7/2018 Coll.

DECREE

of 5 January 2018

on some conditions on the pursuit of business of payment institutions, payment account information administrators, small-scale payment service providers, electronic money institutions and small-scale electronic money issuers

Amendment: 2/2022 Coll.
Amendment: 151/2022 Coll.

PART ONE

GENERAL PROVISIONS

Article 1

Subject of regulation

This Decree incorporates the relevant European Union legislation[1)] and governs

(a) the method for compliance with certain requirements for the management and control system of payment institutions, electronic money institutions and payment account information administrators,

(b) the method for compliance with the requirements for the security and operational risk management system and the complaint and claim handling system of small-scale payment service providers and small-scale electronic money issuers,

(c) the rules for calculating the amount of capital and the capital adequacy of payment institutions and electronic money institutions, including the individual approaches that may be applied when calculating capital adequacy,

(d) the minimum insurance settlement limit and the minimum amount of comparable collateral for payment institutions, electronic money institutions and payment account information administrators,

---

[1)] Art. 4 point 46, Art. 8(2), Art. 9, Art. 9(1) (part) and Art. 9(2) of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
Art. 5(2), Art. 5(3), Art. 5(4) and Art. 5(6) of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, as amended.

(e) the method for compliance with the requirements for complaint and claim handling system of dynamic currency conversion service providers.

PART TWO

METHOD FOR COMPLIANCE WITH CERTAIN REQUIREMENTS

TITLE I

METHOD FOR COMPLIANCE WITH CERTAIN REQUIREMENTS FOR PAYMENT INSTITUTIONS' MANAGEMENT AND CONTROL SYSTEMS

(Re Article 20(4) of the Act)

Article 2

Internal regulations

(1) Payment institutions will incorporate the requirements laid down for the management and control system and the procedures for their implementation in their internal rules, meaning the payment institutions' strategy, organizational rules, plans and other internal policies and procedures.

(2) Payment institutions will set and apply a procedure for the adoption and amendment of internal rules, and ensure that the internal rules are regularly reviewed and revised where necessary.

(3) Payment institutions will ensure that the internal regulations are in accordance with the information specified in the application for authorization to operate payment institutions or their annexes, on the basis of which authorization was granted, possibly amended pursuant to Article 11 of the Act.

(4) Payment institutions will take into account, in their internal rules, general instructions and recommendations issued by the European Banking Authority, the European Securities and Markets Authority, the European Insurance and Occupational Pensions Authority, and the Joint Committee of the European Supervisory Authorities intended for payment service providers.

(5) Payment institutions will ensure that all staff members are familiarized with the relevant internal rules and any amendments to them to the necessary extent, and that they act in accordance with them.

Article 3

Approval and decision-making processes

Payment institutions will ensure that authorizations for the approval and signing of documents in the context of the payment institutions' activities are clearly defined and that all relevant approval, decision-making and control activities, including the related competencies

and powers within the payment institutions' activities and their internal rules, can be recorded, stored, traced and reconstructed. To this end, they will also adapt their information and communication systems accordingly.

Article 4

Security and operational risk management system

(1) To manage the security and operational risks related to the payment services they provide, payment institutions will put in place measures and control mechanisms to mitigate such risks. Payment institutions will establish and maintain effective security and operational incident management procedures, including for the detection and classification of major security and operational incidents.

(2) As part of their security and operational risk management system, payment institutions will also always manage risks in the field of information and communication technologies and security, which will include at least

(a) the risk of loss due to breach of data confidentiality, system and data integrity, or the availability of systems and data, or due to the inability to change information and communication systems within a reasonable time and at reasonable cost if the environment or activities change,

(b) security risks arising from the inadequacy or failure of internal processes, or from external events, including cyberattacks, or from a lack of physical security.

(3) Details of the management of ICT and security risks to which payment institutions are or could be exposed in connection with the payment services they provide are set out in an annex to this Decree.

(4) Payment institutions will prepare an information security policy defining the principles and rules to protect the confidentiality, integrity and availability of the data and information of the payment institution and payment service users. Payment institutions will adapt security measures in their internal rules in accordance with the risk management details set out in an annex to this Decree.

Article 5

Complaints and claims handling system

(1) Payment institutions will define and implement procedures for addressing complaints and claims from payment service users which

(a) are approved by the person who effectively directs the payment institution's activities in the field of payment service provision, while such person will also monitor compliance with such procedures on an ongoing basis,

(b) are laid down in an internal regulation,

(c) allow their proper investigation and ensure that potential conflicts of interest are

identified and mitigated when handling them.

(2) Payment institutions will internally record claims and complaints and their handling in accordance with the prescribed deadlines, and in a manner that meets the information security requirements.

(3) Payment institutions will set up a system for handling complaints and claims in such a way that it allows it to provide the Czech National Bank, upon request, with information on claims and complaints and their handling without undue delay, including the specific procedures for their handling.

(4) Payment institutions will continuously analyze the data on claims and complaints and the results of their handling to ensure the identification and resolution of possible systemic deficiencies and possible risks, and will at least

(a) analyze the reasons for individual complaints and claims and identify the main causes of the individual types of complaints and claims,

(b) assess whether the identified root causes may affect other processes, services or products, including those not directly affected by the complaint or claim,

(c) in the case of systemic deficiencies, they will always eliminate the identified causes of the claims and complaints.

(5) Payment institutions

(a) will provide payment service users, upon request and always in connection with the confirmation of receipt of a claim or complaint, with written information about the handling procedure for their claim or complaint in the Czech language, or in another language if agreed with the payment service user,

(b) will make available, to payment service users and the public, the information referred to in letter (c) by means of the payment service users' e-mail addresses or by any other means agreed with payment service users in their business premises and, if they have a website, also on that, and at least in the Czech language,

(c) will provide clear, accurate and up-to-date information on the complaint and claim handling procedure, which will include
   1. detailed information as to how to submit a complaint or claim, in particular the type of information to be provided by the payment service user and the contact details of the person or department of the payment institution to which the complaint or claim is to be sent,
   2. information on the deadline by which the payment service user will be notified of the handling of their complaint and on the indicative deadline for processing the complaint or claim,
   3. substantial ongoing information on the processing of the complaint or claim,
   4. information on the contact details of the Czech National Bank, the Office of the Financial Arbitrator and the Office of the Public Defender of Rights.

(6) Payment institutions

(a) will make such efforts as may reasonably be required of them to obtain and verify all relevant evidence and information relating to a complaint or claim,

(b) will communicate with the payment service user in a simple and comprehensible manner,

(c) will provide answers without undue delay and at the latest within the deadline pursuant to Article 258 of the Act; if they cannot comply with these deadlines, they will inform the payment service user of the reasons for the delay and the date on which the handling of the complaint or claim will be completed,

(d) when taking a position that does not fully meet the requirements of the payment service user, will explain in detail the resolution of the claim or complaint, and provide information on the possibility that the payment service user may insist on their claim or complaint and contact the Office of the Financial Arbitrator, the Czech National Bank and, in matters of the right to equal treatment and protection against discrimination, the Office of the Public Defender of Rights, including the contact details of the relevant body, or a court.

TITLE II

METHOD FOR COMPLIANCE WITH CERTAIN REQUIREMENTS FOR AN ELECTRONIC MONEY INSTITUTION'S MANAGEMENT AND CONTROL SYSTEM

(Re Article 78(4) of the Act)

Article 6

Articles 2 to 5 apply mutatis mutandis for an electronic money institution.

TITLE III

METHOD FOR COMPLIANCE WITH CERTAIN REQUIREMENTS FOR A PAYMENT ACCOUNT INFORMATION ADMINISTRATOR'S MANAGEMENT AND CONTROL SYSTEM

(Re Article 48(4) of the Act)

Article 7

(1) Articles 2 and 3 apply mutatis mutandis for a payment account information administrator.

(2) To comply with the requirements for the security and operational risk management system, a payment account information administrator will proceed pursuant to Article 4 mutatis mutandis.

(3) To comply with the requirements for the handling of claims and complaints, a payment account information administrator will proceed pursuant to Article 5 mutatis

mutandis.

TITLE IV

METHOD FOR COMPLYING WITH THE SECURITY AND OPERATIONAL RISK MANAGEMENT SYSTEM AND THE CLAIMS AND COMPLAINTS MANAGEMENT SYSTEM FOR A SMALL-SCALE PAYMENT SERVICE PROVIDER

(Re Article 59(4) and Article 65a(2) of the Act)

Article 8

(1) A small-scale payment service provider will reflect the requirements set for a security and operational risk management system and a claims and complaints management system in their internal regulations, and will proceed pursuant to Articles 2(2) to (5) mutatis mutandis to comply with the requirements for these internal regulations.

(2) In order to comply with the requirements for approval and decision-making processes relating to the security and operational risk management system and the claims and complaints management system, a small-scale payment service provider will proceed mutatis mutandis pursuant to Article 3.

(3) In order to comply with the requirements for a security and operational risks management system arising from the provision of payment services, a small-scale payment service provider will proceed mutatis mutandis pursuant to Article 4.

(4) In order to comply with the requirements for a claims and complaints management system, a small-scale payment service provider will proceed mutatis mutandis pursuant to Article 5.

TITLE V

METHOD FOR COMPLYING WITH THE REQUIREMENTS FOR A SECURITY AND OPERATIONAL RISK MANAGEMENT SYSTEM AND A CLAIMS AND COMPLAINTS MANAGEMENT SYSTEM FOR A SMALL-SCALE ELECTRONIC MONEY ISSUER

(Re Article 100(4) and Article 106a(2) of the Act)

Article 9

(1) A small-scale electronic money issuer will reflect the requirements set for a security and operational risk management system and a claims and complaints management system in their internal regulations, and will proceed pursuant to Articles 2(2) to (5) mutatis mutandis to comply with the requirements for these internal regulations.

(2) In order to comply with the requirements for approval and decision-making processes relating to a security and operational risk management system and a claims and complaints management system, a small-scale electronic money issuer will proceed mutatis mutandis pursuant to Article 3.

(3) In order to comply with the requirements for a security and operational risk management system, a small-scale electronic money issuer will proceed mutatis mutandis pursuant to Article 4.

(4) In order to comply with the requirements for a claims and complaints management system, a small-scale electronic money issuer will proceed mutatis mutandis pursuant to Article 5.

TITLE VI

METHOD FOR COMPLYING WITH THE REQUIREMENTS FOR A CLAIMS AND COMPLAINTS MANAGEMENT SYSTEM FOR A DYNAMIC CURRENCY CONVERSION SERVICE PROVIDER

(Re Article 254h(4) of the Act)

Article 10

In order to comply with the requirements for a claims and complaints management system, a dynamic currency conversion service provider will proceed mutatis mutandis pursuant to Article 5.

Article 11

repealed

heading omitted

Article 12

repealed

Article 13

repealed

Article 14

repealed

heading omitted

Article 15

repealed

Article 16

repealed

Article 17

repealed

Article 18

repealed

heading omitted

Article 19

repealed

Article 20

repealed

Article 21

repealed

heading omitted

Article 22

repealed

Article 23

repealed

Article 24

repealed

heading omitted

Article 25

repealed

heading omitted

Article 26

repealed

PART THREE

CAPITAL ADEQUACY AND INSURANCE

TITLE I

PAYMENT INSTITUTION CAPITAL ADEQUACY

(Re Article 16(5) of the Act)

Article 27

Capital

(1) Capital is calculated similarly to own funds as indicated in Art. 4(1) point 118 of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (the "Regulation").

(2) At least 75% of Tier 1 capital will have the form of Common Equity Tier 1 capital pursuant to Art. 50 of the Regulation, and Tier 2 capital is equal to at most one third of Tier 1 capital.

(3) In order to prevent the multiple use of elements eligible for the calculation of capital, a payment institution which is a member of a group of which another payment institution, foreign payment institution, credit institution, investment firm, asset management company or insurance undertaking is also a member, may not include in capital determined pursuant to paragraph (1) those items or parts thereof that are included in capital for the purpose of compliance with any other capital requirements. For the purpose of this Decree, a credit institution, investment firm and asset management company means these entities as

defined in the Regulation.

(4) A payment institution that also performs other business activities than the activity for which it is authorized based on authorization pursuant to the Act (a "hybrid payment institution") may not include in capital determined in accordance with paragraph (1) those items or parts thereof which are used for the performance of activities other than those it is authorized to carry out on the basis of authorization granted pursuant to the Act.

Article 28

Methods for calculating the capital requirement

(1) Methods for calculating the capital requirement:

(a) the overhead-based method ("Method A"),

(b) the payment volume method ("Method B"),

(c) the basic indicator method ("Method C").

(2) A hybrid payment institution will apply one of these methods only for activities under Article 8 of the Act.

Article 29

Method A

(1) The capital requirement determined using Method A will equal 10% of the sum of the overheads for the immediately preceding accounting period; "overheads" will mean

(a) costs of depreciation and amortization of tangible and intangible assets and

(b) administrative costs[5)] or consumption from operations, personnel costs and taxes and fees[6)].

(2) In the event of a significant change in the business of a payment institution that has determined its capital requirement using Method A since the immediately preceding accounting period, the Czech National Bank may allow a change in the calculation of the capital requirement where justified.

[5)] Decree No. 501/2002 Coll., implementing certain provisions of Act No. 563/1991 Coll., on accounting, as amended, for accounting units that are banks and other payment institutions, as amended.

[6)] Decree No. 500/2002 Coll., implementing certain provisions of Act No. 563/1991 Coll., on accounting, as amended, for accounting units that are entrepreneurs keeping accounts in a double-entry bookkeeping system, as amended.

(3) A payment institution that started its activities during the current accounting period shall determine the capital requirement using Method A as 10% of the sum of the overheads as projected for the current accounting period, adjusted in accordance with the requirements of the Czech National Bank where applicable.

Article 30

Method B

(1) The capital requirement determined using Method B will equal the product of the scaling factor defined in Article 32 and the amount designated as the sum of

(a) 4% of the slice of payment volume up to the equivalent of EUR 5 million,

(b) 2.5% of the slice of payment volume above the equivalent of EUR 5 million and up to the equivalent of EUR 10 million,

(c) 1% of the slice of payment volume above the equivalent of EUR 10 million and up to the equivalent of EUR 100 million, and

(d) 0.5% of the slice of payment volume above the equivalent of EUR 100 million and up to the equivalent of EUR 250 million, and

(e) 0.25% of the slice of payment volume above the equivalent of EUR 250 million.

(2) During the period from 31 December to 30 December of the following year, the amounts in euros defined in paragraph (1) will be converted to amounts in the Czech koruna at the exchange rate announced by the Czech National Bank as the last in October of the year in which the period starts.

(3) The payment volume pursuant to paragraph (1) will represent one twelfth of the total amount of payment transactions executed by the payment institution in the immediately preceding accounting period.

(4) Where a payment institution started its activities during the current accounting period, it will determine the volume of payments on the basis of its plan, adjusted in accordance with the requirements of the Czech National Bank where applicable.

Article 31

Method C

(1) The capital requirement determined using Method C will equal the product of the scaling factor defined in Article 32 and the amount designated as the sum of

(a) 10% of the slice of the relevant indicator up to the equivalent of EUR 2.5 million,

(b) 8% of the slice of the relevant indicator above the equivalent of EUR 2.5 million and up to the equivalent of EUR 5 million,

(c) 6% of the slice of the relevant indicator above the equivalent of EUR 5 million and up to the equivalent of EUR 25 million, and

(d) 3% of the slice of the relevant indicator above the equivalent of EUR 25 million and up to the equivalent of EUR 50 million, and

(e) 1.5% of the slice of the relevant indicator above the equivalent of EUR 50 million.

(2) The relevant indicator will equal the sum of interest income, interest expenses, income from fees and commissions and other operating income, and the calculation will be performed as follows:

(a) the relevant indicator will be calculated on the basis of the twelve-monthly observations from data as of the end of the last accounting period,

(b) each item will be taken into account in the corresponding positive or negative value,

(c) extraordinary and irregular income will not be included in the calculation of the relevant indicator, and

(d) expenditure on outsourcing rendered by a person subject to comparable supervision by a competent supervisory authority may be subtracted from the relevant indicator.

(3) Where a payment institution started its activities during the current accounting period, it will determine the volume of the relevant indicator on the basis of its plan, adjusted in accordance with the requirements of the Czech National Bank where applicable.

(4) If the value of the relevant indicator pursuant to paragraph (2) is lower than 80% of the average of the relevant indicator values for the past 3 accounting periods, 80% of the average of the relevant indicator values for the past 3 accounting periods will be used as the value of the relevant indicator for the purposes of determining the capital requirement pursuant to paragraph (1).

(5) During the period from 31 December to 30 December of the following year, the amounts in euros defined in paragraph (1) will be converted to amounts in the Czech koruna at the exchange rate announced by the Czech National Bank as the last in October of the year in which the period starts.

Article 32

Scaling factor

The scaling factor to be used when applying Method B or Method C will be

(a) 0.5 where a payment institution provides only the payment service listed in Article 3(1)(f) of the Act, or

(b) 1 where payment institutions provide any of the payment services listed in Articles 3(1)(a) to (e) of the Act.

TITLE II

ELECTRONIC MONEY INSTITUTION CAPITAL ADEQUACY

(Re Article 74(6) of the Act)

Article 33

Calculation of capital adequacy

For the calculation of the capital adequacy of an electronic money institution, the capital requirement to cover risks will be determined as the sum of the capital requirements pursuant to Article 34 and 35.

Article 34

Capital and the capital requirement to cover risks connected with issuing electronic money

(1) Capital will be calculated mutatis mutandis as capital pursuant to Article 4(1) point 118 of the Regulation.

(2) The capital requirement to cover the risks associated with the issuance of electronic money will be at least 2% of the average amount of electronic money in circulation.

(3) In order to prevent the multiple use of elements eligible for the calculation of capital, an electronic money issuer which is a member of a group of which another payment institution, foreign payment institution, credit institution, investment firm, asset management company or insurance undertaking is also a member, may not include in capital determined pursuant to paragraph (1) those items or parts thereof that are included in capital for the purpose of compliance with any other capital requirements.

(4) An electronic money institution that also performs other business activities than the activity for which it is authorized based on authorization pursuant to the Act may not include in capital determined in accordance with paragraph (1) those items or parts thereof which are used for the performance of activities other than those it is authorized to carry out on the basis of authorization granted pursuant to the Act.

(5) Where it is not possible to establish what portion of funds submitted by the holder to an electronic money institution is designated for activities pursuant to Article 67(1)(b) of the Act, the determination of the average amount of electronic money in circulation will be based on such an amount of these funds that corresponds to a reliable estimate on the basis of data from the previous periods.

(6) If an electronic money institution has issued electronic money for a period of less than 6 calendar months, this capital requirement will equal at least 2% of the average amount of electronic money in circulation determined on the basis of their business plan, or adjusted pursuant to the requirements of the Czech National Bank.

Article 35

Calculation of the capital requirement to cover risks connected with the provision of payment services that do not relate to electronic money

Articles 29 to 32 apply mutatis mutandis for the calculation of the capital requirement to cover risks connected with the provision of payment services that do not relate to electronic money.

TITLE III

MINIMUM INSURANCE SETTLEMENT LIMIT FROM INSURANCE AND MINIMUM LEVEL OF COMPARABLE COLLATERAL

(Re Article 17(3), Article 46(2) and Article 75(3) of the Act)

Article 36

Minimum monetary amount of performance

The minimum insurance settlement limit from insurance and the minimum level of comparable collateral are determined for the preceding calendar year and equal the minimum cash amount of the settlement calculated using the formula

MMA = RP + TA + SA,

where:

MMA denotes the minimum monetary amount of settlement, expressed in euros;

RP denotes the value of the risk profile indicator, expressed in euros;

TA denotes the value of the type of activity indicator, expressed in euros;

SA denotes the value of the scope of activity indicator, expressed in euros.

Article 37

Risk profile indicator

The value of the risk profile indicator is calculated using the formula

RP = CR + NT + NA,

where:

RP denotes the value of the risk profile indicator, expressed in euros;

CR denotes the total value of all claims arising under Article 17(1) or (2), Article 46(1), or

Article 75(1) or (2) of the Act applied by users or providers of a payment service who keep a payment account, against the provider of the indirect payment order payment service or provider of the payment account information service in the previous calendar year; the value is expressed in euros;

the value of claims denominated in a currency other than the euro will be converted into an amount in euros at the rate the Czech National Bank announces as the last in October of the previous calendar year;

if the services were not provided in the given calendar year, the CR will correspond to the estimated amount of the claims, however at least EUR 50 000;

NT denotes the indicator of the number of all payment transactions for which the payment order was issued indirectly, and is calculated using the formula:

$$NT = 0.4\ N_a + 0.25\ N_b + 0.1\ N_c + 0.05\ N_d + 0.00025\ N_e,$$

where:
$N_a = \min \{10\ 000; N\}$
$N_b = \max \{0; \min \{90\ 000; N - 10\ 000\}\}$
$N_c = \max \{0; \min \{900\ 000; N - 100\ 000\}\}$
$N_d = \max \{0; \min \{9\ 000\ 000; N - 1\ 000\ 000\}\}$
$N_e = \max \{0; N - 10\ 000\ 000\}$
N is the total number of payment transactions for which the payment order was issued indirectly in the preceding calendar year, and equals the sum of $N_a+N_b+N_c+N_d+N_e$;

if indirect payment order services were not provided in the given calendar year, the NT will correspond to the estimated amount of the payment transactions for which the payment order will be issued indirectly, however at least 50 000;

NA denotes the indicator of the number of individual payment accounts to which the payment account information service provider has access, and is calculated using the formula:

$$NA = 0.4\ N_a + 0.25\ N_b + 0.1\ N_c + 0.05\ N_d + 0.00025\ N_e,$$

where:
$N_a = \min \{10\ 000; N\}$
$N_b = \max \{0; \min \{90\ 000; N - 10\ 000\}\}$
$N_c = \max \{0; \min \{900\ 000; N - 100\ 000\}\}$
$N_d = \max \{0; \min \{9\ 000\ 000; N - 1\ 000\ 000\}\}$
$N_e = \max \{0; N - 10\ 000\ 000\}$
N is the total number of all payment accounts to which the payment account information service provider had access in the preceding calendar year, and equals the sum of $N_a+N_b+N_c+N_d+N_e$;

if services were not provided in the given calendar year, NA will correspond to the estimated number of payment accounts to which the payment account information service provider had access, however at least 50 000.

Article 38

Type of activity indicator

(1) The value of the type of activity indicator equals zero in the event of the exclusive provision of payment services.

(2) Where a different activity/activities is/are performed than a payment service, the value of the type of activity indicator is EUR 50 000 unless the activity other than a payment service does not affect the provision of the indirect payment order service or the payment account information service because there is a guarantee covering liabilities arising from this activity or other legislation provides determines an obligation to establish a separate entity for payment services business if such other activity impairs or could impair the financial health of the given service provider.

Article 39

Scope of activity indicator

(1) The value of the scope of activity indicator of an indirect payment order service provider is calculated using the formula:

$$SA = 0.4\ N_a + 0.25\ N_b + 0.1\ N_c + 0.05\ N_d + 0.00025\ N_e,$$

where:
N_a = min {500 000; N}
N_b = max {0; min {500 000; N – 500 000}}
N_c = max {0; min {4 000 000; N – 1 000 000}}
N_d = max {0; min {5 000 000; N – 5 000 000}}
N_e = max {0; N – 10 000 000}
N is the total amount of payment transactions for which the payment order was issued indirectly in the preceding calendar year; this amount is expressed in euros and equals the sum of $N_a+N_b+N_c+N_d+N_e$;

if the services were not provided in the given calendar year, the estimated amount of all payment transactions for which the payment order will be issued indirectly will be used, however at least EUR 50 000.

The value of payment transactions denominated in a currency other than the euro will be converted into an amount in euros at the rate the Czech National Bank announces as the last in October of the previous calendar year.

(2) The value of the scope of activity indicator of a payment account information service provider is calculated using the formula:

$$SA = 0.4\ N_a + 0.25\ N_b + 0.1\ N_c + 0.05\ N_d + 0.00025\ N_e,$$

where:
N_a = min {100; N}
N_b = max {0; min {9 900; N – 100}}

N_c = max {0; min {90 000; N – 10 000}}
N_d = max {0; min {900 000; N – 100 000}}
N_e = max {0; N – 1 000 000}
N is the total number of payment account information service users in the preceding calendar year, and equals the sum of $N_a+N_b+N_c+N_d+N_e$;

if these services were not provided in the calendar year in question, the estimated number of users is used, however at least 50 000.

(3) In the event of the provision of the indirect payment order service and concurrently the payment account information service, the value of the scope of activity indicator will equal the sum of the value of the scope of activity indicator for the indirect payment order service provider and the scope of activity indicator for the payment account information service provider.

PART FOUR

EFFECT

Article 40

This Decree will come into effect on 13 January 2018.

Governor:

per pro. Hampl

Deputy Governor

Annex

Details on ICT and security risk management

Adequacy

1. Payment institutions will comply with information and communication technology and security risk (hereinafter "ICT and security risks") management requirements in a manner proportionate to the size of the payment institution, their organizational structure and the nature, scale, complexity and riskiness of the services and products that the payment institution provides or intends to provide.

Strategic and operational management, organizational structure

2. The person that effectively directs the activity of a payment institution in the area of payment service provision (hereinafter the "management body") will ensure that the payment institution has an adequate internal governance and internal control framework in place for ICT and security risks. The management body will clearly define the roles and responsibilities for ICT functions, ICT and security risk management, including information security and the smooth conduct of activities, and the continued functioning of the payment institution, including for themselves.

3. The management body will ensure that staff numbers at the payment institution, and their professional qualifications and experience, are adequate to continuously support the operation of the payment institution in the fields of ICT, ICT and security risk management, and to ensure the implementation of their information and communication technology strategy, and that the allocated budget is consistent with this. Payment institutions will ensure that all staff members receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required (point 49).

4. The management body has overall accountability for setting, approving and overseeing the implementation of payment institutions' information and communication technology strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks.

5. The information and communication technology strategy will be aligned with a payment institutions' overall business strategy and will define

(a) how the payment institution's information and communication technologies will be developed to effectively support the payment institution's overall strategy, including the definition of the development of the organizational structure, changes in information and communication technology systems (hereinafter "ICT systems") and key dependencies with third parties,

(b) the planned strategy and development of the information and communication technologies architecture, including third party dependencies,

(c) clear information security objectives with a focus on ICT systems and ICT services, information and communication technology staff and processes.

6. Payment institutions will establish sets of action plans that contain measures to be taken to achieve the objective of the information and communication technology strategy. Such plans will be communicated to all relevant staff and other relevant persons, including suppliers and external service or activity providers, meaning outsourcing providers, providers within the group of which the payment institution is a member, or other contractors (hereinafter "contractors"), where they are applicable and relevant to them. Payment institutions will regularly review the action plans and ensure their relevance and appropriateness on an ongoing basis. Payment institutions will implement processes to monitor and evaluate the effectiveness of the implementation of their information and communication technology strategy.

7. Payment institutions will ensure that the risk mitigation measures defined in the risk management system are effective even if any operational functions relating to the provision of payment services or ICT systems or services in the field of information and communication technologies (hereinafter "ICT services") are outsourced.

8. To ensure continuity of ICT systems and ICT services, payment institutions will ensure that contracts and similar service level arrangements with all contractors include:

(a) objectives and measures related to information security, including specific requirements and criteria; this always includes minimum cybersecurity requirements, payment institution data lifecycle specifications, any requirements relating to data encryption, network security processes, and data centre security and location monitoring,

(b) operational procedures and procedures for addressing one-off events or a series of related events unplanned by the payment institution that has/have or is/are likely to have an adverse impact on the integrity, availability, confidentiality or authenticity of the services (hereinafter a "security and operational incident"), including escalation and reporting.

9. Payment institutions will monitor and seek assurance on the level of compliance of contractors with the security objectives, measures and operational tasks of the payment institution for which they provide services.

ICT and security risk management system

10. Payment institutions will identify and manage the ICT and security risks to which they are or could be exposed in relation to the payment services they provide. When doing so, they will apply procedures and controls that ensure that all such risks are identified, assessed, measured, monitored, reported and limited in accordance with the approved level of willingness of the payment institution to accept these risks, and that the implemented projects and systems and regular activities carried out are in accordance with other internally established rules of the payment institution and requirements arising from legal regulations or remedial measures imposed by the Czech National Bank.

11. Payment institutions will assign the responsibility for managing and overseeing ICT and security risks to a control function. Payment institutions will ensure the independence and objectivity of such control function by segregating it from information and communication technology operations in an appropriate manner. This control function will be directly accountable to the management body and responsible for monitoring and controlling

adherence to the ICT and security risk management system. It will also ensure that ICT and security risks are identified, evaluated, measured, monitored and reported. Payment institutions will ensure that this control function is not responsible for any internal audit.

12. Payment institutions will define and assign key roles and responsibilities, and relevant reporting lines and competences, for the ICT and security risk management system to be effective. Payment institutions will ensure that ICT and security risk management is fully integrated into the payment institution's risk management system, including ensuring the effectiveness and consistency of relations within that system and that it is in accordance with the various risk management system processes.

13. The ICT and security risk management system will include processes in place to

(a) determine the risk appetite for ICT and security risks, in accordance with the risk appetite of the payment institution,

(b) identify and assess such risks to which the payment institution is exposed,

(c) take measures to reduce the occurrence or impact of the occurrence of such risks,

(d) monitor the effectiveness of measures and the number of notified security and operational incidents in the field of payments, including incidents pursuant to Article 221 of the Act that have an impact on information and communication technology-related activities, and take action to correct the measures where necessary,

(e) report such risks and measures to the management body,

(f) identify and assess whether there are any ICT and security risks resulting from any major change in ICT systems or ICT services, processes or procedures, and/or after any significant operational or security incident.

14. Payment institutions will ensure that the ICT and security risk management system is properly documented and continuously improved on the basis of lessons learned. The management body will approve and review the set-up of the ICT and security risk management system at least once a year.

15. Payment institutions will identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.

16. In addition, payment institutions will identify collected information that needs to be protected (hereinafter "information assets") supporting the business functions and supporting processes, and will establish and update their monitoring. Payment institutions will always be able to manage the information assets that support their critical business functions and processes.

17. Payment institutions will classify the identified business functions, support processes and information assets in accordance with points 15 and 16 in terms of their criticality.

18. To define the criticality of these identified business functions, supporting processes and information assets, payment institutions will, at a minimum, consider the confidentiality, integrity and availability requirements. Payment institutions will clearly define the accountability and responsibility for the information assets.

19. Payment institutions will review the adequacy of the classification of information assets and relevant documentation when risk assessment is performed.

20. Payment institutions will identify ICT and security risks that impact identified and classified business functions, supporting processes and information assets according to their criticality. This risk assessment will be carried out and documented annually or at shorter intervals if required. Such risk assessments will also be performed on any major changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets. Payment institutions will update the applicable risk assessment based on this.

21. Payment institutions will ensure that they continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and will regularly review the risk scenarios impacting them.

22. On the basis of such risk assessment, payment institutions will identify measures to limit recognized ICT and security risks to a level appropriate to the risk appetite of the payment institutions. Payment institutions will also determine whether changes to existing business processes, control measures, ICT systems and ICT services are needed. Payment institutions will consider the time required to implement these changes and the time to take appropriate interim mitigating measures to minimize ICT and security risks to stay within the payment institutions' ICT and security risk appetite.

23. Payment institutions will take measures to limit the identified ICT and security risks and to protect information assets in accordance with their classification.

24. Payment institutions will ensure that the results of the risk assessment are reported to the management body in a clear and timely manner.

Internal ICT and security risks audit

25. The internal audit function will take a risk-oriented approach and will separately review the compliance between all ICT and security activities of the payment institution and the payment institution's principles and procedures and with external requirements, and will review whether those principles and procedures are complied with in the given sections, and provide objective independent assurance to that effect. The internal audit function that the payment institution internally or externally provides will regularly provide the management body with independent assurance on the effectiveness of the ICT and security risk management system. The staff responsible for the internal audit function will have professional qualifications and sufficient experience in relation to ICT and security, and payments risks, and will be independent within the payment institution or from the given payment institution. The frequency and focus of audits will reflect the severity of those risks.

26. The management body will approve the audit plan, including all ICT audits and any material modifications thereto. The audit plan and its execution, including the audit

frequency, will reflect and be proportionate to the inherent ICT and security risks in the payment institution and will be updated regularly.

27. Payment institutions will determine measures for the timely verification and remediation of critical ICT audit findings.

Information security

Information security policy

28. Payment institutions will ensure that the information security policy is in accordance with the payment institutions' information security objectives and is based on risk assessment results. The information security policy will be approved by the management body.

29. The security policy will include a description of the main roles and responsibilities of information security management, and it will set out the requirements for staff and contractors, processes and technology in relation to information security. All staff and contractors will have responsibilities in ensuring the information security of the payment institution, corresponding to the activities carried out by them, the tasks entrusted to them and the authorizations at their disposal. The information security policy will ensure the confidentiality, integrity and availability of a payment institution's critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy will be communicated to all staff and contractors of the payment institution.

30. Based on the information security policy, payment institutions will establish and implement security measures to mitigate the ICT and security risks that they are exposed to. The measures will cover the following areas:

(a) organization and governance in accordance with the requirements of points 10, 11 and 25,

(b) logical security,

(c) physical security,

(d) operational security in the field of information and communication technologies,

(e) security monitoring,

(f) information security reviews, assessment and testing,

(g) information security training and awareness.

Logical security

31. Payment institutions will define, document and implement procedures for logical access control, including checks to monitor anomalies. Payment institutions will monitor the application of those procedures and review them regularly. Those procedures will be based on at least the following principles:

(a) need-to-know basis, least privilege and segregation of duties; payment institutions will manage access rights to information assets and their supporting systems so that the user, including a system user (hereinafter "users") only knows what they need to know, including for remote access; users will be granted minimum access rights that are strictly required to execute their duties to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls,

(b) user accountability; payment institutions will limit, as much as possible, the use of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems,

(c) privileged access rights; payment institutions will implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access entitlements. In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems will be granted only on a need-to-know basis and when strong authentication solutions are used,

(d) logging of user activities; at a minimum, all activities by privileged users will be logged and monitored by payment institutions. Access logs will be secured to prevent unauthorized modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets; payment institutions will use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of services,

(e) access management; access rights will be granted, withdrawn or modified in a timely manner by payment institutions, according to predefined approval workflows that involve the business owner of the information being accessed (information asset owner). In the case of termination of employment, access rights will be promptly withdrawn,

(f) access recertification; access rights will be periodically reviewed by payment institutions to ensure that users do not possess excessive privileges and that access rights are withdrawn as soon as they are no longer required,

(g) authentication methods; payment institutions will enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with, are commensurate with the criticality of ICT systems, information or the process being accessed, including at a minimum complex passwords, two-factor authentication or other strong verification methods, based on relevant risk.

32. Payment institutions will ensure that remote access by applications to data and ICT systems is limited to a minimum required to provide the relevant service.

Physical security

33. Payment institutions will define, document and implement physical security measures to protect their premises, data centres and sensitive areas from unauthorized access and from environmental hazards.

34. Payment institutions will ensure that physical access to ICT systems is permitted to only authorized individuals. Authorization will be assigned in accordance with the individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Payment institutions will ensure that physical access is regularly reviewed to ensure that unnecessary access rights are promptly revoked when not required.

35. Payment institutions will adopt adequate measures to protect from environmental hazards that are commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.

Information and communication technology operational security

36. Payment institutions will define, document and implement procedures to prevent the occurrence of security issues in ICT systems and ICT services, and will minimize their impact on the provision of these services. These procedures will include the following measures

(a) identification of potential vulnerabilities, which will be evaluated and remediated by ensuring that software and firmware are up to date, including the software provided by payment institutions to their users, by deploying critical security patches or by implementing compensating controls,

(b) implementation of secure configuration baselines of all network components,

(c) implementation of network segmentation, data loss prevention systems and the encryption of network traffic, in accordance with the data classification,

(d) implementation of protection of endpoints including servers, workstations and mobile devices; payment institutions will evaluate whether endpoints meet the security standards defined by them before they are granted access to the corporate network,

(e) ensuring that mechanisms are in place to verify the integrity of software, firmware and data,

(f) encryption of data at rest and in transit, in accordance with the data classification.

37. Payment institutions will determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. Payment institutions will ensure that these changes are properly planned, tested, documented, authorized and deployed.

Security monitoring

38. Payment institutions will carry out ongoing security monitoring. To that end, they will establish, document and apply procedures for detecting unusual activities that may have an impact on the security of the payment institutions' information, and for reacting to such events. As part of this continuous monitoring, payment institutions will be capable of detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. Payment institutions will focus on

(a) relevant internal and external factors, including business and ICT administrative functions,

(b) transactions to detect misuse of access by third parties or internal misuse of access,

(c) potential internal and external threats.

39. Payment institutions will have organization structures to identify and constantly monitor security threats that could materially affect their abilities to provide services. Payment institutions will actively monitor technological developments to ensure that they are aware of security risks. Payment institutions will implement measures, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and will check for corresponding new security updates.

40. The security monitoring process will also help payment institutions to understand the nature of operational or security incidents, to identify trends and to support the organization's investigations.

Information security reviews, evaluations and testing

41. Payment institutions will apply different procedures and tools for information security reviews, evaluations and testing to ensure the effective identification of vulnerabilities in ICT systems and ICT services, through differential analysis against information security standards or otherwise, compliance reviews, audits of information systems and physical security checks. Furthermore, payment institution will consider good practices such as source code reviews, vulnerability assessments, penetration tests and exercises simulating real-world intrusion into ICT systems.

42. Payment institutions will establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities identified through threat monitoring and ICT and security risk assessment process.

43. The information security testing framework will ensure that tests

(a) are carried out by independent professionally qualified testers with sufficient experience in testing information security measures and who are not involved in the development of the information security measures,

(b) include vulnerability scans and penetration tests, including threat-led penetration testing where necessary and appropriate, commensurate to the level of risk identified with the business processes and systems.

44. Payment institutions will perform ongoing and repeated tests of the security measures. For all critical ICT systems, these tests will be performed at least on an annual basis, and will be part of the comprehensive assessment of the security and operational risks related to the payment services they provide, about which the payment institutions will inform the Czech National Bank pursuant to Article 222(1) of the Act. Payment institutions will test non-critical systems regularly using a risk-based approach, but at least every 3 years.

45. Payment institutions will ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet-facing critical applications.

46. Payment institutions will monitor and evaluate the results of the security tests and update their security measures accordingly, without undue delays in the case of critical ICT systems.

47. Payment institutions will also apply security measures relating to

(a) payment terminals and devices used for the provision of payment services,

(b) payment terminals and devices used for authenticating the payment service users,

(c) devices and software provided to users to generate/receive an authentication code.

48. Based on the security threats observed and the changes made, payment institutions will perform tests that incorporate scenarios of relevant and known potential attacks.

Information security training and awareness

49. Payment institutions will establish a training programme, including periodic security awareness programmes, for all staff and contractors to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security-related risks. Payment institutions will ensure that the training programme provides training for all staff members and contractors at least annually.

Information and communication technologies operations management

50. Payment institutions will manage their ICT operations based on documented and implemented processes and procedures that are approved by the management body. This set of documents will define how payment institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations and the maintenance of an up-to-date inventory of software and hardware located in the business environment (hereinafter the "ICT asset inventory").

51. Payment institutions will ensure that performance of their ICT operations is aligned to their business requirements. Payment institutions will maintain and improve, when possible, efficiency of their ICT operations, including the need to consider how to minimize potential errors arising from the execution of manual tasks.

52. Payment institutions will determine and implement logging and monitoring procedures for critical ICT operations to allow the detection, analysis and correction of errors.

53. Payment institutions will maintain an up-to-date inventory of their ICT assets, including network devices and databases. The inventory of these assets will store the configuration of the ICT assets and their links and interdependencies to enable a proper

configuration and change management process.

54. The ICT asset inventory will be sufficiently detailed to enable the prompt identification of an ICT asset, their location, security classification and ownership. Payment institutions will document the interdependencies between ICT assets to help in the response to security and operational incidents, including cyberattacks.

55. Payment institutions will monitor and manage the life cycles of ICT assets to ensure that they continue to meet and support business and risk management requirements. Payment institutions will monitor whether their ICT assets are supported by their external or internal providers and whether all relevant patches and upgrades are applied based on documented processes. Payment institutions will assess and mitigate the risks stemming from outdated or unsupported ICT assets.

56. Payment institutions will determine and implement ICT system performance and capacity planning and monitoring processes to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.

57. Payment institutions will define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups will be determined in line with business recovery requirements and the criticality of the data and the ICT systems and evaluated according to the performed risk assessment. Payment institutions will test the backup and restoration procedures and the ICT systems on a periodic basis.

58. Payment institutions will ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.

Information and communication technologies incident and problem management

59. Payment institutions will establish and implement an incident and problem management process to monitor and log operational and security ICT incidents to ensure they can continue or restore, in a timely manner, critical business functions and processes when disruptions occur. Payment institutions will determine appropriate criteria and thresholds for classifying events as operational or security incidents, as well as early warning indicators that will serve as alerts to enable early detection of these incidents. When doing so, payment institutions will apply the classification of major incidents according to the European Banking Authority Guidelines on major incidents reporting under Directive (EU) 2015/2366 on payment services in the internal market (PSD2).

60. To minimize the impact of adverse events and enable timely recovery, payment institutions will determine and apply appropriate processes and have appropriate organizational structures to ensure a consistent and integrated monitoring, handling and follow-up of operational and security incidents and to make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents. The incident and problem management process will include

(a) the procedures to identify, track, log, categorize and classify incidents according to a priority, based on business criticality,

(b) the roles and responsibilities for different scenarios, e.g. errors, malfunctioning, cyberattacks and other incidents,

(c) procedures to identify, analyze and solve the root cause behind one or more incidents, while payment institutions will
   1. analyze operational or security incidents likely to affect them that have been identified or have occurred within and/or outside the payment institution,
   2. consider key lessons learned from these analyses and update the security measures accordingly,

(d) effective internal communication plans, including incident notification and escalation procedures, also covering security-related complaints from payment service users, while these procedures will ensure that
   1. incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant person with competence in the field of information and communication technologies, and the management body,
   2. senior executives and the management body are informed in the event of major incidents and, at least, informed of the impact, the response and the additional controls that payment institutions will define as a result of evaluation of the incidents,

(e) incident response procedures to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner,

(f) specific external communication plans for critical business functions and processes that will enable the payment institution to collaborate with relevant stakeholders to effectively respond to and recover from the incident, and to provide timely information to payment service users and other third parties.

Information and communication technologies project management

61. Payment institutions will implement a programme and/or a project governance process that defines roles, responsibilities and accountabilities to effectively support the implementation of the information and communication technology strategy. ICT projects will be used in the event of replacement, substitution, destruction or deployment of ICT systems and ICT services. These projects may be part of broader ICT or business activities transformation programmes.

62. Payment institutions will appropriately monitor and mitigate risks deriving from their portfolio of ICT projects, considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.

63. Payment institutions will establish and implement an ICT project management policy that includes as a minimum

(a) project objectives,

(b) roles and responsibilities,

(c) a project risk assessment,

(d) a project plan, timeframe and steps,

(e) key project milestones,

(f) change management requirements.

64. The ICT project management policy will ensure that information security requirements are analyzed and approved by a function that is independent from the development function.

65. Payment institutions will ensure that all areas impacted by an ICT project are represented in the project team. The project team must have the knowledge required to ensure secure and successful project implementation and completion.

66. The preparation, beginning and progress of ICT projects and their associated risks will be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. Payment institutions will include project risk in their risk management framework.

ICT systems acquisition and development

67. Payment institutions will determine and implement a process governing the acquisition, development and maintenance of ICT systems. This process will be designed using a risk-based approach.

68. Payment institutions will ensure that, before any acquisition or development of ICT systems takes place, the functional requirements and information security requirements are clearly defined and approved by the relevant business management.

69. Payment institutions will ensure that measures are determined and implemented to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.

70. Payment institutions will determine and implement a methodology for testing and approval of ICT systems prior to their first use. This methodology will consider the criticality of business processes and assets. The testing will ensure that new ICT systems perform as intended. Payment institutions will also use test environments that adequately reflect their production environment.

71. Payment institutions will test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.

72. Payment institutions will implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, payment institutions will ensure the segregation of production environments from development, testing and other non-production environments. Payment institutions will ensure the integrity and confidentiality of production data in non-production

environments. Access to production data will be restricted to authorized users.

73. Payment institutions will determine and implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. Payment institutions will also document the development, implementation, operation and configuration of the ICT systems comprehensively to reduce any unnecessary dependency on subject matter experts. The documentation of ICT systems will contain, where applicable, at least user documentation, technical system documentation and operating procedures.

74. Payment institutions' processes for acquisition and development of ICT systems will also apply to ICT systems developed or managed by business functions and end users outside the ICT organization. In this, the payment institutions will implement a risk-based approach. Payment institutions will maintain a register of applications that support critical business functions or processes.

Information and communication technologies change management

75. Payment institutions will establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner. Payment institutions will handle the changes during emergencies, i.e. changes that must be introduced as soon as possible, following procedures that provide adequate safeguards.

76. Payment institutions will determine whether changes in the existing operational environment influence the existing security measures or require the adoption of additional measures to mitigate the risks involved. These changes will be in accordance with the payment institutions' determined and implemented change management process.

Business continuity management

77. Payment institutions will establish a sound process to ensure the smooth performance of activities and the continued operation of the payment institution (hereinafter "business continuity management") to maximize their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption.

78. As part of sound business continuity management, payment institutions will conduct business impact analysis by analyzing their exposure to severe business disruptions and assessing their potential impacts, including on confidentiality, integrity and availability, quantitatively and qualitatively. They will use internal data, the data of contractors relevant to a business process, publicly available data or other external data that may be relevant to the business impact analysis, and scenario analysis. In their business impact analysis, payment institutions will also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies.

79. Payment institutions will ensure that their ICT systems and ICT services are designed and aligned with their business impact analysis, in particular with redundancy of certain critical components to prevent disruptions caused by events impacting those components.

80. Based on their business impact analysis, payment institutions will prepare business continuity plans, which will be documented and approved by their management bodies. The business continuity plans will specifically consider risks that could adversely impact ICT systems and ICT services. The business continuity plans will support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets. Payment institutions will coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these business continuity plans.

81. Payment institutions will put business continuity plans in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions within the maximum time within which a system or process must be restored after an incident (hereinafter the "recovery time objective") and the maximum time period during which it is acceptable for data to be lost in the event of an incident (hereinafter the "recovery point objective"). In cases of severe business disruption that triggers specific business continuity plans, payment institutions will prioritize business continuity actions using a risk-based approach.

82. In their business continuity plan, payment institutions will consider different scenarios, including less likely scenarios of developments to which they may be exposed, including a cyberattack scenario. Payment institutions will assess the potential impact of the materialization of such scenarios. Based on those scenarios, payment institutions will determine how the continuity of ICT systems and ICT services as well as the information security of the payment institution would be ensured.

83. Payment institutions will develop response and recovery plans based on the business impact analysis and plausible scenarios. These plans will specify what conditions may prompt activation of the plans and what actions will be taken to ensure the availability, continuity and recovery of, at least, payment institutions' critical ICT systems and ICT services.

84. The response and recovery plans will consider both short-term and long-term recovery options. Such plans will be

(a) focused on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of payment institutions and on the payment system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions,

(b) documented and made available to the business and support sections and readily accessible in the event of an emergency,

(c) updated in line with lessons learned from incidents, tests, new risks and threats identified, and changed recovery objectives and priorities.

85. The response and recovery plans will also consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances.

86. As part of the response and recovery plans, payment institutions will take into consideration continuity measures to mitigate failures of contractors, which are of key importance for a payment institution's ICT service continuity, to a reasonable extent in line with the provisions of the EBA Guidelines on outsourcing arrangements issued by the European Banking Authority.

87. Payment institutions will test their business continuity plans periodically. In particular, they will ensure that the business continuity plans of their critical business functions, supporting processes, information assets and their interdependencies, including those functions, processes and assets provided by third parties, where applicable, are tested at least annually.

88. Payment institutions will assess the need to update their business continuity plans at least annually, based on testing results, current threat intelligence, and lessons learned from previous events. Any changes in recovery objectives, including recovery time objectives and recovery point objectives, and/or changes in business functions, supporting processes and information assets, will also be considered, where relevant, as a basis for updating the business continuity plans.

89. Payment institutions' testing of their business continuity plans will demonstrate that they are able to sustain the viability of their businesses until critical operations are re-established. Payment institutions will, in particular

(a) include testing of an adequate set of severe but plausible scenarios, including those considered for the development of the business continuity plans, as well as testing of services provided by third parties, where applicable; this will include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored afterwards,

(b) design the testing to challenge the assumptions on which business continuity plans rest, including governance arrangements and crisis communication plans, and

(c) include procedures to verify the ability of their staff and contractors, ICT systems and ICT services to respond adequately to the scenarios defined under letter (a).

90. Payment institutions will ensure that test results will be documented and any identified deficiencies resulting from the tests will be analyzed, addressed and reported to the management body.

91. In the event of a disruption or emergency, and during the implementation of the business continuity plans, payment institutions will ensure that they have effective crisis communication measures defined and implemented so that all relevant persons inside the payment institution, payment service users and other stakeholders, including the competent authorities when required by national regulations, and also relevant contractors are informed in a timely and appropriate manner.

Payment service user relationship management

92. Payment institutions will define and implement processes to enhance payment service users' awareness of the security risks linked to the payment services by providing payment service users with assistance services and consultancy.

93. Payment institutions will ensure that the assistance services and consultancy offered to payment service users will be updated in the light of new threats and vulnerabilities, and changes will be communicated to the payment service users.

94. Where product functionality permits, payment institutions will allow payment service users to disable specific payment functionalities related to the payment services offered to the payment service user.

95. Where payment institutions have agreed with the payment service user on limits under Article 163 of the Act, they will provide the payment service user with the option to adjust these limits up to the maximum agreed limit.

96. Payment institutions will provide payment service users with the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their accounts.

97. Payment institutions will keep payment service users informed about updates in security procedures that affect payment service users regarding the provision of payment services.

98. Payment institutions will provide payment service users with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services. Payment institutions will appropriately inform payment service users about how such assistance can be obtained.