Principles for Information Security

Expectations of the AFM regarding information security

→ Lees verder

01

Introduction

The Dutch Authority for the Financial Markets (AFM) publishes principles for specific policy areas under its supervision. Principles provide guidance to financial firms and audit firms (hereinafter jointly referred to as firms) on aspects that the AFM believes contribute to the development of the sector. In this way the AFM hopes to increase the predictability of its supervision. Firms determine themselves how they implement the principles. The implementation and application of the principles can differ from firm to firm, depending on their size, as well as the type of services and products they provide.

The AFM now provides principles in the field of information security. The principles do not replace legal requirements. The principles offer guidance in the interpretation of legal requirements. The scope of these principles is included in appendix.

1.1 The importance of information security

The management of information security risks is becoming increasingly important. This is due to the increasing digitalisation of firms and the growing threat of cybercrime.

Information security is important for both the firm and its customers. After all, customers must be able to trust the services provided. In addition, firms must handle their data with integrity and confidentiality. The AFM therefore expects firms to handle information security risks with care.

With eleven principles the AFM hopes to focus the attention of firms on its expectations regarding information security.

The AFM strives for European and national convergence in the supervision of information security within firms.

> Customers must be able to trust the services provided

02

Purpose of the principles

The AFM has defined eleven principles for information security[1]. Each principle is aimed at achieving the following objective:

Firms have taken appropriate measures and implemented procedures and processes to ensure the continuity and reliability of the information technology, the information and the provision of information, and to limit the impact of any security incidents to an acceptable level as determined by the firm.

[1] The principles have been formulated in conformity with internationally accepted risk-management frameworks for IT, such as ISO27001 and ISO27002, COBIT (COBIT 5, published by ISACA), National Institute of Standards and Technology Cybersecurity Framework (NIST), and guidelines from CPMI-IOSCO (Guidance on cyber resilience for financial market infrastructures), as well the existing supervision of information security by financial firms in the Netherlands.

The principles are interconnected and jointly serve the purpose of achieving the above objective. Each principle covers one aspect of information security, namely:

1. **Policy**
2. **Governance**
3. **Identifying threats and assessing risks**
4. **People and culture**
5. **Technology**
6. **Processes**
7. **Physical security**
8. **Data**
9. **Response and recovery**
10. **Outsourcing**
11. **Chain perspective**

The foundation of information security is formed by policy, governance, and identifying threats and assessing risks. The threats are not static. Accordingly, it is important for a firm to ensure that it continuously updates and improves its information security.

With a sound information security policy, prudent governance and the continuous identification and analysis of threats and risks, the appropriate measures can be taken in the areas of: people and culture, technology, processes, and physical security. The aim is to ensure that the data and information processed and produced are adequately protected.

Information security incidents can still occur. For this reason, firms must be able to implement response and recovery measures to limit their impact. Firms' information systems are intertwined with other, external parties. Therefore, not only risks and measures of the own firm are relevant, but also those of external parties involved.

> It is important to ensure that a firm constantly updates and improves its information security

03

Principles for information security

1. Policy

An up-to-date information security policy describes a coherent set of measures, procedures and processes to manage information security risks.

In the information security policy, a firm establishes its objectives for information security and the way in which it achieves these objectives. The AFM encourages firms to use internationally accepted frameworks for information security and cyber security[2] when drawing up their information security policy. The AFM considers cyber security as an integral part of information security.

The policy describes the principles, the IT standards used by a firm and the responsibilities, procedures and processes for embedding information security in a firm.

The information security policy applies to IT assets[3] and processes under management, personal data carriers of employees (insofar as these are authorised for business use), digital products of the organisation and outsourced IT assets and processes.

The policy states how a firm determines the requirements for the confidentiality, integrity and availability[4] of its IT assets and processes, including physical locations and data. The specific measures that follow from the information security policy are in line with these requirements.

The information security policy is kept up to date because threats and risks are evaluated periodically. Additional evaluations take place when new risks arise or the size of existing risks or threats increases significantly.

2. Governance

The firm implements a governance structure that enables effective information security.

The management of a firm is responsible for information security and has the required expertise to take this responsibility. The management is aware of the most important information security risks, threats and incidents.

Where parts of the firm do not comply with the information security policy, additional measures are taken or the risks of non-compliance are accepted after careful consideration. The implementation of the organisational structure for information security is proportionate to the business model of the firm, its size and complexity, the characteristics of the information and data created or processed and the related information security risks.

A clear division of tasks and the availability of sufficient expertise and experience are crucial for the quality of risk assessments and the effectiveness of the information security measures. The roles and responsibilities in organising, managing and controlling information security are therefore clearly assigned . The firm has sufficient capacity, knowledge and experience at its disposal in the field of information security to fulfil these roles and responsibilities.

[2] For example, ISO27001 and ISO27002, COBIT, CPMI-IOSCO and NIST.
[3] All IT hardware and software the firm has purchased or developed.
[4] The CIA triad of Confidentiality, Integrity and Availability is used to guide information security policy in an organisation.
[5] For example, using a responsibility assignment matrix.

3.
Identifying threats and assessing risks

Information security is designed on the basis of an up-to-date understanding of existing threats and risks, the potential impact of existing threats on the firm and the risk appetite of the firm.

When implementing the information security policy, measures are taken based on an understanding of existing threats and risks in the areas covered by principles 4 to 8.

Information security is dynamic. Technology and threat factors are constantly evolving. This gives rise to new risks. The firm therefore updates its risk assessment periodically [on the basis of an up-to-date insights into information security threats that are relevant to the firm]. One way of gaining insight into existing risks is testing effectiveness of the risk control measures, based on known threats. Both internal and external sources can provide added value in determining these threats.

The frequency and depth of the risk assessment is proportionate to the business model of the firm, its size and complexity, and the characteristics of the information and data created or processed. In its risk assessment, the firm takes into account its own interests as well as those of its stakeholders, such as the customers in the sector where it operates.

Based on an understanding of existing and foreseeable threats and risks, the firm assesses the adequacy of its information security measures, implementing additional ones as necessary and accepting (temporary) risks. The firm periodically reassesses risks that have been accepted. To this end, the firm applies statutory requirements and its own objectives for the confidentiality, integrity and availability of processes, systems, data and information.

4.
People and culture

The firm acknowledges the risks of human activity to information security and creates a culture in which employees are aware of their responsibilities with regards to information security and cultivates a culture that fosters open communication of incidents.

People are an important link in information security. Irresponsible or thoughtless behaviour can lead to information security incidents. This is recognised and mitigated by the firm by means of effective measures. The firm sets up processes so that people effectively contribute to adequate information security and to properly handle incident notifications made by employees. In addition, the firm implements measures like awareness programmes and training courses. The effectiveness of these measures is tested periodically in conjunction with other information security measures.

The firm recognises the risks that human activity poses for the effectiveness of the information security policy and takes adequate measures to mitigate these risks. Such risks include those attributable to internal factors (internal fraud for example) and those attributable to external factors (such as phishing via email). To mitigate these risks, firms can adopt technological, procedural and physical measures that support employees in fulfilling their responsibilities relating to information security. Any residual risks are weighed against the costs and impact of additional measures intended to mitigate them.

The management and senior management of the firm promotes the importance of information security, making employees aware of existing threats. All employees are actively made aware of their responsibilities in the field of information security and are trained accordingly.

5. Technology

The principle of 'secure by design' is used in the implementation and maintenance of systems.

The firm is encouraged to use international technology standards to embed information security in the design of IT architecture and systems. Information security risks are taken into account from the design phase onwards.

The firm recognises the risks associated with the use of new and obsolete technology and has taken measures to mitigate these risks. Changes in the firm and the IT infrastructure are implemented in such a way that information risks are reduced to an acceptable level in accordance with policy and risk appetite.

During the implementation and maintenance of systems, the adaptability of the IT infrastructure is taken into account in order to prevent the creation of dependencies on systems that are no longer replaceable.

The effectiveness of technical measures is periodically tested, in combination with other information security measures.

6. Processes

The structure of business processes safeguards the confidentiality, integrity and availability of processes and the systems utilised.

All processes of the firm are set up in such a way that they contain safeguards to guarantee the confidentiality, integrity and availability of these processes and systems (and processed data) in line with the policy and the risk appetite of the firm. Information security is an integral part of the administrative organisation and internal control. The effectiveness of the measures is tested periodically in conjunction with the other information security measures taken by the firm. Findings are followed up and communicated to the firm's (senior) management.

When designing IT development and management processes, firms are encouraged to use internationally accepted frameworks for information security. The firm implements processes to identify and mitigate information security risks in line with the information security policy. In addition, the firm implements processes to monitor threats, detect incidents and respond to them accordingly (see principle 9).

7. Physical security

The design and configuration of a firm's facilities and equipment matches the information security requirements.

The firm has adopted physical measures to supplement technical and procedural measures, like restrictions on access to facilities and equipment. Physical measures to protect facilities and equipment have been taken on the basis of an analysis of the risks of external factors (such as the probability of natural disasters), human factors (unauthorised access for example) and crisis situations (such as a power cut).

The information security risks of facilities and equipment have been mitigated in accordance with the information security policy. The effectiveness of these measures is tested periodically in line with the inherent risk of the facility and/or equipment and in conjunction with the other information security measures taken by the firm.

8. Data

Throughout the entire life cycle of data and information, measures have been taken to comply with the relevant security requirements.

Information security objectives are defined to ensure the confidentiality, integrity and availability of data and information. These have been translated into measures to ensure compliance throughout the data life cycle. These measures relate to the storage, use, and transport of data via communication channels. The effectiveness of these measures is periodically tested in conjunction with other information security measures taken by the firm.

Responsibility for data sources and the processing of this data is embedded in the firm. This concerns the adequate information security of current and historical data. Statutory requirements and internal policy regarding the confidentiality, integrity and availability of data are taken into account by the firm. This also applies to system conversions and data migrations so that historical data and the relationship between data elements remain available in accordance with the requirements stemming from legislation and the objectives arising from the information security policy.

9. Response and recovery

The firm is prepared for information security incidents in order to mitigate their impact on business operations. If such an incident occurs, the firm takes timely and effective response and recovery measures.

The firm has processes and plans in place that are activated when an information security incident is detected. At a minimum, these processes and plans include measures to (1) stop the incident, (2) limit the negative impact, (3) recover from the damage, and (4) communicate effectively with stakeholders.

Assessments are conducted during and after the recovery activities. The insights gained are incorporated into the information security policy, existing processes and systems and the communication to and training of employees.

10. Outsourcing

The firm is responsible for the information security of outsourced processes and systems.

The firm that outsources processes or IT systems to another firm in the same group or to an external party remains responsible for the information security of these processes and systems. Prior to outsourcing IT infrastructure and/or processes, the firm conducts a thorough investigation into the information security of the supplier, in which the scope and depth of the investigation is aligned to the risks to the information security of the firm. The firm is aware of the implications of the outsourcing for its relevant internal division of roles and responsibilities, as well as its risk management and chain integration. The analysis of these risk factors is regularly updated by the firm. The firm determines the impact of outsourcing on the confidentiality, integrity and availability of processes, systems, data and information and takes appropriate control measures.

The firm makes clear legally binding agreements covering the cooperation and division of responsibilities in the field of information security. This also concerns the right to carry out audits at the supplier's premise.

11. Chain perspective

The firm applies an integral chain approach when determining information security risks and appropriate measures for mitigating these risks.

An integrated chain approach means the firm is aware of the dependency of chain parties in ensuring information security of its own IT environment. The chain consists of various links of internal and external parties, including customers and supervisory authorities. The firm applies an integrated chain approach where it factors in its position in the chain, as well as its dependencies on other parties in the chain.

As a baseline, the firm assumes that other firms in the same sector and within the same chain are coalition members in protecting the sector against external information security risks. Weaknesses of one party in the chain may have consequences for other parties in the same chain. In order to identify these risks, the firm participates, where possible and relevant, in information security tests organised by authorities for sectors or chains.

The AFM encourages firms to exchange knowledge and information about information security risks and threats within chains and within the sector. Based on insight into chain dependencies, the firm aims to make agreements on information security with other parties in the chain. This includes agreements to limit the impact of large-scale incidents on the affected firm and the chain as a whole. If such agreements do not exist, the firm takes appropriate measures to limit this risk.

04

Appendix

Scope of the principles for information security

At the time of publication, the scope of the principles for information security is as follows:

- Alternative investment funds (AIF)
- Management companies of AIFs
- Undertakings for collective investment in transferable securities (UCITS)
- Management companies of UCITS
- Investment firms
- Custodians
- Financial service providers (other than banks, insurers and financial institutions)
- Pension funds
- Data reporting services providers
- Regulated markets
- Audit firms

Any questions or remarks about this policy statement?

Send an email to redactie@afm.nl

AFM

The Dutch Authority for the Financial Markets
Vijzelgracht 50, 1017 HS Amsterdam

Telephone
+31 (0)20 797 2000

www.afm.nl →

Follow us:

The text of this publication has been compiled with care and is informative in nature. No rights may be derived from it. Changes to national and international legislation and regulation may mean that the text is no longer fully up to date when you read it. The Dutch Authority for the Financial Markets is not liable for any consequences - such as losses incurred or lost profits - of any actions taken in connection with this text.