Unofficial translation

FJÁRMÁLAEFTIRLITIÐ
THE FINANCIAL SUPERVISORY AUTHORITY, ICELAND

Guidelines

No. 2/2014, on IT Systems of Supervised Entities.

Issued with reference to the second paragraph of Art. 8 of Act No. 87/1998
on Official Supervision of Financial Activities.

21 March 2014

Introduction

The Financial Supervisory Authority (FME) supervises the working practices of supervised entities as provided for in the Act on Official Supervision of Financial Activities, No. 87/1998, to ensure compliance with the rules and legislation governing supervised activities. According to the second paragraph of Art. 8 of the same Act, the FME has statutory authorisation to issue and make public general guidelines regarding the operations of supervised entities.

These Guidelines aim at setting harmonised requirements for all supervised entities with regard to the operation of information systems and the use of information technology (IT).

The principal purpose of the Guidelines is to minimise operational risk of supervised entities and encourage their compliance with rules and legislation concerning operation of IT systems. It should be noted that these Guidelines are in no way intended to replace provisions of Acts and Regulations concerning personal data protection.

Minimising the risk of operating IT systems consists, among other things, of taking measures aimed at managing operational risk, preventing conflicts of interest and ensuring market transparency. Information security also needs to be ensured, i.e. to ensure the access of authorised parties only, when such access is needed, and that data is correct and uncorrupted.

The scope of actions to ensure security of IT systems should be consistent with the scope of the supervised entity's operations and the risks it involves. The Guidelines apply to all supervised entities. However, FME sets stricter requirements on implementation for supervised entities with an extensive and varied range of activities than for smaller parties with simple activities, cf. for details Art. 1.5 of the Guidelines. Simple arrangements are therefore expected to suffice for smaller entities[1], although they should reflect the principles laid down in the Guidelines.

According to the first paragraph of Art. 8 of Act No. 87/1998, on Official Supervision of Financial Activities, the operations of supervised entities should comply with sound and proper business practices. Furthermore, it can be derived from the second paragraph of Art. 10 of the Act that the same parties have an obligation to maintain sound finances and operations. In FME's view, the above implies inter alia, that supervised entities carry out a self-assessment of their IT environment, evaluating the scope of operations and level of complexity of business systems. Based on the first paragraph of Art. 9 of the aforementioned Act on Official Supervision of Financial Activities, the FME requests that the self-assessment be submitted to the FME through its data delivery system. Once an entity has delivered a self-assessment; it is not required to submit a new one unless changes take place in those aspects described in the previous self-assessment.

International standards apply in this area and a considerable quantity of instructions are available on the operation of IT systems. Examples of such are ISO/EC 27001-27005, the ISO 9000 quality standard and CobiT. Many other European states have issued similar guidelines or rules which are taken into consideration in these Guidelines[2].

---

[1]The size of an entity is determined by the number of employees, the set-up of its IT operations and the level of complexity of its business software. A self-assessment form is accessible in FME's report delivery system.

[2] E.g. Norway - http://www.finanstilsynet.no/en/,
Sweden - http://www.fi.se/Folder-EN/Startpage/Regulations/,
Denmark - http://www.finanstilsynet.dk/?sc lang=en,
Finland - http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial sector/Pages/Default.aspx and
England - http://fsahandbook.info/FSA/html/handbook/COBS/11/8

Contents of Guidelines on IT systems operations of supervised entities

1. Scope

1.1. The Guidelines apply to all supervised entities as referred to in Art. 2 of Act No. 87/1998 on Official Supervision of Financial Activities. The above implies that those parties included in the scope of these Guidelines are to take suitable measures to ensure that all IT systems of significance for or affecting the undertaking's activities are operated in accordance with the Guidelines.

1.2. IT systems in the context of these Guidelines refer to the machine systems involved in data processing together with all connections to, from and between them.

1.3. If a supervised entity is part of a corporate group the Guidelines apply to the operations of IT systems of companies in the supervised entity's group if they affect or are of significance for the supervised entity's operations.

1.4. If an outside party is given access to IT systems it must be ensured by a written contract that the requirements of the Guidelines regarding security and documenting are met. An outside party refers e.g. to a person who is not an employee of the supervised entity.

1.5. The FME considers appropriate to take the size and scope of IT systems operations into account, when implementing and following up on these Guidelines.

2. Risk assessment

2.1. The FME considers appropriate for supervised entities to determine a criteria for acceptable risk in connection with the use of IT systems, taking into account their operational sector and level of complexity. In this context, the criterion needs to be reviewed on a regular basis and the risk of IT systems operations analysed.

2.2. In order for the abovementioned risk assessment process to achieve its objective; the FME considers that responsibility, inter alia with regard to follow up measures deriving from a prior risk assessment, must be clearly specified. Furthermore, the FME is of the opinion that a supervised entity should perform a risk assessment annually as well as in connection with changes of significance for information security, to ensure risks are within the set criteria, cf. the first paragraph of this Article.

2.3. Based on the first paragraph of Art. 9 of the Act on Official Supervision of Financial Activities, the FME requests that the implementation and outcome of the risk assessment be documented, together with proposals for improvements as necessary and follow-up.

3. Responsibility

3.1. In FME's view, a supervised entity is responsible for ensuring that IT systems operations satisfy the requirements made in these Guidelines. This also applies to IT system operations which are outsourced in part or in full to a third party. Responsibility for IT systems operations and risk management in connection with outsourcing always lies with the Board of Directors of the supervised entity and cannot be outsourced.

4. Organisation and quality

4.1. It is important for supervised entities to adopt a strategy setting out objectives and security requirements for IT systems operations. Furthermore, that written procedures are available for all work processes of material significance for the operation and security of IT systems.

4.2. It is important that such procedures clearly define the responsibility for the following aspects, with regard to IT systems operations:

- 4.2.1. Management
- 4.2.2. Equipment acquisition
- 4.2.3. Development
- 4.2.4. Operation
- 4.2.5. System maintenance
- 4.2.6. Backups
- 4.2.7. Data security
- 4.2.8. Implementation
- 4.2.9. Removal of systems and equipment from service

4.3. Documented and updated procedures of individual IT systems which are of material significance for the supervised entity's activities should be available at all times.

4.4. The supervised entity should also adopt quality targets for individual IT areas and have written processes available to follow up on quality targets as well as record keeping of deviations.

5. Security

5.1. The FME recommends that supervised entities establish work processes to ensure protection of equipment, lines, systems and data of material significance for the supervised entity's operations, cf. Art. 1.2, for:

- 5.1.1. setbacks
- 5.1.2. abuse
- 5.1.3. unauthorised access
- 5.1.4. unauthorised changes and vandalism.

5.2. Work processes in connection with the above should, in FME's opinion, cover the management, allocation, review and revocation of access authorisations to IT systems, including portable media and data processing equipment. Information security requirements should, in FME's opinion, be quantitative and deviations recorded. It must be ensured that implementation is traceable. A supervised entity should ensure that employees receive satisfactory training and instruction concerning information security as well as conveying employee responsibility with regard to information security in an organised manner.

5.3. A supervised entity should, in FME's opinion, ensure that satisfactory management and controls exist for its network in order to ensure protection against threats and to preserve the security of the systems and software which use the network, including data transmission. In this regard the FME considers that controls need to be set up for public networks and wireless networks to protect systems and user software.

5.4. It is important that a supervised entity ensures its security against viruses and malicious code through suitable defences and surveillance systems.

5.5. To provide data security and ensure confidentiality of supervised entities the FME is of the opinion that supervised entities should establish work processes to protect documents, data and storage media against unauthorised disclosure, modification, removal and destruction. Portable data media includes: inter alia smart phones, tablets and laptops, magnetic tape, magnetic discs, memory sticks, memory cards, portable hard disc drives, CDs, internal memory storage of equipment and other similar data media.

6. Systems operations

6.1. FME recommends that supervised entities base their IT systems operations on written work processes.

6.2. Work processes must ensure adequate and correct processing, handling and storage of data and access to information systems, cf. Art. 9 of these Guidelines on preservation and handling of data.

6.3. It is important that supervised entities ensure maintenance and surveillance of information systems so their operations will be stable and in accordance with plans. Maintenance should be performed on the grounds of written work processes which contribute to a reliable, organised and predictable operation of information systems.

7. System development and maintenance

7.1. It is important that supervised entities have written work processes for acquiring, developing and testing information systems.

7.2. The party responsible for the IT system in question should give approval for the use of and/or introduction of modifications to the system, before they are taken into service or changes are implemented.

7.3. Work processes concerning modifications must cover all modifications which can have an effect on information systems and must ensure suitable formal handling together with record keeping. Furthermore, work processes must cover the allocation and revocation of access authorisations to those IT environments containing real data used for development or testing.

7.4. Any deviations which arise when systems are taken into use or changes implemented in the real environment must be recorded, cf. Art. 8.4.

8. Deviations

8.1. It is important that supervised entities follow written processes covering treatment of deviations.

8.2. The processes must cover deviations occurring in the operations of information systems.

8.3. The objective of dealing with deviations should be to re-establish a normal operating situation, find the causes of the deviations and prevent them from re-occurring.

8.4. It is important that supervised entities record deviations electronically.

8.5. With reference to the first paragraph of Art. 9 a of the Act on Official Supervision of Financial Activities, the FME requires all serious deviations involving interruptions to the preservation, secrecy, integrity and availability of information systems and data to be notified to the FME.

8.6. Serious deviations as referred to in Art. 8.5 include, inter alia hacking of information systems, data leaks and data losses, unexpected interruption of the operation of information system (in part or in full) which affects activities and other similar incidents.

8.7. Serious deviations shall be notified to the FME without delay, and no later than 24 hours after they are discovered. Notifications of deviations shall be made on the form for the purpose in FME's reporting system.

9. Preservation and handling of data

9.1. The first paragraph of Art. 9 of the Act No. 87/1998, on Official Supervision of Financial Activities, provides for FME to examine the operations of supervised entities as often as necessary. They must grant the FME access to all their accounts, minutes, documents and other data in their possession regarding their activities which FME considers necessary. Furthermore, according to the provision, FME may request information in such a manner and as often as it deems necessary.

9.2. In order to achieve the objectives of the afore-mentioned provision regarding FME´s access to data of supervised entities, it is important that requested data is available at the time a request is made. As a result of this and having regard to the main purpose of these Guidelines to minimise operational risk, FME considers that preservation and handling of data by supervised entities must fulfil the following requirements:

9.2.1. Backups are made of data and information systems;

9.2.2. Arrangements and procedures for backups must, in FME's opinion, be done in an organised manner and include regular checks that backups are taken according to a documented procedure, are usable and accessible and contain, for instance, a description of the storage time, location of backups and equipment necessary for their recovery;

9.2.3. Backups of information systems containing business information shall be available for a minimum of two years from their original recording, including the backup systems needed to recover the data;

9.2.4. Backups of information systems preserving communications with orders for transactions shall be available for a minimum of five years from their original recording, including the backup systems needed to recover the data;

9.2.5. Backups of accounting systems shall be available for a minimum of seven years from their original recording, as provided for in Articles 19 and 20 of Act No. 145/1994 on Accounting, including backup systems needed to recover the data;

9.2.6. Backups shall be available to supervisory authorities on short notice and accessibility to specific data is straightforward.

9.3. The above-mentioned systems include all the supervised entity's information systems which contain records or data concerning business information and/or orders to trade. This therefore applies to all information and communication systems connected to business transactions, such as e-mail, telephone systems, mobile telephones, faxes, chat or other communication systems, as well as other data containing orders to trade.

9.3.1. .Business information refers to all information and documentation on customers and their position towards the relevant supervised entity.

9.3.2. Orders to trade refer to communications which comprise binding decisions between the parties, such as orders to execute specific transactions, confirmation of contracts etc.

9.3.3. The FME raises no objections if a supervised entity chooses to restrict the receipt of orders to trade to specific systems, such as e-mail or other equally verifiable means.

9.4. The above-mentioned backups can be necessary for the FME to reconstruct each important step in the process of specific transactions. Such reconstruction is an important part of FME's supervisory role, both as provided for in the first paragraph of Art. 8 of the Act on Official Supervision of Financial Activities as well as in provisions on supervision in various special legislation concerning sectors of supervised activities. In light of all of the above and due to the fact that it is not certain, when backups are taken, whether or when FME will request specific data it is important that the data be preserved for the specified period.

9.4.1. To preserve the security and credibility of the business information and orders to trade which are preserved in backups it is important that backups procedures take the following into account:

9.4.2.

9.4.3. Users cannot permanently erase documents, entries, messages or a transaction history from the respective information systems during the period referred to in Art. 9.2.3. The backups taken shall contain all entries in business systems, documents, records of telephone conversations, e-mails, messages or similar documentation in a continuous and traceable time sequence, if the above-mentioned data contain business information;

9.4.4. Backups are protected in such manner that it is impossible to delete or modify them by mistake in any way;

9.4.5. Access to backups is limited to authorised parties;

9.4.6. It is ensured that backups are readable to the end of the retention period;

9.4.7. Backups are preserved in a secure location in suitable distance from the original data.

10. Contingency arrangements

10.1. The FME regards it as part of sound and healthy business practices cf. the first paragraph of Art. 8 and the second paragraph of Art. 10 of the Act on Official Supervision of Financial Activities, for supervised entities to anticipate possible setbacks that could affect the continuing operations of IT systems. As a result, FME is of the opinion that supervised entities should set up an overall framework for management of continuous operations, defining roles, responsibilities, tasks and risks.

10.2. Based on a risk assessment, cf. Art. 2, the FME considers it important to define those information systems which are important for the entity's activities and are to be included in the framework.

10.3. The framework should include, in FME's opinion, the following aspects:

10.3.1. An analysis and assessment of the individual factors which may fail and what suitable measures are to be taken;

10.3.2. Clear criteria should be set for when alternate solutions are to be applied;

10.3.3. Recovery processes;

10.3.4. Information disclosure to the Board of Directors, employees, customers and other parties who need to be informed of an interruption of operations.

10.4. It is important that the framework is proportional to the size and scope of the supervised entity.

10.5. The framework must be reviewed and updated at regular intervals.

10.6. It is important that supervised entities have a documented contingency plan or emergency plan which can be applied following a setback which causes an interruption in the operation of information systems. Setbacks in this context refer to events causing reduction in the capacity of information systems.

10.7. The plan, in FME´s opinion, should at a minimum include the following aspects:

10.7.1. Oversight over information systems included in the plan

10.7.2. A description of setbacks solutions

10.7.3. Clear criteria for implementing setbacks solutions

10.7.4. Acceptable time limits for interruption of operations before setback solutions are applied

10.7.5. Work processes to return information systems to working order

10.7.6. Oversight over areas of responsibility and launching processes for setback solutions

10.7.7. Information disclosure to the Board of Directors, employees, suppliers, customers, public 10.7.8.authorities and the media.

10.8. It is important that implementation and execution of the plan entails instructions, practice exercises and testing of alternate solutions which ensure that they work as intended. Furthermore it is important that tests are documented in order to assess the implementation and performance.

11. Outsourcing

11.1. The FME recommends that supervised entities have an outsourcing policy which prescribes what aspects of IT systems operations can be outsourced and to whom they can be outsourced.

11.2. If a choice is made to outsource hosting of data to a third party, the FME instructs supervised entities to ensure that the FME can at all times retrieve information and/or data hosted by third parties in the same manner as if the Authority were seeking data stored by the supervised entity itself.

11.3. If a supervised entity chooses to outsource to a party abroad, the FME requests to be informed in advance of such outsourcing, in addition to receiving the necessary information as to where the Authority can obtain the data if necessary. Necessary information in this context includes, inter alia information on the outsourcing service provider, its country and domicile where data will be stored, information on the outsourcing service provider's contact persons and confirmation that the outsourcing service provider has been informed that the FME is authorised to have access to the data in question;

11.4. With reference to the objective in the first paragraph of Art. 9 of the Act on Official Supervision of Financial Activities, cf. also the discussion in Art. 9.1 above, the FME expects supervised entities not to use chain outsourcing when hosting information systems and data further than to a third party3, either partially or fully.

11.4.1. Chain outsourcing refers to a situation where outsourcing of IT systems by a supervised entity to a hosting party is subcontracted from the contracted hosting party to a third-party. It is not considered chain outsourcing when activities are outsourced within a corporate group.

[3] Chain outsourcing to a third party refers to a situation where a supervised entity outsources to a second party and that party outsources to a third party. FME raises no objections to such outsourcing but is of the opinion that chains should not extend to fourth parties or farther.

11.4.2. FME recommends that supervised entities do not outsource activities outside of the European Economic Area and, if they do so, only on the condition that the legal environment in the state to which activities are outsourced does not inhibit FME's access to the entities data.

11.5. A written contract with an outsourcing service provider should include at least the following in FME´s opinion:

11.5.1. Provisions as to what service(s) the outsourcing service provider is to perform (Service Level Agreement);

11.5.2. Provisions on the supervised entity's right to supervise the activities of the outsourcing service provider under the contract;

11.5.3. Provisions on confidentiality obligations of the outsourcing service provider and its employees, consistent with the confidentiality obligations which the supervised entity is subject to;

11.5.4. Provisions on FME's authorisation to access the supervised entity's data and information in the custody of the outsourcing service provider;

11.5.5. Provisions for authorising examinations, which FME considers a necessary aspect of its supervision of the supervised entity, to be carried out at the outsourcing service provider's workplace;

11.5.6. Provisions as to whether chain outsourcing is authorised and, if so, to what extent, as well as what restrictions the supervised entity places on the outsourcing service provider regarding chain outsourcing.

11.6. In connection with provisions of Art. 11.5 FME considers it important for the supervised entity to ensure, by its own actions or formal collaboration with parties other than the outsourcing service provider, that it possesses sufficient expertise (technical and legal) to fulfil its obligations under the outsourcing contract.

11.7. It is important that a service level agreement with an outsourcing service provider includes a provision specifying the responsible party within the supervised entity who is responsible for the requirements made in Art. 11.1-11.5. Furthermore, the responsible party shall monitor that the outsourcing service provider satisfies the requirements made in the service level agreement.

11.7.1. In specifying a responsible party, FME considers it sufficient to state the working title or position of the employee within the undertaking concerned, i.e. naming a specific individual is not necessary.

11.8. Management responsibility, including responsibility for follow-up of these Guidelines, cannot be outsourced in the opinion of the FME.

12. Record keeping

12.1. A documented and updated description of important IT systems, which are of significance for the supervised entity's activities, should always be available.

12.2. The FME expects supervised entities to request their internal auditor or an independent party, e.g. a party which undertakes an audit of IT systems, to assess all those aspects specified in these Guidelines. It is important that the assessor's

evaluation is organised and effective and in accordance to generally known and accepted methodology.

12.3. An evaluation as provided for in Art. 12.2 shall take into consideration the size and scope of operations.

12.4. Certification of the regulated entity according to the ISO 27001 standard for information security is equivalent to an assessment as referred to in Art. 12.2, provided that the certification is valid and the scope of the certification covers those requirements laid down in these Guidelines. A certification assessment carried out within the last year by a competent party, is equivalent to the conclusion of an assessment as referred to in Art. 12.2.

12.5. Based on the first paragraph of Art. 9 of the Act on Official Supervision of Financial Activities the FME requests that the carrying out and conclusions of an assessment as referred to in Art. 12.2, together with proposals for improvements as necessary, be documented and delivered to the FME annually in accordance with instructions found in the FME's reporting system. The same applies if a party chooses to use a certification assessment as referred to in Art. 12.4.

Reykjavík, 21 March 2014

FINANCIAL SUPERVISORY AUTHORITY

Unnur Gunnarsdóttir

Jón Andri Sigurðarson