OFFICIAL INFORMATION
OF THE CZECH NATIONAL BANK

of 27 May 2011

regarding the pursuit of business in the financial market – operational risk in the area of information systems

1. This Official Information follows up on the Official Information of the Czech National Bank of 10 December 2010 regarding the pursuit of business in the financial market: Qualitative Requirements Relating to the Conduct of Business – Fundamental Information.

2. The intention of the Czech National Bank is to provide a substantive explication and additional information on the pursuit of business in the financial market as regards qualitative requirements[1] relating to operational risk in the area of information systems to which a financial services provider[2] is or could be exposed. More detailed information of the Czech National Bank is provided in the annex to this Official Information.

---

[1] For instance:
- banks and savings and credit unions are required by law to establish, maintain and apply a functional and effective management and control system, including a risk management system and an information system; more detailed qualitative requirements for these areas are specified in part three and in Annex No. 1, Part 3, of Decree No. 123/2007 Coll., as amended (hereinafter "Decree No. 123/2007 Coll.");
- as regards the pursuit of the business of a central depository of securities, some qualitative prerequisites are specified in Decree No. 233/2009 Coll., on applications, approval of persons and the manner of proving professional qualifications, trustworthiness and experience of persons, and on the minimum amount of funds to be provided by a foreign bank to its branch (hereinafter "Decree No. 233/2009 Coll."), e.g. in Article 12 (a) (5); if the central depository of securities operates a settlement system, the depository will be subject, among other, to Article 83 (9) (k) of Act No. 256/2004 Coll. on capital market undertakings, as amended (hereinafter the "Act on Capital Market Undertakings");
- under the Act on Capital Market Undertakings, an investment firm is obligated to apply a management and control system which also includes risk management; more detailed requirements are set out in part three of Decree No. 123/2007 Coll., which implements the relevant provisions of the Act on Capital Market Undertakings;
- under Article 48 (b) and (c) of the Act on Capital Market Undertakings, a regulated market operator is obligated to introduce procedures for risk management and for ensuring the proper operation of its business and other systems; some qualitative prerequisites for the performance of the activities of a regulated market operator are further specified in Decree No. 233/2009 Coll., e.g. in Article 9 (l);
- under Article 6 (1) of Act No. 277/2009 Coll., on the insurance industry, insurers and reinsurers are obligated to establish and, at all times, maintain a functional and effective management and control system, to evaluate, on a regularly basis, the information produced by the system and to take adequate measures on a timely basis; more detailed requirements for the management and control system, including the requirements for risk management and information system, are set out in Annex No. 1 of Decree No. 434/2009 Coll., which implements certain provisions of the Act on the Insurance Industry;
- under, among other, Article 83 (9) (k) of the Act on Capital Market Undertakings, a settlement system operator is obligated to have in place the settlement system rules that define a risk management system; some qualitative prerequisites for the performance of the activities of a settlement system operator are further specified in Decree No. 233/2009 Coll., e.g. in Article 11 (d).

[2] Annex No. 1 (1) (d) of the Official Information of the Czech National Bank of 10 December 2010 regarding the pursuit of business in the financial market: Qualitative Requirements Relating to the Conduct of Business – Fundamental Information.

3. While exercising its supervision powers, the Czech National Bank checks the compliance of financial service providers with the applicable requirements of legal regulations. While exercising supervision, the Czech National Bank acts individually, taking into account the specific conditions of the type of business and the arrangement of the performance of the given financial services provider's activities. The Czech National Bank also takes into account the published Official Information regarding the qualitative requirements relating to the performance of activities in the financial market; this is without prejudice to the financial service provider's right to individually stipulate and apply different internal procedures (the *"comply or explain"* principle).

4. The Official Information of the Czech National Bank of 10 December 2010 regarding the pursuit of the business of a regulated market organizer, settlement system operator and a central depository of securities in the financial market – operational risk in the area of information systems, published in CNB Bulletin under number 18 of 21 December 2010, is hereby repealed.

Vice-Governor
prof. PhDr. Ing. Vladimír Tomšík, Ph.D. v. r.

Annex
More detailed information of the Czech National Bank regarding the pursuit of business in the financial market as regards qualitative requirements relating to operational risk in the area of information systems

Financial Market Regulation and Analyses Department
Financial Market Supervision Department
Responsible:
Ing. Mazánková, tel. 224 412 821
Ing. Rott, tel. 224 412 659

Annex

More detailed information of the Czech National Bank regarding the pursuit of business in the financial market as regards qualitative requirements relating to operational risk in the area of information systems

Main goals, elements and parameters of operational risk management in the area of information systems

1. The management body of a financial services provider shall approve and regularly evaluate the goals and main principles of operational risk management[3] in the area of information systems (hereinafter the "operational risk") as part of the financial services provider's risk management strategy, information systems development strategy and safety principles.

   Example 1:

   A financial services provider shall, for instance, in its information system development strategy, state the main goals and specific development tasks, a general schedule for their achievement and a sufficient specification of financial and human resources for the implementation of the strategy, including the specification of resources that are necessary for the management of related risks in case any risks of this kind can come up, shall evaluate and, as the case may be, adjust the strategy in case of significant changes in the business strategy or in its organization and the management body of the financial services provider shall take measures to implement the strategy or any changes thereto.

   Example 2:

   A financial services provider shall, for instance, based on an analysis of information system risks (clause 6) and trends in the area of information technology security, define in security policies the main security goals and principles and methods for ensuring confidentiality, integrity and availability of information.

2. In accordance with the goals and principles under clause 1, a financial services provider shall establish, maintain and apply an operational risk management system. This system shall always include especially the following elements and their mutual links:

   a) organizational prerequisites (arrangements) for operational risk management,
   b) the principles and procedures of operational risk management, which are integrated into internal rules,
   c) operational risk management controls and controls for the performance of related activities.

   Example 3:

   A financial services provider shall, for instance, integrate into its operational risk management system the main goals and principles (strategies, policy) of its activities, shall ensure that the system takes into account significant operational risk factors of its activities and processes and external risk factors (e.g. legal environment changes), shall establish and maintain the system on the basis of an analysis of the system's efficiency and effectiveness and shall take measures aimed at the mitigation of operational risk.

3. Organizational prerequisites (arrangements) for operational risk management shall include especially the following:

   a) allocating operational risk management responsibilities to units and employees;

[3] 'Operational risk' means the risk of loss due to deficiencies or failings in internal procedures, the human factor or systems, or the risk of loss due to external factors, including legal risk; the risks in the area of information systems, including outsourcing and compliance risks, constitute an important part of operational risk.

b) informing all the relevant employees to the extent necessary about the goals, principles and processes of operational risk management;
c) allocating responsibilities for the protection of assets and compliance with security principles in the area of information systems;
d) ensuring that the development of information systems takes place in a development environment logically and physically separated from the production environment;
e) performing the administration of the information system separately from the evaluation of security audit records, the inspection of the access rights allocation and the drafting and updating of security rules for the information system;
f) evaluating security audit records by an employee who is not able to alter (modify) information in the information system that relates to the activity for which the security audit record has been made.

Example 4:

A financial services provider shall, for instance, identify and regularly monitor [letter a)] the areas with a potential conflict of interest in operational risk management and shall allocate responsibilities for the performance of the relevant tasks in the operational risk management system so as to sufficiently prevent a potential conflict of interest. The responsibilities of the bodies, employees, units and committees of the financial services provider, if they have been established, shall also be defined with regard to ensuring effective communication and cooperation at the relevant levels of management and with regard to ensuring functional, effective, proper and prudent operational risk management.

Example 5:

A financial services provider shall, for instance, ensure [letter b)] that employees whose activities have an influence on operational risk management are informed to the extent necessary about the approved strategy, principles and processes of operational risk management and that they abide by these.

Example 6:

A financial services provider shall, for instance, ensure [letter d)] that:
(i) no employee involved in the development of the information system has access to the operating environment of the system and in exceptional and justified cases where any such employee has access to the operating environment it must be ensured that his/her activity in the system is checked and documented;
(ii) no employee involved in the operation of the information system has access to the development environment;
(iii) anonymised traffic data are used during the development of the information system; in exceptional and justified cases where the attainment of a goal necessitates the use of traffic data that must be at least out-of-date, it is necessary to take measures to ensure confidentiality of such data, including measures to prevent the retroactive use of such data in the production environment.

Example 7:

A financial services provider shall, for instance, ensure [letter e)] that no employee who is in charge of the administration of the information system evaluates security audit records, inspects access rights allocation, drafts or updates the security rules for the system under his/her administration or determines/decides on auditing/logging in the system under his/her factual or technical administration.

Example 8:

A financial services provider shall, for instance, ensure [letter f)] that the evaluation of security audit records is separated from activities related to the recording of events that may endanger or compromise the security of the information system and shall also ensure that these activities are subject to inspection.

4. The principles and procedures of operational risk management shall include especially the following:

a) the principles and procedures for the identification, evaluation or measuring, monitoring, reporting and mitigation of operational risk to which a financial services

provider is or may be exposed, including taking account of low frequency high severity events;

b) a set of limits used in operational risk management, including related procedures, the method of record-keeping and information flows when the limits are exceeded;
c) the principles and procedures for setting the level of accepted operational risk;
d) the principles and procedures for limiting the occurrence or unfavourable impact of the occurrence of operational risk events;
e) the principles and procedures for potential transfer of operational risk outside the financial services provider;
f) the security principles and procedures for ensuring the confidentiality, integrity and availability of information;
g) the principles of controls and procedures for controls activities in the management of this risk at all the relevant managerial and organisational levels, including checking the compliance with the defined procedures and limits for the management of this risk and verifying the output from the evaluation or measuring of this risk;
h) the principles and procedures for the physical protection of the financial services provider's assets in the area of the information system;
i) the principles and procedures for ensuring personnel security in the area of the information system;
j) the principles and procedures for dealing with security incidents in the area of the information system;
k) the principles and procedures for handling operational risk in procuring the supply of goods and services and/or in performing certain activities in the area of the information system through other parties (outsourcing), if this is being conducted or considered.

Example 9:

A financial services provider shall define [letter a)] the principles and procedures for operational risk management e.g. with regard to its size, method of governance, number of employees and the nature, scope and complexity of its operations. The financial services provider shall integrate these principles and procedures into its internal rules and ensure that all the relevant employees are made aware of these principles and procedures.

Example 10:

A financial services provider shall, for instance, define [letter b)] the limits for the purposes of management, monitoring and evaluation of operational risk and its events (e.g. limits expressed in value for including individual and/or recurring operational risk events into operational risk records) and shall predefine the procedures for defining these limits.

Example 11:

A financial services provider shall, for instance, define [letter c) to e)] the procedures for analyzing the causes of the occurrence and impact of potential and actual operational risk events on the financial services provider, for comparing the impact of the assumed operational risk related to the activities performed or planned and related expenses for risk mitigation measures against the benefits of the activities concerned and for deciding on the acceptance of the risk, transfer of operational risk outside the financial services provider and/or any restriction or termination of activities due to the impact of the operational risk assumed.

Example 12:

A financial services provider shall, for instance, define [letter f)] the security principles for the information system and important parts thereof. This definition shall be based on the financial services provider's own risk analysis and own classification (classification and evaluation) of information system assets and the parts thereof (e.g. individual information subsystems) and related processes.

Example 13:

A financial services provider shall, for instance, define [letter i)] the procedures for the management of the access of employees, customers and other authorised persons to the financial services provider's tangible and intangible information system assets (e.g. the place where important information technologies and/or other information system assets are located) and shall further define the authorised persons' material responsibility for the damage, destruction and/or theft of tangible and intangible information system assets.

Example 14:

A financial services provider shall, for instance, define [letter j)] the concept of a security incident in the area of the information system and provide for the monitoring, evaluation, resolution and reporting on security incidents and documentation of these processes.

Example 15:

When handling its activities through outsourcing, a financial services provider shall, for instance, define [letter k)], in its procedures for dealing with operational risk, the rules for the selection and evaluation of outsourcing providers (which shall be based e.g. on the basis of a combination of the following criteria: price, quality of services and products and the provider's credibility) and the method of assessing the effectiveness of services delivered by outsourcing providers and shall also determine the responsibilities and inspection and other duties of the relevant employees for the outsourced activities.

5. Operational risk management controls shall include especially the following:
   a) monitoring the compliance with the operational risk management principles and procedures at all managerial and organisational levels;
   b) reasonable controls for individual processes, including those that have been outsourced;
   c) an on-site inspection in the area of the information system,
   d) an independent verification of the operational risk management system and the functionality and security of the information system by an internal audit or another comparable independent verification;
   e) establishing and maintaining a system for monitoring measures to remedy any identified deficiencies.

Example 16:

A financial services provider shall, for instance, monitor [letter a)] the compliance with the rules for approving rights of access to the information system, the monitoring of access to the information system, the recording and evaluation of operational risk events in the area of access to the information system.

Example 17:

A financial services provider shall, for instance, define [letter b)] the criteria/indicators for the monitoring and evaluation of operational risk in processes and management lines in the area of the information system and shall integrate their review into its routine control activities.

Example 18:

A financial services provider shall, for instance, check [letter c)] physical restrictions on access to tangible property and other information system assets.

Example 19:

A financial services provider shall, for instance, keep records [letter e)] of all measures taken to remedy any identified deficiencies in the area of the information system, shall monitor and evaluate the remedy of such deficiencies in these records and motivate the relevant employees to remedy the deficiencies.

Selected procedures

6. A financial services provider shall perform an analysis of risks associated with the information system for the purposes of defining security goals and principles and adopting measures to minimize the information system risks. In this analysis the financial services

provider shall, most importantly, define the information system assets[4], the threats to which they are exposed, the vulnerable points in the information system, the likelihood of the threats being fulfilled, and an estimate of their impacts and countermeasures. A financial services provider shall regularly update the analysis of risks associated with the information system.

Example 20:

A financial services provider shall, for instance, develop procedures for analysing the risks associated with the information system and shall develop its own classification of its information system assets. The risk analysis shall be updated e.g. in the event of significant changes in the information system, significant information technology developments (changes) and/or significant changes in any areas related to their security.

7. A financial services provider

a) shall develop and maintain plans for the resumption of its activities in the event of an unplanned interruption or restriction of its activities in the area of the information system, especially a breakdown of the information system, a failure by any person through whom activities in the area of the information system are performed (outsourcing), or a failure of an external infrastructure important for the information system, e.g. energy supplies (hereinafter the "contingency plans");
b) shall ensure that the contingency plans are regularly tested, evaluated and, where necessary, updated;
c) shall ensure that the relevant employees are familiarised with the contingency plans and act according to them.

Example 21:

A financial services provider shall, for instance, define [letter a)] the priorities for the resumption of its activities in the area of the information system and the procedures for the development and modification of the contingency plans, identify the risk events posing a threat to these activities and evaluate the likelihood of their occurrence and the impact on the financial services provider.

For the purposes of the resumption of activities, the contingency plans shall stipulate e.g. the following measures:

(i) the actions to be taken immediately after the occurrence of a crisis situation in order to minimise damage;
(ii) the actions to be taken after the occurrence of a crisis situation in order to liquidate the consequences of the crisis situation;
(iii) the method of backing-up;
(iv) the method of ensuring emergency operations, including the minimum functions that must be maintained;
(v) a method to resume activities, including activities performed by third parties (outsourcing).

In its contingency plans a financial services provider shall, for instance, also define the specific responsibilities of units and employees and the deadlines for the resumption of activities.

Example 22:

A financial services provider shall, for instance, evaluate and, where appropriate, modify [letter b)] the contingency plans in the event of significant changes in the organization and/or the nature, scope or complexity of activities, shall test the effectiveness of procedures and their practical implementation. The results of these tests shall be documented.

Example 23:

A financial services provider shall, for instance, verify [letter c)] whether up-to-date contingency plans are available to all the relevant employees and whether they able to act in accordance with these plans.

[4] 'Information system asset' means information technology, information stored in the information system and the documentation of the information system.

8. When performing its activities, a financial services provider shall ensure especially the following in the area of the information system:

   a) compliance of the operational risk management activities performed with legal and internal rules;
   b) that all approval and decision-making procedures and control activities in operational risk management, including related responsibilities, powers and internal rules, can be viewed retrospectively (reconstructed);
   c) identification of the sources of operational risk and integration of the evaluation and monitoring of this risk into routine processes;
   d) information flows in operational risk management at all the relevant managerial and organisational levels;
   e) evaluation and monitoring of information on significant and recurring operational risk events and on both actual and potential impacts and losses resulting from these events;
   f) that the relevant employees are informed about the operational risk assumed that is associated with their activities (operational risk reporting);
   g) observance of security principles and procedures;
   h) allocation of access rights to users in the information system and clear user authentication (identity verification), which must precede the user's activities in the information system;
   i) that access to information stored in the information system is provided only to the user that has been authorised for this access;
   j) protection of confidentiality and integrity of authentication information;
   k) that events that have threatened or breached the security of the information system are entered in security audit records and that these records are protected against unauthorised access, in particular their alteration (modification) or destruction, and archived;
   l) regular evaluation and, where appropriate, modification of operational risk management principles and procedures.

Example 24:

A financial services provider shall, for instance, make records of communications with the customer in connection with the provision of investment services and shall keep [letter b)] the original records of communications with the customer in connection with the provision of investment services in the event that communication with the customer takes place by means of remote communication. A financial services provider shall also use and administer equipment for communication with the customer in the event that communication with the customer takes place by means of remote communication, shall ensure that this equipment is administered only by the designated administrator, shall have an option to create a full authentic output of the communication from this equipment and shall ensure that these communication records cannot be altered.

Example 25:

A financial services provider shall, for instance, identify [letter c)] the sources of operational risk with regard to significant and other activities and at the relevant organizational levels of the financial services provider, but it shall also focus on the detection of new, not yet identified, operational risks in the area of the information system.

Example 26:

A financial services provider shall, for instance, ensure [letter e)] the monitoring and evaluation of the following:

(i) over-the-limit operational risk events and their impact on the financial services provider;
(ii) the proportion/significance of the impact of under-the-limit and recurring operational risk events to the overall impact of operational risk on the financial services provider;

(iii) operational risk on the basis of up-to-date, reliable and consistent information on events and losses resulting from this risk.

Example 27:

A financial services provider shall, for instance, ensure [letter f)] that the relevant employees are reasonably informed about the following:

(i) the evaluation of events and losses resulting from operational risk that are related to the activities of such employees;
(ii) the evaluation of operational risk criteria/indicators in the management processes and lines that concern such employees;
(iii) the results of analyses and measures taken to mitigate operational risk that is associated with the activities of such employees;
(iv) the current threats that may cause the occurrence of an operational risk event in an area of responsibility of such employees.

Example 28:

A financial services provider shall, for instance, ensure [letter h)] that:

(i) access rights are allocated to each user of the information system according to the definition of the user's activity in the information system, classification of information, verification of the user (this applies to users whose activity performed on the basis of the allocated access rights may significantly influence the security and operation of the information system) or, as the case may be, according to the conditions set forth in a written contractual agreement made between the financial services provider and a third party (an outsourcing provider, customer, etc.);
(ii) the approval procedure for the allocation of access rights is separated from the technical implementation of access rights in the information system;
(iii) an inspection of the allocation and removal of access rights is always performed for any important parts of the information system;
(iv) the information system contains tools ensuring clear user identification;
(v) the user authentication process ensures reliable verification of the user's identity, that the user authentication process is subject to inspection and that measures are taken to prevent any unauthenticated access.

Example 29:

A financial services provider shall, for instance, ensure [letter i) and j)] that:

(i) the information system contains tools ensuring that access to information in the information system is provided only to authorized users;
(ii) users' access to important parts of the information system is monitored and evaluated;
(iii) any attempts for unauthorized access are recorded and evaluated and that the performance of this activity is subject to inspection;
(iv) the information system contains tools ensuring the confidentiality and integrity of authentication information;
(v) any breach of the confidentiality and integrity of authentication information is recorded and evaluated and that the performance of this activity is subject to inspection.

Example 30:

A financial services provider shall, for instance, ensure [letter k)] that the information system supports or directly provides for the recording of any events that have threatened or breached the security of the information system into security audit records and that these events are recorded and evaluated and that the performance of this activity is subject to inspection.

Example 31:

A financial services provider shall, for instance, ensure [letter l)] regular evaluation and, where appropriate, modification of operational risk management principles and procedures, especially in connection with significant changes in its business strategy, organization of the management of internal processes, employees and/or systems and also in the conditions of the external economic, legal, technical etc. environment.

9. When operating the information system, a financial services provider shall ensure especially the following:

a) that no change in the information system can be made until the evaluation of the impact of this change on the security of the information system;
b) that it uses only software[5] that has been tested and where the test results have proved that the security features of such software comply with the approved security principles of the information system; the testing environment must be logically and physically separated from the production environment and the test results must be documented;
c) that any servicing activities are organised so as to minimise the threat to the security of the information system;
d) the backing-up of information and software that are important for the information system's proper function; any backed-up information and software shall be kept so that they are protected from damage, destruction and theft;
e) the connection of its internal network to an external communication network that is not under the financial services provider's control in a manner that minimises the possibility of infiltration into the financial services provider's information system;
f) reasonable confidentiality and integrity of information and reliable authentication of the communicating parties, including the protection of authentication information, during the transfer of confidential information via an external communication network;
g) regular verification and evaluation of the security of the information system.

Example 32:

A financial services provider shall, for instance, define and monitor the compliance with the procedures for:
(i) making changes in the information system;
(ii) software testing;
(iii) servicing activities within the information system;
(iv) the backing-up of information and software;
(v) the approval of access rights for the information system.

These procedures shall be regularly evaluated and, where appropriate, modified, especially with regard to changes in the information system and the information technology developments.

Example 33:

A financial services provider shall, for instance, draft [letter a)] a proposal for a change in the information system that contains:
(i) an analysis of the anticipated impacts;
(ii) the proposed change implementation process;
(iii) an analysis of risks, including the methods proposed for managing this risk;
(iv) an identification of the resources that need to be put aside to ensure proper management of related operational risk.

Example 34:

A financial services provider shall, for instance, ensure [letter b)] that the testing and production environments are separated and that only fictitious or anonymised data are used during testing and during the documentation of test results; in exceptional and justified cases where the attainment of a goal necessitates the use of traffic data that must be at least out-of-date, it is necessary to take measures to ensure confidentiality of such data, including measures to prevent the retroactive use of such data in the production environment.

Example 35:

A financial services provider shall, for instance, record and evaluate [letter g)] any breaches of the security of the information system.

Example 36:

[5] 'Software' means applications, procedures and rules necessary for the relevant technical equipment to perform the function required.

A financial services provider shall, for instance, ensure [letter e)] that the information system contains tools ensuring a secure connection of the financial services provider's internal network to an external communication network and that any connection security breaches are recorded and regularly evaluated and that the performance of this activity is subject to inspection.

Example 37:

A financial services provider shall, for instance, ensure [letter f)] that the information system contains tools ensuring confidentiality and integrity of information during transfer via an external communication network, especially as regards confidential information, as well as tools ensuring sufficiently reliable authentication of the communicating parties during the transfer of information via an external communication network, and shall also ensure that any breaches of confidentiality and integrity of information during transfer are recorded and regularly evaluated and that the performance of this activity is subject to inspection.

10. In the event that a financial services provider performs activities in the area of the information system through someone else (outsourcing), the financial services provider shall enter into the outsourcing contract in a manner that allows for capturing the contract's content and for the contract's inspection and potential enforcement, as well as the contract's storage (usually on paper) and shall not be thereby released from any of its duties and responsibilities; the financial services provider shall also ensure that the outsourcing arrangement does not compromise the compliance of any outsourced activities with the applicable legal regulations, the possibility of inspecting these activities by the financial services provider or the exercise of supervision by the Czech National Bank, including the potential verification of any facts related to the outsourcing arrangement with the outsourcing provider.

Example 38:

A financial services provider shall, for instance, ensure:

(i) the preparation and submission of a summary of the financial services provider's significant activities in the area of the information system that are performed by the financial services provider or the performance of which is supported on an outsourcing basis to the relevant units and persons including the Czech National Bank supervisors; this summary shall contain a description of the outsourced activities and services and the identification data of each outsourcing provider in the area of the information system;

(ii) that any contracts with outsourcing providers are concluded in an appropriate form, usually in writing;

(iii) that the outsourcing provider assumes the following contractual obligations: to perform the outsourced activities in accordance with the applicable legal regulations and the instructions of the financial services provider and to ensure the fulfilment of all outsourcing requirements even in the case of sub-outsourcing (chain outsourcing); to enable and provide assistance to the authorised/empowered employees of the financial services provider or of any third parties designated by the financial services provider during their inspections of outsourced activities; to enable and provide assistance to the Czech National Bank during the exercise of supervision; to enable and provide assistance during the performance of an audit of the financial services provider's financial statements and during other verifications prescribed by the legal regulations applicable to the financial services provider; to ensure that employees who work for the outsourcing provider have been also adequately familiarised with the financial services provider's security principles and that they will respect confidentiality, including the confidentiality of the financial services provider's security measures;

(iv) the evaluation of the potential consequences of default or non-performance by the outsourcing provider in the area of the information system and shall adequately protect itself against this possibility in the contract.