the management established an IS service consisting of no less than two persons (have the authorised persons been designated) for implementing, operating, monitoring and maintaining IS Maintenance System at the appropriate level, have the goals and objectives of its activities been approved?	Required	Category 3						
M11.2	Has the management approved for the IS service the authority and resources necessary to perform the established goals and objectives?	Required	Category 3						
M11.3	Does the IS service have a supervisor appointed from among the management, who at the same time is not an IT (automation) service supervisor?	Required	Category 3						
M11.4	Has the IS service been allocated its own budget?	Recommended	Category 3						
M11.5	Has the RF BS organisations with a network of branches or regional representative offices formed local IS units (appointed authorised persons) and have these units been provided with necessary resources and regulatory framework?	Required	Category 1						
M11.6	Has the IS service been given the authority to arrange the preparation and monitor the performance of all IS plans in the RF BS organisation?	Required	Category 3						
M11.7	Has the IS service been given the authority to draft and submit proposals for changing IS policies of the RF BS organisation?	Required	Category 3						
M11.8	Has the IS service been given the authority to arrange changes in existing internal documents and adoption by the management of new internal documents regulating IS activities in the RF BS organisation?	Required	Category 3						
M11.9	Has the IS service been given the authority to define the requirements for measures to ensure IS in the RF BS organisation?	Required	Category 3						
M11.10	Has the IS service been given the authority to monitor the employees of the RF BS organisation in terms of their compliance with the requirements of internal documents regulating IS activities, primarily, the employees with maximum authority to access protected information assets?	Required	Category 3						
M11.11	Has the IS service been given the authority to monitor IS related events?	Required	Category 3						
M11.12	Has the IS service been given the authority to participate in the investigation of events related to IS incidents and, if necessary, submit proposals on applying sanctions against the persons who committed UA and URA (for example, violated the requirements of IS instructions and guidelines of the RF BS organisation)?	Required	Category 3						

M11.13	Has the IS service been given the authority to participate in activities aimed at restoring the operability of the ABS after failures and accidents?	Required	Category 3						
M11.14	Has the IS service been given the authority to monitor IS at the stages of ABS LC, including during testing and commissioning of ABS subsystems in the RF BS organisation?	Required	Category 3						
M11.15	Has the IS service been given the authority to participate in the creation, maintenance, operation and improvement of IS Maintenance System in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M11									

Group indicator M12 ‘Defining/correcting IS Maintenance System scope’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M12.1	Have the procedures for recording information assets structured by classes(types) been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M12.2	Is the classification of information assets based on assessing the value of information assets for the interests (objectives) of the RF BS organisation, such as in accordance with the severity of the consequences arising from the loss of IS properties in information assets?	Recommended	Category 3						
M12.3	Has the RF BS organisation established the criteria for allocating specific information assets to one or more types of information assets?	Required	Category 2						
M12.4	Have the procedures for recording the environment objects for each information asset and/or type of information asset covering all levels of information infrastructure of RF BS organisation, as defined in section 6 of STO BR IBBS-1.0, been defined, complied with, recorded and monitored?	Required	Category 1						
M12.5	Have the roles for recording the environment objects for each information asset and/or type of information asset covering all levels of information infrastructure of the RF BS organisation, as defined in section 6 of STO BR IBBS-1.0, been defined in the RF BS organisation?	Required	Category 3						
M12.6	Have the persons responsible for performing the roles for recording the environment objects for each information asset and/or type of information asset covering all levels of information infrastructure of the RF BS organisation, as defined in section 6 of STO BR IBBS-1.0, been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M12									

Group indicator M13 'Selecting/correcting the approach to IS breach risk assessment and conducting IS breach risk assessment'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M13.1	Has the methodology for assessing the risks of IS breaches/approach to assessing the risks of IS breaches been adopted and corrected in the RF BS organisation?	Required	Category 1						
M13.2	Have the criteria for accepting the risks of IS breaches and the level of acceptable risk of IS breaches been defined in the RF BS organisation?	Required	Category 2						
M13.3	Does the methodology for assessing the risks of IS breaches/approach to assessing the risks of IS breach define the method and procedure for qualitative or quantitative assessment of the risk of IS breaches based on assessing the following: - Probability of IS threats materialising as a result of identified and/or anticipated sources of IS threats recorded in the model of threats and violator following their impact on environment objects of information assets of the RF BS organisation (types of information assets); - Severity of the consequences arising from the loss of IS properties, in particular, such properties as availability, integrity and confidentiality of considered information assets (types of information assets)?	Required	Category 2						
M13.4	Does the procedure for assessing the risks of IS breaches define the procedures required assessing the risks of IS breaches, as well as the sequence of their performance?	Required	Category 2						
M13.5	Is there any assessment of risks of IS breaches performed with regard to IS properties of all information assets (types of information assets) within IS Maintenance System scope?	Required	Category 3						
M13.6	Do the levels of risks obtained following the assessment of risks of IS breaches match the level of acceptable risk adopted in the RF BS organisation?	Required	Category 3						
M13.7	Has the list of unacceptable risks of IS breaches, based on comparing the values obtained by assessing the risks of IS breaches with the level of acceptable risk adopted in the RF BS, been recorded in the RF BS organisation?	Required	Category 2						
M13.8	Have the roles, associated with the activities aimed at defining/correcting the methodologies used for assessing the risks of IS breaches/approach to assessing the risks of IS breaches, been defined in the RF BS organisation?	Required	Category 3						
M13.9	Have the persons responsible for performing the roles associated with the activities aimed at defining/correcting the methodologies used for assessing the risks of IS breaches/approach to assessing the risks of IS breaches, been designated?	Required	Category 3						
M13.10	Have the roles for assessing the risks of IS breaches been defined in the RF BS organisation?	Required	Category 3						
M13.11	Have the persons responsible for performing the roles for assessing the risks of IS breaches been designated?	Required	Category 3						
Final assessment of group indicator M13									

Group indicator M14 'Developing processing plans for risks of IS breaches'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M14.1	Has the plan establishing one of the possible ways of risk processing for each of unacceptable risks been defined in the RF BS organisation: - Transfer of risk to third-party organisations (e.g. through insurance of this risk); - Risk avoidance (e.g. by refraining from activities that give rise to the risk); - Informed acceptance of risk; - Preparing IS requirements that reduce the risk to an acceptable level, and preparing plans for implementing such requirements?	Required	Category 2						
M14.2	Have the plans for processing the risks of IS breaches been agreed with the head of the IS service or the person responsible for IS in the RF BS organisation?	Required	Category 2						
M14.3	Has the management of the RF BS organisation approved the plans for processing the risks of IS breaches?	Required	Category 2						
M14.4	Do the plans for implementing IS requirements include the sequence and periods for implementing and deploying organisational, technical and other safeguards?	Required	Category 3						
M14.5	Have the roles for developing the plans for processing the risks of IS breaches been defined in the RF BS organisation?	Required	Category 3						
M14.6	Have the persons responsible for performing the roles for developing the plans for processing the risks of IS breaches been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M14									

Group indicator M15 'Developing/correcting internal documents regulating activities in the IS area'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M15.1	Are the internal documents regulating IS activities in the RF BS organisation developed and corrected in accordance with the recommendations of the Bank of Russia for standardisation RS BR IBBS-2.0 'Maintenance of Information Security of the Russian Banking System Organisations' Methodological guidelines for documentation in the area of information security in accordance with the requirements of STO BR IBBS-1.0'?	Recommended	Category 3						
M15.2	Has the IS policy of the RF BS organisation been developed?	Required	Category 2						
M15.3	Has the IS policy of the RF BS organisation been approved by the management?	Required	Category 2						
M15.4	Has the IS policy of the RF BS organisation corrected?	Required	Category 3						
M15.5	Have individual IS policies of the RF BS organisation been developed?	Required	Category 2						
M15.6	Have individual IS policies of the RF BS organisation been corrected?	Required	Category 3						
M15.7	Have the documents regulating procedures for performing specific types of IS-related activities been developed in the RF BS organisation?	Required	Category 2						
M15.8	Are the documents regulating procedures for performing specific types of IS-related activities corrected in the RF BS organisation?	Required	Category 3						
M15.9	Have the list and forms of documents confirming the performance of IS activities been defined in the RF BS organisation?	Required	Category 2						
M15.10	Has the IS policy (individual IS policies) of the RF BS organisation defined the following: - Goals and objectives of ensuring IS; - Main areas of ensuring IS; - Main types of protected information assets; - Models of threats and violators; - Set of rules, requirements and guidelines in the area of IS; - Basic requirements for ensuring IS; - Principles of countering IS threats for the types of main protected information assets; - Basic principles of raising awareness and knowledge in the area of IS; - Guidelines for implementing and monitoring compliance with the requirements of IS policy?	Required	Category 2						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M15.11	Are the following corrected in IS policy (individual IS policies) of the RF BS organisation: - Goals and objectives of ensuring IS; - Main areas of ensuring IS; - Main types of protected information assets; - Models of threats and violators; - Set of rules, requirements and guidelines in the area of IS; - Basic requirements for ensuring IS; - Principles of countering IS threats for the types of main protected information assets; - Basic principles of raising awareness and knowledge in the area of IS; - Guidelines for implementing and monitoring compliance with the requirements of IS policy?	Required	Category 3						
M15.12	Are the internal documents regulating the activities in the area of IS based on the following: - Laws of the Russian Federation; - Comprehensive set of requirements of the Bank of Russia for IS of the banking system, in particular, the requirements of sections 7 and 8 of STO BR IBBS-1.0; - Regulatory acts and instructions issued by regulatory and supervisory authorities; - Third-party contractual requirements of the RF BS organisation; - Results of the risk assessment performed at the level of detail of considered information assets or types of information assets corresponding to the level of developed document?	Required	Category 3						
M15.13	Are the internal documents regulating the activities in the area of IS corrected based on the following: - Laws of the Russian Federation; - Comprehensive set of requirements of the Bank of Russia for IS of the banking system, in particular, the requirements of sections 7 and 8 of STO BR IBBS-1.0; - Regulatory acts and instructions issued by regulatory and supervisory authorities; - Third-party contractual requirements of the RF BS organisation; - Results of the risk assessment performed at the level of detail of considered information assets or types of information assets corresponding to the level of developed document?	Required	Category 3						
M15.14	Does the set of internal documents regulating the activities in the area of IS include the requirements for ensuring IS of all identified information assets or types of information assets within the scope of IS Maintenance System of the RF BS organisation?	Required	Category 3						
M15.15	Are the documents regulating the procedures for certain types of activities related to ensuring IS not in conflict with the provisions of IS policy and individual IS policies?	Required	Category 2						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M15.16	Do the documents regulating the procedures for certain types of activities related to ensuring IS detail the provisions of IS policy and individual IS policies?	Required	Category 3						
M15.17	Has the management of the RF BS organisation approved the procedure for IS service interaction (work coordination) with employees responsible for ensuring IS in structural units of the RF BS organisation (if structural units of the RF BS organisation have employees responsible for IS)?	Required	Category 2						
M15.18	Have the list of evidence confirming the performance of activities for ensuring IS and responsibility of employees of the RF BS organisation for performing these activities been defined within the documents regulating the activities for ensuring IS?	Required	Category 2						
M15.19	Have the procedures selecting and allocating the roles in the area of IS been defined in the RF BS organisation?	Required	Category 2						
M15.20	Has the procedure for developing, supporting, reviewing and monitoring the compliance with the internal documents regulating the activities for ensuring IS in the RF BS organisation been defined in the RF BS organisation?	Required	Category 2						
M15.21	Have the roles for developing, supporting, reviewing and monitoring the compliance with the internal documents regulating the activities for ensuring IS in the RF BS organisation been defined in the RF BS organisation?	Required	Category 3						
M15.22	Have the persons responsible for the roles for developing, supporting, reviewing and monitoring the compliance with the internal documents regulating the activities for ensuring IS in the RF BS organisation been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M15									

Group indicator M16 ‘RF BS organisation management adoption of IS Maintenance System implementation and operation decisions’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M16.1	Has the management recorded and approved the decisions on implementing and operating IS Maintenance System, in particular, the following decisions: - On analysing and accepting residual risks of IS breaches; - On planning the stages of implementing IS Maintenance System, in particular, the requirements set forth in sections 7 and 8 of STO BR IBBS-1.0; - On allocating the roles in the area of IS of the RF BS organisation; - On management adoption of plans for introduction of safeguards aimed at implementing the requirements of sections 7 and 8 of STO BR IBBS-1.0 and IS risk reduction; - On allocating resources necessary for implementing and operating IS Maintenance System?	Required	Category 2						
M16.2	Has the management approved all plans for implementing IS Maintenance System, in particular, the plans for implementing the requirements of sections 7 and 8 of STO BR IBBS-1.0, plans for processing the risks of IS breaches and introduction of safeguards, which plans define the following: - Sequence of measures taken within these plans; - Start and end dates of planned measures; - Officials (units) responsible for implementing each of these measures?	Required	Category 2						
M16.3	Has the procedure for developing, reviewing and monitoring the implementation of plans aimed at ensuring IS in the RF BS organisation been defined in the RF BS organisation?	Required	Category 2						
M16.4	Have the decisions of the management, related to the designation and allocation of roles for all structural units in accordance with the provisions of internal documents regulating the activities for ensuring IS in the RF BS organisation, been recorded?	Required	Category 2						
Final assessment of group indicator M16									

Group indicator M17 ‘Arranging the implementation of IS Maintenance System deployment plans’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M17.1	Have the procedures for designing/acquiring/deploying, implementing, operating, monitoring and following-up the operation of safeguards (ISS), provided by the plans for implementing the requirements of the IS, been defined, complied with, recorded and monitored in the RB BS organisation?	Required	Category 1						
M17.2	Are the safeguards, applied to environment objects in accordance with requirements to IS established in the RF BS organisation and stated in IS policy and other internal documents of the RF BS organisation, implemented when building the elements of ISS (with regard to specific area of activities of the RF BS organisation)?	Required	Category 1						
M17.3	Have the roles associated with the implementation of plans for processing the risks of IS breaches and implementation of required safeguards been defined?	Required	Category 3						
M17.4	Have the persons, responsible for performing the roles associated with the implementation of plans for processing the risks of IS breaches and implementation of required safeguards, been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M17									

Group indicator M18 'Developing and arranging the implementation of programmes for training and raising awareness in the area of IS'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M18.1	Has work with personnel and customers, authorised by the management of the RF BS organisation and aimed at improving the awareness and training in the area of IS, been arranged?	Required	Category 3						
M18.2	Have the plans and programmes, aimed at training and raising awareness in the area of IS, and which require checking the knowledge obtained following their completion, been developed?	Required	Category 1						
M18.3	Have the plans and programmes aimed at training and raising awareness established the requirements for periodic training and raising of awareness?	Required	Category 2						
M18.4	Are the programmes aimed at training and raising awareness of various groups of employees developed based on their official duties and performed roles? Do they include the following information: - Existing IS policies; - Protection measures applicable in the organisation; - Proper use of safeguards in accordance with the internal documents of the RF BS organisation; - Significance and importance of activities conducted by employees to ensure IS in the RF BS organisation?	Required	Category 2						
M18.5	Has the list of evidence, confirming the completion of programmes aimed at training and raising awareness in the area of IS, been defined in the RF BS organisation? In particular, such evidence may be as follows: - Documents (logs) confirming completion by executives and employees of the RF BS organisation of training in the area of IS along with the indication of the level of education, skills, experience and qualifications of trainees; - Documents containing the results of checks performed on the training of employees of the RF BS organisation; - Documents containing the results of checks performed with regard to awareness in the area of IS in the RF BS organisation.	Required	Category 2						
M18.6	Is the employee assigned a new role trained or briefed in the area of IS according to the assigned role?	Required	Category 3						
M18.7	Have the roles aimed at developing, implementing the plans and programmes for training and raising awareness in the area of IS and monitoring their results, been defined in the RF BS organisation?	Required	Category 3						
M18.8	Have the people responsible for performing the roles aimed at developing, implementing the plans and programmes for training and raising awareness in the area of IS and monitoring their results, been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M18									

Group indicator M19 'Arranging detection and response to IS incidents'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M19.1	Have the procedures for processing incidents been defined, complied with, recorded and monitored in the RF BS organisation, including: - Procedures for detecting IS incidents; - Procedures for reporting incidents, including informing the IT service; - Procedures for classification of incidents and assessment of damage caused to IS by the incident; - Procedures for responding to an incident; - Procedures for analysing the causes of IS incidents and assessing the results of responding to IS incidents (if necessary with the participation of external experts in the area of IS)?	Required	Category 1						
M19.2	Have the procedures for storage and distribution of information on IS incidents, practices for analysing IS incidents and results of responding to IS incidents been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M19.3	Have the procedures for actions of employees of the RF BS organisation when detecting unusual events associated with IS and the procedure for reporting such events, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M19.4	Are employees of the RF BS organisation aware of the procedure upon detection of unusual events associated with IS and the procedure for reporting such events?	Required	Category 3						
M19.5	Do the procedures for investigating the incidents take into account the current laws of the Russian Federation, provisions of regulatory acts of the Bank of Russia, as well as internal documents of the RF BS organisation in the area of IS?	Required	Category 3						
M19.6	Are the decisions on all detected incidents adopted, recorded and complied with in the RF BS organisation?	Required	Category 1						
M19.7	Have the roles for detection, classification, response, analysis and investigation of IS incidents been defined in the RF BS organisation?	Required	Category 3						
M19.8	Have the persons responsible for performing the roles for detection, classification, response, analysis and investigation of IS incidents been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M19									

Group indicator M20 ‘Arranging business continuity and its restoration after interruptions’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M20.1	Have the procedures for recording the information assets or types of information assets which are essential to ensure the business continuity of the RF BS organisation been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M20.2	Have the requirements for ensuring IS, regulating the issues of business continuity and its restoration after interruption, including requirements for measures aimed at restoring the necessary information, software, hardware, and communication channels, been established in the RF BS organisation?	Required	Category 2						
M20.3	Has the plan for business continuity and its restoration after possible interruption, containing instructions and procedures for employees of the RF BS organisation and including the following, been defined in the RF BS organisation: - Conditions for activating the plan; - Procedure for actions to be taken after an IS incident (instructions for personnel); - Restoration procedures; - Procedures for testing and verifying the plan; - Plan for training and raising awareness of employees of the RF BS organisation; - Obligations of employees of the RF BS organisation along with indication of persons responsible for implementing each provision of the plan?	Required	Category 2						
M20.4	Is the development of plans for ensuring business continuity and its restoration after interruption based on assessing the risks of IS breaches in the RF BS organisation with regard to information assets essential for ensuring business continuity and its restoration after interruption?	Required	Category 3						
M20.5	Are the safeguards for ensuring business continuity applied with regard to information assets essential for ensuring business continuity and its restoration after interruption?	Required	Category 3						
M20.6	Is the application of safeguards for ensuring business continuity and restoration after interruption based on the relevant requirements for ensuring IS?	Required	Category 3						
M20.7	Has the plan for ensuring business continuity and restoration after interruptions been reconciled with procedures for processing IS incidents existing in the RF BS organisation?	Required	Category 2						

M20.8	Have the procedures for periodic testing of the plan for ensuring business continuity and its restoration after interruption been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M20.9	Has the scenario of the testing plan for ensuring business continuity and restoration after interruption been prepared by taking into account the model of threats and violators existing in the RF BS organisation and results of risk assessment?	Required	Category 3						
M20.10	Is the plan for ensuring business continuity plan and restoration after interruption corrected, when necessary, based on test results?	Required	Category 3						
M20.11	Has the programme for training and raising the awareness of employees in the area of business continuity and restoration after interruptions been implemented in the RF BS organisation?	Required	Category 3						
M20.12	Have the roles for developing the business continuity plan and its restoration after interruption been defined in the RF BS organisation?	Required	Category 3						
M20.13	Have the persons responsible for the roles in developing the business continuity plan and its restoration after interruption been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M20									

Group indicator M21 'IS monitoring and safeguard control'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M21.1	Have the procedures for monitoring IS and safeguards (including the monitoring of configuration parameters and settings of tools and protection mechanisms), which cover all implemented and operated safeguards included in ISS and are arranged by IS service, been defined, complied with and recorded in the RF BS organisation?	Required	Category 1						
M21.2	Have the procedures for collecting and storing information on the actions of employees of the RF BS organisation, events and parameters related to the functioning of safeguards been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M21.3	Do the procedures for storing information on IS incidents take into account the information on all IS incidents detected during the monitoring of IS and safeguards?	Required	Category 3						
M21.4	Are the procedures for monitoring IS and safeguards subject to regular and recorded revisions due to changes in the composition and methods of using the safeguards, identification of new threats and vulnerabilities of IS, as well based on information on IS incidents?	Required	Category 3						
M21.5	Have the roles associated with implementing the procedures for monitoring IS and safeguards, as well as with the revision of such procedures, been defined in the RF BS organisation?	Required	Category 3						
M21.6	Have the persons responsible for the roles associated with implementing the procedures for monitoring IS and safeguards, as well as with the revision of such procedures, been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M21									

Group indicator M22 ‘Conducting IS self-assessment’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M22.1	Is the IS self-assessment performed independently and at the initiative of the RF BS organisation management?	Required	Category 3						
M22.2	Is the IS self-assessment performed in accordance with this standard?	Required	Category 3						
M22.3	Has the procedure for IS self-assessment been arranged in accordance with the recommendations of the Bank of Russia for standardisation RS BR IBBS-2.1 ‘Maintenance of Information Security of the Russian Banking System Organisations. Guidelines for Self-Assessment of Conformity of Information Security of the Russian Banking System Organisations to Requirements of STO BR IBBS-1.0-2014’?	Recommended	Category 3						
M22.4	Has a programme for IS self-assessment containing the information necessary for planning and arranging IS self-assessments, their monitoring, analysis and improvement, as well as for providing them with the resources necessary for efficient and effective performance of these IS self-assessments within the specified periods been established and implemented in the RF BS organisation?	Required	Category 1						
M22.5	Have the following procedures been defined, complied with, recorded and monitored in the RF BS organisation: - Generating, collecting and storing the evidence of IS self-assessment; - Complying with the established frequency of IS self-assessment; - Storing and distributing the results of IS self-assessment?	Required	Category 1						
M22.6	Has the IS self-assessment plan defining the following been established in the RF BS organisation for each IS self-assessment performed in the RF BS organisation: - Purpose of the IS self-assessment; - Entities and activities that are subject to IS self-assessment; - Procedure and period for taking IS self-assessment measures; - Distribution of roles among the employees of the RF BS organisation associated with IS self-assessment of IS?	Required	Category 2						
M22.7	Are the reports prepared following the IS self-assessment?	Required	Category 3						
M22.8	Are the results of IS self-assessment and relevant reports communicated to the management of the RF BS organisation?	Required	Category 3						
M22.9	Have the roles associated with implementing the IS self-assessment programme been defined in the RF BS organisation?	Required	Category 3						
M22.10	Have the persons responsible for the roles associated with implementing the IS self-assessment programme been designated in the RF BS organisation?	Required	Category 3						
M22.11	Does the RF BS organisation assess IS conformity in the form of IS self-assessment or IS audit no less than once every two years?	Required	Category 1						
Final assessment of group indicator M22									

Group indicator M23 'Performing an IS audit'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M23.1	Does the RF BS organisation perform an IS audit in accordance with the requirements of STO BR IBBS-1.1 'Maintenance of Information Security of the Russian Banking System Organisations. Information Security Audit' and STO BR IBBS-1.0?	Required	Category 3						
M23.2	Has a programme for IS audits containing the information necessary for planning and arranging IS audits, their monitoring, analysis and improvement, as well as for providing them with the resources necessary for efficient and effective performance of these IS audits within the specified periods been established and implemented in the RF BS organisation?	Required	Category 1						
M23.3	Has the IS audit plan defining the following been established in the RF BS organisation for each IS audit held in the RF BS organisation: - IS audit purpose; - IS audit criteria; - IS audit area; - Date and duration of the IS audit; - Audit team; - Description of activities and measures for IS audit; - Allocation of resources during the IS audit?	Required	Category 2						
M23.4	Have the contracts been concluded with auditing organisations with the following procedures included in such contracts: - Storage, access and use of materials obtained during IS audit; - Liaison with the auditing organisation during IS audit; - Liaison between the audit team and management that allows the representatives of the audit team to directly contact the management when needed; - Arrangements for interviews with employees; - Arrangements for monitoring the activities of employees of the RF BS organisation by representatives of the auditing organisation?	Required	Category 2						
M23.5	Are reports prepared following IS audits?	Required	Category 2						
M23.6	Are the results of IS audits and relevant reports communicated to the management of the RF BS organisation?	Required	Category 3						
M23.7	Have the procedures for storing, accessing and using materials obtained in the course of audits, in particular, the audit reports, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						

M23.8	Have the roles associated with the arrangements for implementing the audit programmes and plans for individual audits been defined in the RF BS organisation?	Required	Category 3						
M23.9	Have the persons responsible for the roles associated with the arrangements for implementing the audit programmes and plans for individual audits been designated in the RF BS organisation?	Required	Category 3						
M23.10	Does the RF BS organisation assess IS conformity in the form of IS audit or IS self-assessment no less than once every two years?	Required	Category 1						
Final assessment of group indicator M23									

Group indicator M24 'Analysing IS Maintenance System functioning'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M24.1	Have the procedures for analysing IS Maintenance System by using, among other things, the following been defined, complied with, recorded and monitored in the RF BS organisation: - Results of IS monitoring and safeguard control; - Details of IS incidents; - Results of IS audits, IS self-assessments; - Information on IS threats, possible violators and vulnerabilities; - Information on changes within the RF BS organisation, such as the information on changes in processes and technologies implemented as part of basic process flow, changes in internal documents of the RF BS organisation; - Information on changes outside the RF BS organisation, such as the information on changes in the laws of the Russian Federation, changes in the comprehensive set of requirements of the Bank of Russia for IS of the banking system, changes in contractual obligations of the RF BS organisation?	Required	Category 1						
M24.2	Is there any analysis of the comprehensive set of internal documents regulating the activities for ensuring IS in the RF BS organisation to the requirements of the laws of the Russian Federation, requirements of the Bank of Russia, contractual requirements of the organisation?	Required	Category 3						
M24.3	Is there any analysis of conformity of internal documents of the lower levels of hierarchy regulating the activities for ensuring IS in the RF BS organisation to the requirements of IS policies in the RF BS organisation?	Required	Category 3						
M24.4	Is there any assessment of IS risks of the RF BS organisation, including the assessment of residual and acceptable risks, as well as the assessment of adequacy of the model of threats of the RF BS organisation to existing IS threats?	Required	Category 3						
M24.5	Is there any assessment of the adequacy of safeguards to the requirements of internal documents of the RF BS organisation and the results of risk assessment?	Required	Category 3						
M24.6	Is there any analysis of the gaps in technological processes aimed at ensuring IS, as well as inconsistencies in the use of safeguards?	Required	Category 3						
M24.7	Have the roles associated with procedures for analysing the functioning of IS Maintenance System been defined in the RF BS organisation?	Required	Category 3						
M24.8	Have the persons responsible for the roles associated with procedures for analysing the functioning of IS Maintenance System been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M24									

Group indicator M25 'Analysing IS Maintenance System by the management of the RF BS organisation'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M25.1	Has the list of documents (data) required for preparing the information provided to the management in order to analyse IS Maintenance System been defined in the RF BS organisation?	Required	Category 2						
M25.2	Does the list of documents necessary for preparing the information provided to the management in order to analyse IS Maintenance System include reports with results of the following: - IS monitoring and safeguard control; - Analysis of IS Maintenance System functioning; - IS audits; - IS self-assessments?	Required	Category 3						
M25.3	Does the list of documents necessary for preparing the information provided to the management in order to analyse IS Maintenance System include documents with the following information: - Ways and methods of protection, safeguards or procedures for their use, which could be used to improve the functioning of IS Maintenance System; - Newly detected IS vulnerabilities and threats; - Actions taken following previous analyses of IS Maintenance System made by the management; - Changes that could affect the arrangements for IS Maintenance System, for example, changes to the laws of the Russian Federation and/or provisions of the standards of the Bank of Russia; - Detected IS incidents?	Required	Category 3						
M25.4	Does the list of documents necessary for preparing the information provided to the management in order to analyse IS Maintenance System include documents confirming the completion of required activities aimed at ensuring IS, such as the implementation of plans for processing the risks?	Required	Category 3						
M25.5	Does the list of documents necessary for preparing the information provided to the management in order to analyse IS Maintenance System include documents confirming the compliance with the requirements for business continuity and its restoration after interruption?	Required	Category 3						
M25.6	Has a plan for completing the activities aimed at monitoring and analysing IS Maintenance System been established in the RF BS organisation?	Required	Category 2						
M25.7	Does the plan for completing the activities aimed at monitoring and analysing IS Maintenance System include the provisions for holding management-level meetings, which, among other things, perform search and analysis of IS problems affecting the business of the RF BS organisation?	Required	Category 3						
M25.8	Have the roles associated with preparing the information necessary in order to analyse IS Maintenance System been defined in the RF BS organisation?	Required	Category 3						
M25.9	Have the persons responsible for the roles associated with preparing the information necessary in order to analyse IS Maintenance System been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M25									

*In case of any translation ambiguity the Russian version shall prevail.

Group indicator M26 ‘Adopting decisions on tactical improvements of IS Maintenance System’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M26.1	Are the results of the following considered when adopting decisions related to tactical improvements of IS: - IS audits; - IS self-assessments - IS monitoring and safeguard control; - Analysis of IS Maintenance System functioning; - Processing of IS incidents; - Detection of new IS threats and vulnerabilities; - Risk assessments; - Analysis of potential safeguards list; - Strategic improvements of IS Maintenance System; - Analysis of IS Maintenance System by the management; - Analysis of successful practices in the area of IS (proprietary or those of other organisations)?	Required	Category 3						
M26.2	Have the decisions on tactical improvements of IS Maintenance System, containing conclusions on the absence of need for tactical improvements of IS Maintenance System or areas of tactical improvements of IS Maintenance System, been documented?	Required	Category 2						
M26.3	Are the activities aimed at implementing the tactical improvements of IS Maintenance System recorded?	Required	Category 2						
M26.4	Have the plans for implementing the tactical improvements of IS Maintenance System been established in the RF BS organisation?	Required	Category 2						
M26.5	Does the RF BS organisation have any documents to record the results of performing the plans for implementing the tactical improvements of IS Maintenance System?	Required	Category 3						
M26.6	Does the management of the IS service in the RF BS organisation authorise and monitor activities related to implementing the tactical improvements of IS Maintenance System?	Required	Category 3						
M26.7	Have the procedures for agreeing and informing the stakeholders on tactical improvements of IS Maintenance System, in particular, on changes related to ensuring IS, responsibility in the area of IS, IS requirements, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M26.8	Have the roles been established and responsible persons designated with regard to decisions on implementation of tactical improvements of IS Maintenance System?	Required	Category 3						
Final assessment of group indicator M26									

Group indicator M27 'Adopting decisions on strategic improvements of IS Maintenance System'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M27.1	Are the results of the following considered when adopting decisions related to strategic IS Maintenance System improvements: - IS audits; - IS self-assessments - IS monitoring and safeguard control; - Analysis of IS Maintenance System functioning; - Processing of IS incidents; - Identification of new information assets of the RF BS organisation or their types; - Detection of new IS threats and vulnerabilities; - Risk assessments; - Review of the main IS risks; - Analysis of IS Maintenance System by the management; - Analysis of successful practices in the area of IS (proprietary or those of other organisations)?	Required	Category 3						
M27.2	Are the changes in business interests, goals and objectives of the RF BS organisation, contractual obligations of the RF BS organisation, as well as changes in the laws of the Russian Federation and regulatory acts of the Bank of Russia, considered when adopting decisions related to strategic improvements of IS Maintenance System?	Required	Category 2						
M27.3	Are the decisions on strategic improvements of IS Maintenance System, containing either conclusions on the absence of need for strategic improvements of IS Maintenance System or areas of strategic improvements of IS Maintenance System, documented in the RF BS organisation?	Required	Category 2						
M27.4	Are there any areas for strategic improvements of IS Maintenance System in the form of corrective or preventive actions established, such as: - Clarifying/reviewing IS goals and objectives defined within IS policy (individual IS policies) of the RF BS organisation; - Changing IS Maintenance System scope; - Reviewing models of threats and violators; - Changing approaches to IS risk assessment, criteria for accepting IS risk?	Required	Category 1						
M27.5	Are the activities aimed at implementing the strategic improvements of IS Maintenance System recorded?	Required	Category 3						
M27.6	Have the plans for implementing the strategic improvements of IS Maintenance System been established in the RF BS organisation?	Required	Category 2						
M27.7	Does the RF BS organisation have any documents to record the results of performing the plans for implementing the strategic improvements of IS Maintenance System?	Required	Category 2						
M27.8	Are the activities related to implementing the strategic improvements of IS Maintenance System agreed with the IS service, does the management of the RF BS organisation authorise and monitor such activities?	Required	Category 1						

M27.9	In the event of strategic improvements of IS Maintenance System, are the activities for implementing the relevant tactical improvements of IS Maintenance System performed for all necessary procedures aimed at ensuring IS, safeguards and relevant internal documents, in particular, is the following performed: - Elaborating the plans for tactical improvements of IS Maintenance System; - Clarifying the plans for processing risks; - Clarifying the programmes for implementing safeguards; - Clarifying the procedures for using safeguards?	Required	Category 3						
M27.10	Have the procedures for agreeing and informing the stakeholders on strategic improvements of IS Maintenance System, in particular, on changes related to ensuring IS, responsibility in the area of IS, IS requirements, been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M27.11	Have the roles been established and responsible persons designated with regard to implementation of decisions on strategic improvements of IS Maintenance System, in the event of their adoption?	Required	Category 2						
Final assessment of group indicator M27									

Group indicator M28 'Assessment of the activities of the management of the RF BS organisation aimed at supporting the functioning of the IS service of the RF BS organisation'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M28.1 (similar to M11.1)	Has the management formed an IS service consisting of at least two persons (have the authorised persons been appointed) for implementing, operating, monitoring and maintaining IS Maintenance System at the appropriate level, have the goals and objectives of its activities been approved?	Required	Category 3						
M28.2 (similar to M11.2)	Has the management approved for IS service the authority and resources necessary to perform the established goals and objectives?	Required	Category 3						
M28.3 (similar to M11.3)	Does the IS service have a supervisor appointed from among the management, who at the same time is not the IT (automation) service supervisor?	Required	Category 3						
M28.4 (similar to M11.4)	Has the IS service been allocated its own budget?	Recommended	Category 3						
M28.5 (similar to M11.5)	Have RF BS organisations with a network of branches or regional representative offices established local IS units (appointed authorised persons) and have these units been provided with the necessary resources and regulatory framework?	Required	Category 1						
M28.6 (similar to M11.6)	Has the IS service been given the authority to arrange the preparation and monitor the performance of all IS plans in the RF BS organisation?	Required	Category 3						
M28.7 (similar to M11.7)	Has the IS service been given the authority to draft and submit proposals for changing IS policies of the RF BS organisation?	Required	Category 3						
M28.8 (similar to M11.8)	Has the IS service been given the authority to arrange changes in existing internal documents and adoption by the management of new internal documents regulating IS activities in the RF BS organisation?	Required	Category 3						
M28.9 (similar to M11.9)	Has the IS service been given the authority to define the requirements for measures to ensure IS in the RF BS organisation?	Required	Category 3						
M28.10 (similar to M11.10)	Has the IS service been given the authority to monitor the employees of the RF BS organisation in terms of their compliance with the requirements of internal documents regulating IS activities, primarily, the employees with maximum authority to access protected information assets?	Required	Category 3						
M28.11 (similar to M11.11)	Has the IS service been given the authority to monitor IS related events?	Required	Category 3						

M28.12 (similar to M11.12)	Has the IS service been given the authority to participate in the investigation of events related to IS incidents and, if necessary, submit proposals on applying sanctions against the persons who committed UA and URA (for example, violated the requirements of IS instructions and guidelines of the RF BS organisation)?	Required	Category 3						
M28.13 (similar to M11.13)	Has the IS service been given the authority to participate in activities aimed at restoring the operability of the ABS after failures and accidents?	Required	Category 3						
M28.14 (similar to M11.15)	Has the IS service been given the authority to participate in the creation, maintenance, operation and improvement of IS Maintenance System in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M28									

Group indicator M29 'Activities of the management of the RF BS organisation aimed at adopting the decisions on IS Maintenance System implementation and operation decisions'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M29.1 (similar to M16.1)	Has the management recorded and approved the decisions on implementing and operating IS Maintenance System, in particular, the following decisions: - On analysing and accepting residual risks of IS breaches; - On planning the stages of implementing IS Maintenance System, in particular, the requirements set forth in sections 7 and 8 of STO BR IBBS-1.0; - On allocating the roles in the area of IS of the RF BS organisation; - On management adoption of plans for introduction of safeguards aimed at implementing the requirements of sections 7 and 8 of STO BR IBBS-1.0 and IS risk reduction; - On allocating resources necessary for implementing and operating IS Maintenance System?	Required	Category 2						
M29.2 (similar to M16.2)	Has the management approved all plans for implementing IS Maintenance System, in particular, the plans for implementing the requirements of sections 7 and 8 of STO BR IBBS-1.0, plans for processing the risks of IS breaches and introduction of safeguards, which plans define the following: - Sequence of measures taken within these plans; - Start and end dates of planned measures; - Officials (units) responsible for implementing each of these measures?	Required	Category 2						
M29.3 (similar to M16.3)	Has the procedure for developing, reviewing and monitoring the implementation of plans aimed at ensuring IS in the RF BS organisation been defined in the RF BS organisation?	Required	Category 2						
M29.4 (similar to M16.4)	Have the decisions of the management, related to the designation and allocation of roles for all structural units in accordance with the provisions of internal documents regulating the activities for ensuring IS in the RF BS organisation, been recorded?	Required	Category 2						
Final assessment of group indicator M29									

*In case of any translation ambiguity the Russian version shall prevail.

Group indicator M30 'Assessment of activities of the management of the RF BS organisation aimed at supporting IS Maintenance System planning'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M30.1 (similar to M12.1)	Have the procedures for recording information assets structured by classes(types) been defined, complied with, recorded and monitored in the RF BS organisation?	Required	Category 1						
M30.2 (similar to M12.5)	Have the roles for recording the environment objects for each information asset and/or type of information asset covering all levels of information infrastructure of the RF BS organisation, as defined in section 6 of STO BR IBBS-1.0, been defined in the RF BS organisation?	Required	Category 3						
M3O.3 (similar to M12.6)	Have the persons responsible for performing the roles for recording the environment objects for each information asset and/or type of information asset covering all levels of information infrastructure of the RF BS organisation, as defined in section 6 of STO BR IBBS-1.0, been designated in the RF BS organisation?	Required	Category 3						
M30.4 (similar to M13.1)	Has the methodology for assessing the risks of IS breaches/approach to assessing the risks of IS breaches been adopted and corrected in the RF BS organisation?	Required	Category 1						
M30.5 (similar to M13.2)	Have the criteria for accepting the risks of IS breaches and the level of acceptable risk of IS breaches been defined in the RF BS organisation?	Required	Category 2						
M30.6 (similar to M13.4)	Does the procedure for assessing the risks of IS breaches define the procedures required assessing the risks of IS breaches, as well as the sequence of their performance?	Required	Category 2						
M30.7 (similar to M13.8)	Have the roles, associated with the activities aimed at defining/correcting the methodologies used for assessing the risks of IS breaches/approach to assessing the risks of IS breaches, been defined in the RF BS organisation?	Required	Category 3						
M30.8 (similar to M13.9)	Have the persons responsible for performing the roles associated with the activities aimed at defining/correcting the methodologies used for assessing the risks of IS breaches/approach to assessing the risks of IS breaches, been designated?	Required	Category 3						
M30.9 (similar to M13.10)	Have the roles for assessing the risks of IS breaches been defined in the RF BS organisation?	Required	Category 3						
M30.10 (similar to M13.11)	Have the persons responsible for performing the roles for assessing the risks of IS breaches been designated?	Required	Category 3						
M30.11 (similar to M14.3)	Has the management of the RF BS organisation approved the plans for processing the risks of IS breaches?	Required	Category 2						
M30.12 (similar to M14.5)	Have the roles for developing the plans for processing the risks of IS breaches been defined in the RF BS organisation?	Required	Category 3						
M30.13 (similar to M14.6)	Have the persons responsible for performing the roles for developing the plans for processing the risks of IS breaches been designated in the RF BS organisation?	Required	Category 3						
M30.14 (similar to M15.2)	Has the IS policy of the RF BS organisation been developed?	Required	Category 2						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M30.15 (similar to M15.3)	Has the IS policy of the RF BS organisation been approved by the management?	Required	Category 2						
M30.16 (similar to M15.4)	Has the IS policy of the RF BS organisation been corrected?	Required	Category 3						
M30.17 (similar to M15.5)	Have individual IS policies of the RF BS organisation been developed?	Required	Category 2						
M30.18 (similar to M15.6)	Are individual IS policies of the RF BS organisation corrected?	Required	Category 3						
M30.19 (similar to M15.10)	Has the IS policy (individual IS policies) of the RF BS organisation defined the following: - Goals and objectives of ensuring IS; - Main areas of ensuring IS; - Main types of protected information assets; - Models of threats and violators; - Set of rules, requirements and guidelines in the area of IS; - Basic requirements for ensuring IS; - Principles of countering IS threats for the types of main protected information assets; - Basic principles of raising awareness and knowledge in the area of IS; - Guidelines for implementing and monitoring compliance with the requirements of IS policy?	Required	Category 2						
M30.20 (similar to M15.11)	Are the following corrected in IS policy (individual IS policies) of the RF BS organisation: - Goals and objectives of ensuring IS; - Main areas of ensuring IS; - Main types of protected information assets; - Models of threats and violators; - Set of rules, requirements and guidelines in the area of IS; - Basic requirements for ensuring IS; - Principles of countering IS threats for the types of main protected information assets; - Basic principles of raising awareness and knowledge in the area of IS; - Guidelines for implementing and monitoring compliance with the requirements of IS policy?	Required	Category 3						
M30.21 (similar to M15.12)	Are the internal documents regulating the activities in the area of IS based on the following: - Laws of the Russian Federation; - Comprehensive set of requirements of the Bank of Russia for IS of the banking system, in particular, the requirements of sections 7 and 8 of STO BR IBBS-1.0; - Regulatory acts and instructions issued by regulatory and supervisory authorities; - Third-party contractual requirements of the RF BS organisation; - Results of the risk assessment performed at the level of detail of considered information assets or types of information assets corresponding to the level of developed document?	Required	Category 3						

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M30.22 (similar to M15.13)	Are the internal documents regulating the activities in the area of IS corrected based on the following: - Laws of the Russian Federation; - Comprehensive set of requirements of the Bank of Russia for IS of the banking system, in particular, the requirements of sections 7 and 8 of STO BR IBBS-1.0; - Regulatory acts and instructions issued by regulatory and supervisory authorities; - Third-party contractual requirements of the RF BS organisation; - Results of the risk assessment performed at the level of detail of considered information assets or types of information assets corresponding to the level of developed document?	Required	Category 3						
M30.23 (similar to M15.17)	Has the management of the RF BS organisation approved the procedure for IS service interaction (work coordination) with employees responsible for ensuring IS in structural units of the RF BS organisation (if structural units of the RF BS organisation have employees responsible for IS)?	Required	Category 2						
M30.24 (similar to M15.19)	Have the procedures selecting and allocating the roles in the area of IS been defined in the documents of the RF BS organisation?	Required	Category 2						
M30.25 (similar to M15.21)	Have the roles for developing, supporting, reviewing and monitoring the compliance with the internal documents regulating the activities for ensuring IS in the RF BS organisation been defined in the RF BS organisation?	Required	Category 3						
M30.26 (similar to M15.22)	Have the persons responsible for the roles for developing, supporting, reviewing and monitoring the compliance with the internal documents regulating the activities for ensuring IS in the RF BS organisation been designated in the RF BS organisation?	Required	Category 3						
M30.27 (similar to M17.3)	Have the roles associated with the implementation of plans for processing the risks of IS breaches and implementation of required safeguards been defined?	Required	Category 3						
M30.28 (similar to M17.4)	Have the persons, responsible for performing the roles associated with the implementation of plans for processing the risks of IS breaches and implementation of required safeguards, been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M30									

Group indicator M31 'Assessment of activities of the management of the RF BS organisation aimed at supporting IS Maintenance System implementation'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M31.1 (similar to M18.1)	Has work with personnel and customers, authorised by the management of the RF BS organisation and aimed at improving the awareness and training in the area of IS, been arranged?	Required	Category 3						
M31.2 (similar to M18.2)	Have the plans and programmes, aimed at training and raising awareness in the area of IS, and which require checking the knowledge obtained following their completion, been developed?	Required	Category 1						
M31.3 (similar to M18.7)	Have the roles aimed at developing, implementing the plans and programmes for training and raising awareness in the area of IS and monitoring their results, been defined in the RF BS organisation?	Required	Category 3						
M31.4 (similar to M18.8)	Have the people responsible for performing the roles aimed at developing, implementing the plans and programmes for training and raising awareness in the area of IS and monitoring their results, been designated in the RF BS organisation?	Required	Category 3						
M31.5 (similar to M19.7)	Have the roles for detection, classification, response, analysis and investigation of IS incidents been defined in the RF BS organisation?	Required	Category 3						
M31.6 (similar to M19.8)	Have the persons responsible for performing the roles for detection, classification, response, analysis and investigation of IS incidents been designated in the RF BS organisation?	Required	Category 3						
M31.7 (similar to M20.3)	Has the plan for business continuity and its restoration after possible interruption, containing instructions and procedures for employees of the RF BS organisation and including the following, been defined in the RF BS organisation: - Conditions for activating the plan; - Procedure for actions to be taken after an IS incident (instructions for personnel); - Restoration procedures; - Procedures for testing and verifying the plan; - Plan for training and raising awareness of employees of the RF BS organisation; - Obligations of employees of the RF BS organisation along with indication of persons responsible for implementing each provision of the plan?	Required	Category 2						
M31.8 (similar to M20.12)	Have the roles for developing the business continuity plan and its restoration after interruption been defined in the RF BS organisation?	Required	Category 3						
M31.9 (similar to M20.13)	Have the persons responsible for the roles in developing the business continuity plan and its restoration after interruption been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M31									

Group indicator M32 'Assessment of activities of the management of the RF BS organisation aimed at supporting IS Maintenance System audit'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M32.1 (similar to M21.5)	Have the roles associated with implementing the procedures for monitoring IS and safeguards, as well as with the revision of such procedures, been defined in the RF BS organisation?	Required	Category 3						
M32.2 (similar to M21.6)	Have the persons responsible for the roles associated with implementing the procedures for monitoring IS and safeguards, as well as with the revision of such procedures, been designated in the RF BS organisation?	Required	Category 3						
M32.3 (similar to M22.4)	Has a programme for IS self-assessment containing the information necessary for planning and arranging IS self-assessments, their monitoring, analysis and improvement, as well as for providing them with the resources necessary for efficient and effective performance of these IS self-assessments within the specified periods been established and implemented in the RF BS organisation?	Required	Category 1						
M32.4 (similar to M22.8)	Are the results of IS self-assessment and relevant reports communicated to the management of the RF BS organisation?	Required	Category 3						
M32.5 (similar to M22.9)	Have the roles associated with implementing the IS self-assessment programme been defined in the RF BS organisation?	Required	Category 3						
M32.6 (similar to M22.10)	Have the persons responsible for the roles associated with implementing the IS self-assessment programme been designated in the RF BS organisation?	Required	Category 3						
M32.7 (similar to M22.11, M23.10)	Does the RF BS organisation assess IS conformity in the form of IS self-assessment or IS audit no less than once every two years?	Required	Category 1						
M32.8 (similar to M23.2)	Has a programme for IS audits containing the information necessary for planning and arranging IS audits, their monitoring, analysis and improvement, as well as for providing them with the resources necessary for efficient and effective performance of these IS audits within the specified periods been established and implemented in the RF BS organisation?	Required	Category 1						
M32.9 (similar to M23.6)	Are the results of IS audits and relevant reports communicated to the management of the RF BS organisation?	Required	Category 3						
M32.10 (similar to M23.8)	Have the roles associated with the arrangements for implementing the audit programmes and plans for individual audits been defined in the RF BS organisation?	Required	Category 3						
M32.11 (similar to M23.9)	Have the persons responsible for the roles associated with the arrangements for implementing the audit programmes and plans for individual audits been designated in the RF BS organisation?	Required	Category 3						
M32.12 (similar to M24.7)	Have the roles associated with procedures for analysing the functioning of IS Maintenance System been defined in the RF BS organisation?	Required	Category 3						
M32.13 (similar to M24.8)	Have the persons responsible for the roles associated with procedures for analysing the functioning of IS Maintenance System been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M32									

Group indicator M33 'Assessment of activities of the management of the RF BS organisation aimed at supporting IS Maintenance System analysis'

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M33.1 (similar to M25.1)	Has the list of documents (data) required for preparing the information provided to the management in order to analyse IS Maintenance System been defined in the RF BS organisation?	Required	Category 2						
M33.2 (similar to M25.2)	Does the list of documents necessary for preparing the information provided to the management in order to analyse IS Maintenance System include reports with results of the following: - IS monitoring and safeguard control; - Analysis of IS Maintenance System functioning; - IS audits; - IS self-assessments?	Required	Category 3						
M33.3 (similar to M25.3)	Does the list of documents necessary for preparing the information provided to the management in order to analyse IS Maintenance System include documents with the following information: - Ways and methods of protection, safeguards or procedures for their use, which could be used to improve the functioning of IS Maintenance System; - Newly detected IS vulnerabilities and threats; - Actions taken following previous analyses of IS Maintenance System made by the management; - Changes that could affect the arrangements for IS Maintenance System, for example, changes to the laws of the Russian Federation and/or provisions of the standards of the Bank of Russia; - Detected IS incidents?	Required	Category 3						
M33.4 (similar to M25.4)	Does the list of documents necessary for preparing the information provided to the management in order to analyse IS Maintenance System include documents confirming the completion of required activities aimed at ensuring IS, such as the implementation of plans for processing the risks?	Required	Category 3						
M33.5 (similar to M25.5)	Does the list of documents necessary for preparing the information provided to the management in order to analyse IS Maintenance System include documents confirming the compliance with the requirements for business continuity and its restoration after interruption?	Required	Category 3						
M33.6 (similar to M25.6)	Has a plan for completing the activities aimed at monitoring and analysing IS Maintenance System been established in the RF BS organisation?	Required	Category 2						

M33.7 (similar to M25.7)	Does the plan for completing the activities aimed at monitoring and analysing IS Maintenance System include the provisions for holding management-level meetings, which, among other things, perform search and analysis of IS problems affecting the business of the RF BS organisation?	Required	Category 3						
M33.8 (similar to M25.8)	Have the roles associated with preparing the information necessary in order to analyse IS Maintenance System been defined in the RF BS organisation?	Required	Category 3						
M33.9 (similar to M25.9)	Have the persons responsible for the roles associated with preparing the information necessary in order to analyse IS Maintenance System been designated in the RF BS organisation?	Required	Category 3						
Final assessment of group indicator M33									

Group indicator M34 ‘Assessment of activities of the management of the RF BS organisation aimed at improving IS Maintenance System’

IS individual indicator code	Individual IS indicator	Requirement to complete	Audit category of individual indicator	Assessment of individual IS indicator					
				0	0.25	0.5	0.75	1	N/A
M34.1 (similar to M26.6)	Does the management of the IS service in the RF BS organisation authorise and monitor activities related to implementing the tactical improvements of IS Maintenance System?	Required	Category 3						
M34.2 (similar to M26.8)	Have the roles been established and responsible persons designated with regard to decisions on implementation of tactical improvements of IS Maintenance System?	Required	Category 3						
M34.3 (similar to M27.8)	Are the activities related to implementing the strategic improvements of IS Maintenance System agreed with the IS service, does the management of the RF BS organisation authorise and monitor such activities?	Required	Category 2						
M34.4 (similar to M27.11)	Have the roles been established and responsible persons designated with regard to implementation of decisions on strategic improvements of IS Maintenance System, in the event of their adoption?	Required	Category 2						
Final assessment of group indicator M34									

*In case of any translation ambiguity the Russian version shall prevail.

Annex B
(Mandatory)
Forms for collecting IS audit evidence

IS individual indicator code	Sources of evidence and IS audit evidence (documents, results of interviews or observations)	Who provided the IS audit evidence	Signature of employee/executive	Date

(Signature)

(Signature)

(Signature)

Annex C
(Mandatory)
Table of conformity of individual indicators and requirements for data protection for money transfers specified in Annex 2 to the Regulations of the Bank of Russia No. 382-P of June 9, 2012 and considered in the assessment of individual indicators

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of June 9, 2012	Sub-item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M1.3	P. 32	2.6.4	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure that their employees are granted the minimum access rights to protected information required to perform their functional duties
M1.4	P. 1	2.4.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of persons with access rights to protected information
	P. 2	2.4.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of persons with the rights to manage cryptographic keys
	P. 3	2.4.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of persons with the rights to influence information infrastructure objects, which can lead to disruption in the provision of money transfer services, with the exception of ATMs, payment terminals and electronic means of payment
	P. 4	2.4.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of their employees with the rights to generate electronic messages
M1.7	P. 5	2.4.2	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the implementation of the prohibition on the simultaneous performance by one person of the roles associated with the creation (upgrading) of information infrastructure object and operation of information infrastructure object
M1.8	P. 6	2.4.2	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the implementation of the prohibition on simultaneous performance by one person of the roles associated with the operation of information infrastructure object in terms of its use for intended purpose and operation of information infrastructure object in terms of its maintenance and repairs
M1.11	P. 1	2.4.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of persons with access rights to protected information
	P. 2	2.4.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of persons with the rights to manage cryptographic keys
	P. 3	2.4.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of persons with the rights to influence information infrastructure objects, which can lead to disruption in the provision of money transfer services, with the exception of ATMs, payment terminals and electronic means of payment

*In case of any translation ambiguity the Russian version shall prevail.

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
	P. 4	2.4.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of their employees with the rights to generate electronic messages
	P. 7	2.4.3	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the monitoring and registration of actions performed by persons assigned with the roles defined in sub-clause 2.4.1 of clause 2.4 of the Regulations of the Bank of Russia No. 382-P of 9 June 2012 (hereinafter, the "Regulations")
M2.2	P. 9	2.5.2	The money transfer operator, bank payment agent (sub-agent), being a legal entity, payment infrastructure services operator ensure the participation of the information security service in the development and agreement of requirements specifications for creating (upgrading) the information infrastructure objects
	P. 10	2.5.3	The money transfer operator, bank payment agent (sub-agent), being a legal entity, payment infrastructure services operator ensure the monitoring by the information security service of compliance of created (upgraded) information infrastructure objects with the requirement specifications
M2.4	P. 8	2.5.1	The money transfer operator, payment infrastructure services operator ensure the inclusion of requirements for information protection during money transfers in the requirement specifications for creating (upgrading) information infrastructure objects
M2.5	P. 14	2.5.5	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the implementation of the prohibition on the use of protected information at the stage of creating the information infrastructure objects
M2.6	P. 11	2.5.4	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the availability of electronic documentation for information protection equipment
M2.10	P. 12	2.5.4	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the monitoring of compliance with the requirements set forth in the electronic documentation for information protection equipment throughout the entire period of its operation
	P. 15	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the implementation of the prohibition on unauthorised copying of protected information
	P. 16	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the protection of backup copies of protected information
	P. 17	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the destruction of protected information in cases when this information is no longer used, except for protected information that is transferred to the archives, the maintenance and safety of which are provided by the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia, rules of the payment system and/or contracts concluded by the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
	P. 54	2.8.1	When using the Internet for money transfers, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the application of organisational measures aimed at protecting the information and/or use of information protection equipment designed to prevent unauthorised access to protected information through the use of software vulnerabilities
M2.11	P. 13	2.5.4	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the restoration of functioning of information protection equipment used in money transfers in the event of faults and/or failures in their operation
	P. 71	2.10.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure record-keeping and monitoring of software installed and/or used in computing equipment
M2.15	P. 38	2.6.8	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the adoption of measures aimed at preventing the theft of protected information media
M2.16	P. 16	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the protection of backup copies of protected information
	P. 17	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the destruction of protected information in cases when this information is no longer used, except for protected information that is transferred to the archives, the maintenance and safety of which are provided by the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia, rules of the payment system and/or contracts concluded by the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator
M2.18	P. 15	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the implementation of the prohibition on unauthorised copying of protected information
M2.19	P. 15	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the implementation of the prohibition on unauthorised copying of protected information
	P. 16	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the protection of backup copies of protected information
	P. 17	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the destruction of protected information in cases when this information is no longer used, except for protected information that is transferred to the archives, the maintenance and safety of which are provided by the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia, rules of the payment system and/or contracts concluded by the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M3.1	P. 18	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the destruction of protected information, including the information in the archives, by using a method that prevents its restoration
M3.3	P. 19	2.6.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the record-keeping of information infrastructure objects used for processing, storage and/or transfer of protected information, including ATMs and payment terminals
	P. 20	2.6.2	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the application non-cryptographic tools for protecting the information from unauthorised access, including the tools that passed their conformity assessment in accordance with the established procedure
M3.7	P. 21	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure compliance with the procedures for identification, authentication, authorisation of their employees when accessing the protected information
	P. 22	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the identification, authentication, authorisation of payment system members during money transfers
	P. 26	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent) ensure compliance with the procedures for identification, authentication, authorisation of persons accessing ATM and payment terminal software
	P. 29.3	2.6.3	The money transfer operator defines the following in the internal documents: The procedure for generating unique customer identifier in the automated system, software; list of codes established for customer actions performed during money transfers by using the automated system, software; device identifier to be registered; The procedure for registration and storage of information specified in paragraphs 13-16 of sub-clause 2.6.3 of clause 2.6 of the Regulations
M3.9	P. 25	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of actions related to assignment and distribution of rights to access the protected information
	P. 29	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent), ensure the registration of actions performed by the customers with the use of automated systems, software The bank payment agent (sub-agent) ensures the registration of actions performed by customers with the use of automated systems, software subject to technical capability and given the performed list of operations and used automated systems, software, the operation of which is provided by the bank payment agent (sub-agent)

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M3.10	P. 29.4	2.6.3	The money transfer operator defines the requirements for procedure, form and period established for providing it with information on actions performed by the customers with the use of automated systems, software and registered by the bank payment agents (sub-agents)
M3.11	P. 23	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the determination of the procedure for the use of information required to perform the authentication
M3.21	P. 31	2.6.4	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the implementation of the prohibition on unauthorised extension of access rights to protected information
M3.22	P. 24	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of actions when their employees access protected information
	P. 28	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of these Regulations, the money transfer operator, bank payment agent (sub-agent) ensure the registration of actions related to the assignment and allocation of customer rights provided to the customers in automated systems and software
	P. 29.1	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent) ensure the registration of the following information on actions performed by the customers with the use of automated systems, software: date (day, month, year) and time (hours, minutes, seconds) of actions performed by the customer; customer ID; code corresponding to performed action; device ID
	P. 30	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator ensures the registration of actions performed with information on bank accounts, including operations for opening and closing bank accounts
M3.24	P. 29.2	2.6.3	The money transfer operator ensures the storage of information specified in paragraphs 13- 16 of sub-clause 2.6.3 of clause 2.6 of the Regulations for no less than five years from the date of the action performed by the customer with the use of automated system, software
	P. 29.3	2.6.3	The money transfer operator defines the following in the internal documents: The procedure for generating unique customer identifier in the automated system, software; list of codes established for customer actions performed during money transfers by using the automated system, software; device identifier to be registered; the procedure for registration and storage of information specified in paragraphs 13-16 of sub-clause 2.6.3 of clause 2.6 of these Regulations

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M3.27	P. 29.1	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent) ensure the registration of the following information on actions performed by the customers with the use of automated systems, software: date (day, month, year) and time (hours, minutes, seconds) of actions performed by the customer; customer ID; code corresponding to performed action; device ID
M3.3O	P. 29.2	2.6.3	The money transfer operator ensures the storage of information specified in paragraphs 13-16 of sub-clause 2.6.3 of clause 2.6 of the Regulations for no less than five years from the date of the action performed by the customer with the use of automated system, software
M3.38	P. 27	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent) ensure compliance with the procedures for identification and monitoring of activities performed by persons maintaining ATMs and payment terminals
	P. 33	2.6.5	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator adopt and record in their internal documents the decisions on the need to apply organisational measures aimed at protecting information and/or use information protection equipment designed for monitoring physical access to information infrastructure objects (with the exception of ATMs, payment terminals and electronic means of payment), the faults and/or failures in operation of which make it impossible to provide services for money transfers or cause delayed money transfers, as well as for monitoring access to buildings and premises that host them
	P. 34	2.6.5	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator adopt and record in their internal documents the decisions on the need to apply organisational measures aimed at protecting information and/or use information protection equipment designed for preventing the physical impact on computing and telecommunication equipment, the faults and/or failures in operation of which make it impossible to provide services for money transfers or cause delayed money transfers, with the exception of ATMs, payment terminals and electronic means of payment
	P. 35	2.6.5	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator adopt and record in their internal documents the decisions on the need to apply organisational measures aimed at protecting information and/or use information protection equipment designed for registering access to ATMs, including by using video surveillance systems
	P. 36	2.6.6	If the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator adopt the decision on the need to apply organisational measures aimed at protecting information and/or use information protection equipment specified in sub-clause 2.6.5 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the application of these organisational measures aimed at protecting information and/or use information protection equipment

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M3.39	P. 25	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the registration of actions related to assignment and distribution of rights to access the protected information
	P. 29	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator, bank payment agent (sub-agent), ensure the registration of actions performed by the customers with the use of automated systems, software The bank payment agent (sub-agent) ensures the registration of actions performed by customers with the use of automated systems, software subject to technical capability and given the performed list of operations and used automated systems, software, the operation of which is provided by the bank payment agent (sub-agent)
	P. 30	2.6.3	When accessing protected information located on information infrastructure objects specified in sub-clause 2.6.1 of clause 2.6 of the Regulations, the money transfer operator ensures the registration of actions performed with information on bank accounts, including operations for opening and closing bank accounts
M3.53	P. 52	2.8.1	When using the Internet for money transfers, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the application of organisational measures aimed at protecting the information and/or use of information protection equipment designed to prevent access to the content of protected information transmitted over the Internet
M4.1	P. 40	2.7.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the use of information protection equipment against the impact of malicious code on computing equipment, including ATMs and payment terminals, when technically feasible
M4.2	P. 41	2.7.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure regular updates of the versions of information protection equipment used against the impact of malicious code and databases used by information protection equipment against the impact of malicious code and containing the description of malicious code and methods for neutralising it
M4.3	P. 42	2.7.1	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the functioning of information protection equipment used against the impact of malicious code in automatic mode, when technically feasible
M4.5	P. 43	2.7.2	The money transfer operator ensures the preparation of recommendations for customer on protecting information from the impact of malicious code
M4.7	P. 44	2.7.3	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the use of information protection equipment designed against the impact of malicious code and produced by different manufacturers and its separate installation on computers and servers used for money transfers, as well as on firewalls involved in money transfers, when technically feasible

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M4.8	P. 45	2.7.4	When technically feasible, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the performance of preliminary checks for the absence of malicious code in software which is being installed or modified on computing equipment, including ATMs and payment terminals
M4.9	P. 46	2.7.4	When technically feasible, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the performance of checks for the absence of malicious code in computing equipment, including ATMs and payment terminals, after the installation or modification of software
M4.10	P. 47	2.7.5	In the event that malicious code or actual impact of malicious code is detected, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the adoption of measures aimed at preventing the spread of such malicious code
	P. 48	2.7.5	In the event that malicious code or actual impact of malicious code is detected, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the adoption of measures aimed at eliminating the impact of the malicious code
	P. 49	2.7.5	When necessary, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator shall suspend money transfers while the consequences of malicious code infection are eliminated
	P. 50	2.7.5	In the event that any malicious code or actual impact of any malicious code is detected, the money transfer operator, payment infrastructure services operator shall inform the payment system operator
	P. 51	2.7.5	In the event that any malicious code or actual impact of any malicious code is detected, the payment system operator shall inform the payment infrastructure services operators and payment system members
M5.7	P. 52	2.8.1	When using the Internet for money transfers, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the application of organisational measures aimed at protecting the information and/or use of information protection equipment designed to prevent access to the content of protected information transmitted over the Internet
M5.8	P. 53	2.8.1	When using the Internet for money transfers, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the application of organisational measures aimed at protecting the information and/or use of information protection equipment designed to prevent unauthorised access to protected information on information infrastructure objects by using the Internet
	P. 56	2.8.1	When using the Internet for money transfers, the money transfer operator, the bank payment agent (sub-agent), payment infrastructure services operator ensure network packet filtering in the exchange of information between computing networks hosting information infrastructure objects and the Internet
M5.9	P. 57	2.8.2	The money transfer operator ensures the generation of recommendations for customers aimed at protecting information from unauthorised access through the use of false (spoofed) Internet resources

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M5.24	P. 55	2.8.1	When using the Internet for money transfers, the money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator ensure the reduction of the severity of consequences resulting from the impact on information infrastructure objects in order to create conditions for rendering impossible the provision of money transfer services or delaying money transfers
M6.1	P. 70	2.9.5	The payment systems operator determines the need to use DET, unless otherwise provided for by federal laws and other regulatory legal acts of the Russian Federation
M6.3	P. 58	2.9.1	Works on ensuring information protection by using DET are performed in accordance with Federal law No. 63-FZ 'On electronic signature' of 6 April 2011, the Regulations on development, production, implementation and operation of encryption (cryptographic) information protection tools (Regulations PKZ-2005) approved by Order of the Federal Security Service of the Russian Federation No. 66 of 9 February 2005 and technical documentation on DET
M6.6	P. 60	2.9.2	The money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall apply DET which allow DET integration in the processes used for money transfers and interact with application software at the level of processing queries for cryptographic conversions and results output
M6.7	P. 61	2.9.2	The money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall apply DET which are supplied by developers with the full set of operating documentation, including the description of the key system, rules of its operation, as well as the rationale for the necessary organisational and staffing support
M6.8	P. 59	2.9.1	If the money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator apply DET produced by the Russian manufacturer, such DET must have certificates issued by the authorised government body
M6.10	P. 62	2.9.2	The money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall apply DET that support continuous logging of DET processes and ensure the integrity of the software for DET environment that represents the aggregate of hardware and software, which accompany the standard functioning of DET and may affect compliance with requirements for DET
M6.11	P. 62	2.9.2	The money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall apply DET that support continuous logging of DET processes and ensure the integrity of the software for DET environment that represents the aggregate of hardware and software, which accompany the standard functioning of DET and may affect compliance with requirements for DET

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M6.14	P. 63	2.9.3	In the event of applying DET, the money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall define in their internal documents and perform the procedure established for using DET, including procedures for integrating DET in automated systems used for money transfers
	P. 64	2.9.3	In the event of applying DET, the money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall define in their internal documents and perform the procedure established for using DET, including the procedure for operating DET
	P. 65	2.9.3	In the event of applying DET, the money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall define in their internal documents and perform the procedure established for using DET, including the procedure for restoring DET operability in the event of faults and/or failures
	P. 66	2.9.3	In the event of applying DET, the money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall define in their internal documents and perform the procedure established for using DET, including the procedure for modifying DET software and DET documentation
	P. 67	2.9.3	In the event of applying DET, the money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall define in their internal documents and perform the procedure established for using DET, including the procedure for decommissioning DET
	P. 68	2.9.3	In the event of applying DET, the money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall define in their internal documents and perform the procedure established for using DET, including the procedure for managing the key system
	P. 69	2.9.3	In the event of applying DET, the money transfer operator, the bank payment agent (sub-agent), the payment infrastructure services operator shall define in their internal documents and perform the procedure established for using DET, including the procedure for handling cryptographic key media, including the procedure for applying organisational measures aimed at protecting information and using information protection equipment designed for preventing unauthorised use of cryptographic keys and the procedure for actions in the event of changed or compromised keys
M7.3	P. 72	2.10.2	The payment system operator defines the procedure for applying organisational measures aimed at protecting information and/or using information protection equipment used in operations involving the exchange of electronic messages and other information during money transfers
	P. 73	2.10.2	The money transfer operator, the payment infrastructure services operator ensure compliance with the provision specified in sub-clause 2.10.2 of clause 2.10
M7.6	P. 72	2.10.2	The payment system operator defines the procedure for applying organisational measures aimed at protecting information and/or using information protection equipment used in operations involving the exchange of electronic messages and other information during money transfers
	P. 73	2.10.2	The money transfer operator, the payment infrastructure services operator ensure compliance with the provision specified in sub-clause 2.10.2 of clause 2.10

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
	P. 74	2.10.3	Customer instructions, instructions issued by a member of the payment system and instructions from the payment clearing centre in electronic form may be certified by electronic signature and, in accordance with clause 3 of article 847 of the Civil Code of the Russian Federation, by the equivalent of a handwritten signature, codes, passwords and other means that allow to confirm the preparation of the instruction by a duly authorised person
	P. 75	2.10.4	When operating information infrastructure objects, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure protection of electronic messages from distortion, falsification, redirection, unauthorised review and/or destruction, false authorisation
M7.8	P. 76	2.10.4	When operating information infrastructure objects, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure control (monitoring) of compliance with technology established for preparation, processing, transmission and storage of electronic messages and protected information on information infrastructure objects
M7.9	P. 72	2.10.2	The payment system operator defines the procedure for applying organisational measures aimed at protecting information and/or using information protection equipment used in operations involving the exchange of electronic messages and other information during money transfers
	P. 73	2.10.2	The money transfer operator, the payment infrastructure services operator ensure compliance with the provision specified in sub-clause 2.10.2 of clause 2.10
	P. 77	2.10.4	When operating information infrastructure objects, the money transfer operator, bank payment agent (sub-agent), operator of payment infrastructure services ensure authentication of incoming electronic messages
M7.10	P. 78	2.10.4	When operating information infrastructure objects, the money transfer operator, bank payment agent (sub-agent), operator of payment infrastructure services ensure mutual (bi-directional) authentication of incoming electronic messages
M7.12	P. 81	2.10.4	When operating information infrastructure objects, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the detection of falsified electronic messages, including the imitation by third parties of customer actions during the use of electronic means of payment and performance of operations related to transfers of funds by a hacker on behalf of an authorised customer (substitution of authorised customer) after performing the authorisation procedure
M7.13	P. 79	2.10.4	When operating information infrastructure objects, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the restoration of information on the balances of funds in bank accounts, information on the balances of electronic funds and data of payment card holders in the event of intentional (accidental) destruction (distortion) or failure of computing equipment

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M7.14	P. 72	2.10.2	The payment system operator defines the procedure for applying organisational measures aimed at protecting information and/or using information protection equipment used in operations involving the exchange of electronic messages and other information during money transfers
	P. 73	2.10.2	The money transfer operator, the payment infrastructure services operator ensure compliance with the provision specified in sub-clause 2.10.2 of clause 2.10 of the Regulations
	P. 80	2.10.4	When operating information infrastructure objects, the money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the matching of relevant incoming messages to processed messages during the settlements in the payment system
M7.15	P. 39	2.6.9	The money transfer operator ensures the ability of the customer to suspend (block) the acceptance of instructions on money transfers submitted on behalf of the specified customer
M7.16	P. 72	2.10.2	The payment system operator defines the procedure for applying organisational measures aimed at protecting information and/or using information protection equipment used in operations involving the exchange of electronic messages and other information during money transfers
	P. 73	2.10.2	The money transfer operator, the payment infrastructure services operator ensure compliance with the provision specified in sub-clause 2.10.2 of clause 2.10 of the Regulations
M7.22	P. 37	2.6.7	The money transfer operator, bank payment agent (sub-agent) ensure control over the absence on the payment terminals and ATMs of specialised tools designed for unauthorised reception (collection) of information necessary for money transfers
M11.1	P. 82	2.11.1	The money transfer operator, bank payment agent (sub-agent), being a legal entity, payment infrastructure services operator ensure the establishment of an information security service and define the goals and objectives of this service in its internal documents
M11.2	P. 83	2.11.1	The money transfer operator, bank payment agent (sub-agent) being a legal entity, the payment infrastructure services operator shall provide the authority and allocate resources necessary for the information security service to perform its established goals and objectives
M11.3	P. 84	2.11.1	The money transfer operator, the payment infrastructure services operator shall appoint an information security service supervisor from among the members of their management body and define its authority
	P. 85	2.11.1	The information security service and IT (automation) service shall not have a common supervisor
M11.5	P. 86	2.11.2	The money transfer operator, which has branches, ensures the establishment of information security services in these branches, defines their authority and allocates the necessary resources
	P. 87	2.11.2	The money transfer operator, which has branches, ensures liaison and coordination of the information security services
M11.6	P. 88	2.11.3	The information security service plans and monitors information protection for money transfers and, for this purpose, it is empowered to control (monitor) the implementation of the procedure established for protecting money transfer information

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M11.9	P. 89	2.11.3	The information security service plans and monitors information protection for money transfers and, for this purpose, it is empowered to determine the requirements regarding information protection equipment and organisational measures aimed at protecting information
M11.10	P. 90	2.11.3	The information security service plans and monitors the information protection for money transfers and, for this purpose, it is empowered to control the compliance of employees with the requirements for protecting money transfer information
M11.12	P. 91	2.11.3	The information security service plans and monitors information protection for money transfers and, for this purpose, it is empowered to participate in investigations of incidents related to breaches of the requirements for money transfer information protection and propose the application of disciplinary action, as well as submit proposals to improve information protection
M11.13	P. 92	2.11.3	The information security service plans and monitors information protection for money transfers and, for this purpose, it is empowered to participate in activities related to compliance with the requirements for money transfer information protection applied when restoring the provision of payment system services after faults and failures in the operation of information infrastructure objects
M12.1 (M30.1)	P. 18	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the destruction of protected information, including the information in the archives, by using a method that prevents its restoration
M12.4	P. 18	2.5.6	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure, at the stages of operating and decommissioning the information infrastructure objects, the destruction of protected information, including the information in the archives, by using a method that prevents its restoration
M17.1	P. 107	2.14.2	The payment system operator establishes the allocation of responsibilities for defining the information protection procedure for money transfers by: independent determination by the payment system operator of the information protection procedure for money transfers; allocation of responsibilities to define the information protection procedure for money transfers between the payment system operator, payment infrastructure services operators and members of the payment system; transfer of functions for defining the information protection procedure for money transfers by a payment system operator, which is not a credit institution, to the settlement centre
	P. 108	2.14.2	The money transfer operator, bank payment agent (sub-agent), the payment infrastructure services operator ensure the definition of information protection procedure for money transfers as part of the allocation of responsibilities established by the payment system operator
	P. 109	2.14.3	The money transfer operator, the payment infrastructure services operator ensure compliance with the information protection procedure for money transfers
	P. 110	2.14.4	The money transfer operator, the payment infrastructure services operator ensure the appointment of persons responsible for compliance with the information protection procedure for money transfers

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
	P. 111	2.14.5	The information security service of the money transfer operator, the payment infrastructure services operator controls (monitors) the application of organisational measures aimed at protecting information
	P. 112	2.14.5	The information security service of the money transfer operator, the payment infrastructure services operator controls (monitors) the use of information protection equipment
M18.1	P. 93	2.12.1	The money transfer operator, bank payment agent (sub-agent), being a legal entity, the payment infrastructure services operator ensure the raising of awareness of employees in the area of information protection in accordance with the procedure established for the application of organisational measures aimed at information protection
	P. 94	2.12.1	The money transfer operator, bank payment agent (sub-agent), being a legal entity, the payment infrastructure services operator ensure the raising of awareness of employees in the area of information protection in accordance with the procedure established for the use of information protection equipment
	P. 96	2.12.3	The money transfer operator ensures that customers are informed about possible risks of unauthorised access to protected information in order to transfer money by the persons without the right to dispose such money, and about recommended measures to reduce such risks
M18.4	P. 93	2.12.1	The money transfer operator, bank payment agent (sub-agent), being a legal entity, the payment infrastructure services operator ensure the raising of awareness of employees in the area of information protection in accordance with the procedure established for the application of organisational measures aimed at information protection
M18.6	P. 95	2.12.2	The money transfer operator, bank payment agent (sub-agent), being a legal entity, the payment infrastructure services operator ensure the raising of awareness of employees who are appointed to a new role associated with the application of organisational measures aimed at information protection or use of information protection equipment
M19.1	P. 97	2.13.1	The payment system operator defines the requirements for the procedure, form and period established for informing the payment system operator, money transfer operators and payment infrastructure services operators about incidents detected in the payment systems and related to violations of requirements for ensuring information protection for money transfers
	P. 98	2.13.1	The payment system operator shall be informed of incidents related to violations of requirements for ensuring information protection for money transfers detected by money transfer operators, which are members of the payment system, and payment infrastructure services operators, which are engaged to provide information infrastructure services in the payment system, on a monthly basis
	P. 99	2.13.1	The payment system operator defines the requirements for interaction of the payment system operator, money transfer operators and payment infrastructure services operators in the event of incidents detected in the payment systems and related to violations of requirements for ensuring information protection for money transfers
	P. 100	2.13.1	The money transfer operator, the payment infrastructure services operator ensure compliance with the provision specified in sub-clause 2.13.1 of clause 2.13 of the Regulations
	P. 101	2.13.2	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the application of organisational measures aimed at protecting information and/or use of information protection equipment designed for detecting incidents related to violations of requirements for ensuring information protection for money transfers

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
	P. 102	2.13.2	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure that the information security service, if there is one, is notified about detected incidents related to violations of requirements for ensuring information protection for money transfers
	P. 103	2.13.2	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the response to detected incidents related to violations of requirements for ensuring information protection for money transfers
	P. 104	2.13.2	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure the analysis of the causes of detected incidents related to violations of requirements for ensuring information protection for money transfers and the assessment of results of responding to such incidents
	P. 106.1	2.13.4	The money transfer operator, payment infrastructure services operator ensure the registration of independently detected incidents related to violations of requirements for ensuring information protection for money transfers The money transfer operator ensures the registration of incidents that come to its knowledge and are related to violations of requirements for ensuring information protection for money transfers, and have been detected by customers of this money transfer operator The money transfer operator ensures the registration of incidents that come to its knowledge and are related to violations of requirements for ensuring information protection for money transfers, and have been detected by the bank payment agents (sub-agents)
M19.2	P. 105	2.13.3	The payment system operator ensures information is recorded on incidents detected in the payment system and related to violations of requirements for ensuring information protection for money transfers and ensures the availability of such information to money transfer operators, which are members of the payment system, and payment infrastructure services operators, which are engaged to provide information infrastructure services in the payment system
	P. 106	2.13.3	The payment system operator ensures information is recorded on the methods used for analysing and responding to incidents related to violations of requirements for ensuring information protection for money transfers funds and ensures the availability of such information to money transfer operators, which are members of the payment system, and payment infrastructure services operators, which are engaged to provide information infrastructure services in the payment system
	P. 106.2	2.13.4	The money transfer operator, payment infrastructure services operator define in their internal documents the procedure for the registration and storage of information on incidents specified in paragraphs 1-3 of sub-clause 2.13.4 of clause 2.13 of the Regulations
M22.4 (M32.3)	P. 113	2.15.2	The money transfer operator, bank payment agent (sub-agent), payment infrastructure services operator ensure conformity assessment at least every two years and at the request of the Bank of Russia
	P. 113.1	2.15.2	The organisation, which has become a money transfer operator, payment system operator, payment infrastructure services operator shall perform the first conformity assessment within six months after receiving the corresponding status

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M22.5	P. 114	2.16.1	The payment system operator establishes the requirements for content, form and frequency of providing information submitted by the money transfer operators, payment infrastructure services operators to the payment system operators for the purposes of analysing information protection in the payment system during money transfers
	P. 115	2.16.1	The money transfer operator, the payment infrastructure services operator ensure compliance with the provision specified in sub-clause 2.16.1 of clause 2.16 of the Regulations
	P. 116	2.16.2	Information submitted by the money transfer operators and payment infrastructure services operators, except for operation centres located outside the Russian Federation, to the payment system operator for the purposes of analysing the information protection in the payment system during money transfers includes information on the degree of compliance with the requirements for ensuring information protection for money transfers
M22.7	P. 113	2.15.2	Based on results of the conformity assessment and in order to document it, the money transfer operator, the payment system operator, payment infrastructure services operator prepare a report which is approved by the executive management bodies and stored in accordance with the procedure established by the relevant operator
M24.1	P. 117	2.16.2	Information submitted by the money transfer operators and payment infrastructure services operators, except for operation centres located outside the Russian Federation, to the payment system operator for the purposes of analysing the information protection in the payment system during money transfers includes information on implementing the procedure for ensuring information protection for money transfers
	P. 118	2.16.2	Information submitted by the money transfer operators and payment infrastructure services operators, except for operation centres located outside the Russian Federation, to the payment system operator for the purposes of analysing the information protection in the payment system during money transfers includes information on detected incidents related to violations of requirements for ensuring information protection for money transfers
	P. 119	2.16.2	Information submitted by the money transfer operators and payment infrastructure services operators, except for operation centres located outside the Russian Federation, to the payment system operator for the purposes of analysing the information protection in the payment system during money transfers includes information on results of conformity assessments
	P. 120	2.16.2	Information submitted by the money transfer operators and payment infrastructure services operators, except for operation centres located outside the Russian Federation, to the payment system operator for the purposes of analysing the information protection in the payment system during money transfers includes information on detected threats and vulnerabilities in the provision of information protection

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
M26.1	P. 121	2.17.1	The payment system operator, money transfer operator, payment infrastructure services operator regulate the review of the procedure established for ensuring information protection for money transfers within the responsibilities established by the payment system operator in connection with changes in the requirements regarding information protection defined by the rules of the payment system
	P. 122	2.17.1	The payment system operator, money transfer operator, payment infrastructure services operator regulate the review of the procedure established for ensuring information protection for money transfers within the responsibilities established by the payment system operator in connection with changes in the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia governing the relations in the national payment system
	P. 123	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in requirements for information protection defined by the rules of the payment system
	P. 124	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia governing relations in the national payment system
	P. 125	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in the procedure for information protection for money transfers
	P. 126	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that threats, risks and vulnerabilities are detected in the provision of information protection for money transfers
	P. 127	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that deficiencies are identified in the control (monitoring) of compliance with the procedure for information protection for money transfers
	P. 128	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that deficiencies are identified in the conformity assessment
M26.4	P. 121	2.17.1	The payment system operator, money transfer operator, payment infrastructure services operator regulate the review of the procedure established for ensuring information protection for money transfers within the responsibilities established by the payment system operator in connection with changes in the requirements regarding information protection defined by the rules of the payment system
	P. 122	2.17.1	The payment system operator, money transfer operator, payment infrastructure services operator regulate the review of the procedure established for ensuring information protection for money transfers within the responsibilities established by the payment system operator in connection with changes in the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia governing the relations in the national payment system

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
	P. 123	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in requirements for information protection defined by the rules of the payment system
	P. 124	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia governing relations in the national payment system
	P. 125	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in the procedure for information protection for money transfers
	P. 126	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that threats, risks and vulnerabilities are detected in the provision of information protection for money transfers
	P. 127	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that deficiencies are identified in the control (monitoring) of compliance with the procedure for information protection for money transfers
	P. 128	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that deficiencies are identified in the conformity assessment
M26.6	P. 129	2.17.3	The decisions of the money transfer operator, payment infrastructure services operator aimed at improving information protection for money transfers shall be agreed with the information security service
M27.1	P. 122	2.17.1	The payment system operator, money transfer operator, payment infrastructure services operator regulate the review of the procedure established for ensuring information protection for money transfers within the responsibilities established by the payment system operator in connection with changes in the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia governing the relations in the national payment system
	P. 123	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in requirements for information protection defined by the rules of the payment system
	P. 124	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia governing relations in the national payment system

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
	P. 125	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in the procedure for information protection for money transfers
	P. 126	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that threats, risks and vulnerabilities are detected in the provision of information protection for money transfers
	P. 127	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that deficiencies are identified in the control (monitoring) of compliance with the procedure for information protection for money transfers
	P. 128	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that deficiencies are identified in the conformity assessment
M27.6	P. 122	2.17.1	The payment system operator, money transfer operator, payment infrastructure services operator regulate the review of the procedure established for ensuring information protection for money transfers within the responsibilities established by the payment system operator in connection with changes in the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia governing the relations in the national payment system
	P. 123	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in requirements for information protection defined by the rules of the payment system
	P. 124	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in the legislative acts of the Russian Federation, regulatory acts of the Bank of Russia governing relations in the national payment system
	P. 125	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event of changes in the procedure for information protection for money transfers
	P. 126	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that threats, risks and vulnerabilities are detected in the provision of information protection for money transfers

Individual indicator of STO BR IBBS-1.2	Item number in the table of Annex 2 to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Sub-item number to the Regulations of the Bank of Russia No. 382-P of 9 June 2012	Wording of requirements for ensuring the protection of information in money transfers
	P. 127	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that deficiencies are identified in the control (monitoring) of compliance with the procedure for information protection for money transfers
	P. 128	2.17.2	The money transfer operator, payment infrastructure services operator regulate the procedure for taking measures aimed at improving information protection for money transfers in the event that deficiencies are identified in the conformity assessment
M27.7	P. 129	2.17.3	The decisions of the money transfer operator, payment infrastructure services operator aimed at improving information protection for money transfers shall be agreed with the information security service

Keywords: banking system of the Russian Federation, information security, conformity assessment method, information security indicators, current level of information security, information security management system, information security awareness, information security requirements.

*In case of any translation ambiguity the Russian version shall prevail.