Consultation on Principles for Information Security

Expectations of the AFM regarding information security

AFM - Public

Publication date: May 14th 2019

The Dutch Authority for the Financial Markets

The AFM is committed to promoting fair and transparent financial markets.

As an independent market conduct authority, we contribute to a sustainable financial system and prosperity in the Netherlands.

Contents

1. Introduction

The Dutch Authority for the Financial Markets (AFM) is opening a consultation on the Principles for information security. As a statement of policy, principles express what the AFM expects from financial firms and audit firms (hereinafter jointly referred to as “firms”) for a specific policy area. Firms determine themselves how to meet these expectations.

The principles do not constitute new regulations, but general specifications for a wide area subject to a variety of legal standards supervised by the AFM. Accordingly, the principles do not set out how firms can comply with particular standards. Instead, they outline the AFM's expectations for an organisation's assumptions and results. The implementation and application of the principles can differ from firm to firm, depending on its size and type, as well as on the types of services and products it provides. More information on how to apply the principles can be found in Appendix 1.

Over the next few years, the AFM will hold a dialogue with firms and the financial and audit sector as whole on the application of the principles. Pursuant to these discussions, the AFM will publish good practices or further explanations as necessary. Consulting on the Principles for information security forms the starting point for this dialogue.

1.1 Scope of the Principles for information security

The target group for the Principles for information security comprises managers of alternative investment funds, managers of undertakings for collective investment in transferable securities, investment firms, custodians, financial service providers (other than banks, insurers and financial institutions), pension trustees, data reporting services providers, regulated markets and audit firms. The AFM invites the aforementioned firms and other interested parties to make their contributions to the consultation before June 25th 2019, by sending the consultation template by email to consultatieprincipes@afm.nl.

Specifically, we would like answers to the following questions:

1. To what extent do you agree with the policy statement "Principles for information security"?
2. To what extent do you disagree with the policy statement? Do you foresee any problems? If so, why?
3. What are your proposals for improvements?

After the consultation period, the AFM will use the responses as input for the final version of the Principles for information security. These will be published on its website, accompanied by a feedback statement.

2. The importance of information security

Managing the risks that threaten information security is becoming increasingly important, not only because of the ever-greater digitisation of financial firms and audit firms (see appendix 1), but also from the growing threat of cyberattacks.

Information security is important for the firm as well as for its customers. A customer needs to trust the services provided, and that its data is handled with integrity and confidentially. The AFM therefore expects firms to take a conscientious approach to the risks relating to information security.

With twelve principles[1], the AFM will help focus the attention of firms on its expectations regarding information security. The implementation will differ from firm to firm, according to nature of the services provided and to the size of the enterprise.

For its supervision of information security, the AFM adheres as closely as possible to supervisory frameworks of the Dutch Central Bank (De Nederlandsche Bank, DNB).

[1] The principles have been formulated in conformity with internationally accepted risk-management frameworks for ICT, such as 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.

3. The Principles for information security

The AFM has defined twelve Principles for information security, each one rooted in realising the main objective:

Companies have introduced measures to guarantee the confidentiality and integrity of information and the availability of information, data and systems.

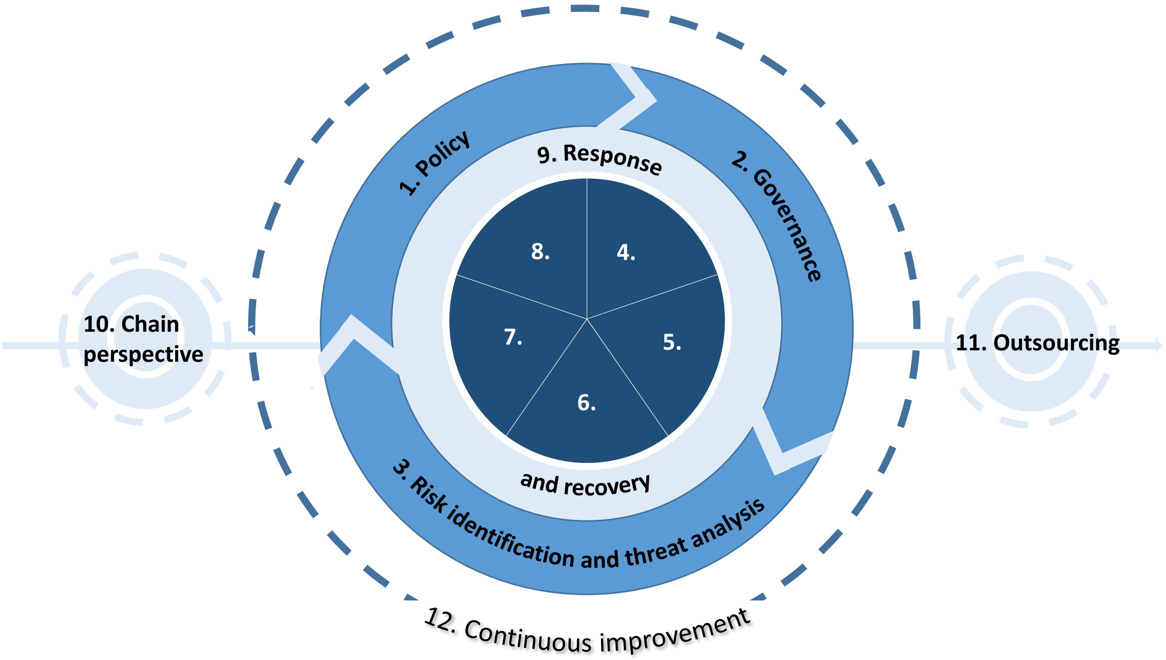
The principles are interconnected and jointly serve the purpose of achieving the above objective. Each principle covers one aspect of information security, namely:

1. Policy
2. Governance
3. Risk identification and threat analysis
4. Processes
5. People and culture
6. Data
7. Technology
8. Physical security
9. Response and recovery
10. Chain perspective
11. Outsourcing
12. Continuous improvement

The AFM has broken down the scope of information security into five areas:

a) Base (principles 1 to 3)
b) Measures (principles 4 to 8)
c) Response and Recovery (principle 9)
d) Impact of external parties on a firm's information security (principles 10 and 11)
e) Dynamics of information security (principle 12)

This is represented by the following graphic:



The base for information security comprises policy, governance, and risk identification and threat analysis. The threats are not static. Accordingly, it is important for a firm to ensure that its information security is always up-to-date and undergoing improvement.

With a sound information policy, strict governance and continuous identification and analysis of risks and threats, the correct measures can be adopted for people and culture, processes, technology, data and physical security.

Information security incidents can still occur. For this reason, firms must be able to execute response and recovery procedures to limit the impact of such incidents.

A firm's information systems are intertwined with those of other, external parties. Hence, not only are a firm's own risks and measures relevant for it, but also those of the external parties concerned.

4. Base

The first three principles concern the base for information security. In line with its policy for information security, a firm assigns the responsibilities for information security within its organisation to address the risks and threats.

4.1 Principle 1 – Policy

A current information security policy sets out the layered approach[2] to managing the risks in question.

The firm documents its objectives for information security, including how it will achieve them in an information security policy. When drawing up its information security policy, the firm utilises internationally accepted frameworks for information security and cyber security[3].

The policy sets out the assumptions and risk appetite[4], the ICT standards the firm applies, together with the responsibilities, procedures and processes for embedding information security in the organisation.

At a minimum, the information policy covers the ICT assets[5] and processes the firm manages itself, as well as the personal data devices of employees, and any outsourced ICT assets and processes.

The policy describes the method the firm uses to determine the requirements for the integrity, confidentiality and availability of its ICT assets, including physical locations and data. The procedures and measures that derive from the information security policy match the risk classifications of systems, information, data and physical locations.

It is kept up-to-date by periodically evaluating the risks and the threats. Additional assessments are carried out if new risks arise or the size of existing risks or threats increases significantly.

Firms belonging to an international group ensure that the group's centralised information policy is translated into a version tailored to local risks and requirements.

4.2 Principle 2 – Governance

The firm implemented a governance structure that underpins effective information security.

The firm’s management is responsible for information security, and is aware of the major information risks, threats and incidents. If a firm fails to comply with the standards of the

[2] The layered structure consists of a combination of technological, procedural and physical security measures employed to ensure the information security.
[3] For example, ISO27001 and ISO27002, COBIT, CPMI-IOSCO and NIST.
[4] The risk appetite for information security states the degree to which the firm is prepared to be exposed to specific information security risks.
[5] All ICT equipment that the firm has purchased or developed itself, both hardware and software.

information policy, either additional measures are taken, or the resulting (residual) risk is explicitly accepted by the firm's management.

The firm's organisation structure for information security is aligned to the business model for the firm, its size and complexity, as well as to the characteristics of the information and data that the firm creates or processes and the related information security risks.

4.3 Principle 3 – Risk identification and threat analysis

Information security is designed in accordance with up-to-date insight into the internal and external risks and threats, the potential impact of existing threats and the risk appetite of the firm.

Risk and threat analyses are conducted at regular intervals. The frequency is tailored to the business model for the firm, its size and complexity, as well as to the characteristics of the information and data that the firm creates or processes. Risk analyses are revised periodically, or if new threats to information security and vulnerabilities are identified.

When conducting a risk and threat analysis, the firm factors in 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 inherent risks and threats, the firm assesses the adequacy of its information security measures, implementing additional ones as necessary. As part of the process, the firm takes into account legal requirements and its own objectives for the continuity, confidentiality and integrity of systems and data.

5. Measures

The firm adopts a variety of measures to comply with its information security policy. Such measures cover at least process structure, people and culture, data, technology and physical security.

5.1 Principle 4 – Processes

The structure of business processes safeguards the confidentiality and integrity of information, as well the availability of data and systems.

Information security is an integral part of the administrative organisation and internal control systems. The firm's processes are configured to guarantee the continuity, integrity and confidentiality of systems and data, in line with the firm's risk appetite. The effectiveness of these measures is periodically tested, also in combination with the firm's other information security measures.

When designing ICT development and management processes, the firm utilises internationally accepted frameworks for information and cyber security[6]. It implements processes to identify information security risks and to detect threats and incidents should these arise. In this respect, we encourage firms to implement "Coordinated Vulnerability Disclosure"[7] to receive information on weaknesses in their ICT systems that are identified by third parties.

5.2 Principle 5 – People and Culture

The firm acknowledges that human action can pose an information security risk. It therefore creates a culture in which people are aware of their responsibilities with regards to information security and a culture that fosters open communication of incidents.

People are a weak link in ensuring information security. Irresponsible or thoughtless actions by a person can lead to information security incidents. This is recognised by the firm, which mitigates the possibility of such incidents occurring, for example by deploying awareness programmes and training courses. The firm designs processes that lead to employees being able to contribute effectively to an adequate level of information security, and to properly handle incident notifications made by employees. The effectiveness of these measures is periodically tested, also in combination with the firm's other information security measures.

The firm knows the risks that human action poses for the effectiveness of the information security policy and takes effective measures to mitigate these risks. Such risks include those attributable to internal factors (internal fraud for example) and those attributable to external factors (phishing by email for example). To mitigate these risks, firms can adopt technological, procedural and

[6] For example, ISO27001 and ISO27002, COBIT, CPMI-IOSCO and NIST.

[7] Such as described in "Coordinated Vulnerability Disclosure" issued by the Ministry of Justice and Security. This is a guideline for notifying and dealing with weaknesses in information systems and software products.

physical measures that support employees in fulfilling their responsibilities relating to information security. Residual risks, if any, are explicitly assessed against the effects (positive as well as negative) of additional technological measures intended to mitigate them.

Senior management communicates the importance of information security, creating employee awareness of the existing threats. In a variety of ways, all employees are actively made aware of their responsibilities for information security, and are trained to take their responsibility.

5.3 Principle 6 – Data

Measures are adopted in order to satisfy the security requirements for data and information throughout the data life cycle.

Information security measures are defined for guaranteeing the integrity, confidentiality and availability of information, data and systems. These are then translated into measures to ensure this is guaranteed throughout the entire data life cycle. These measures apply to the storage and use of data, as well to their transport through communication channels. The effectiveness of these measures is periodically tested, also in combination with the firm's other information security measures.

Security requirements governing data are taken into account in system development.

The responsibility for data sources and the processing of this data is embedded in the organisation. It concerns the effective security of current information as well as historical data. Legal requirements and internal policies applying to the availability, reliability and integrity of data are taken in consideration by the firm. These should also be adhered to in case of system conversions and/or data migrations to preserve historical data and the relationships among data elements, in conformity with the requirements stemming from the information security policy.

5.4 Principle 7 – Technology

"Secure by design" is the starting point for the design, implementation and maintenance of systems, meaning that information security measures are part of the design.

Companies are encouraged to embed information security in the design of the ICT architecture and systems. Information security risks are considered realistic possibilities that are taken into account beginning with the design phase. ICT architecture and systems are designed and configured to be secure.

The risks of using new or out-of-date technology are known to the firm, which has taken measures to mitigate these risks. Changes within the firm and its ICT infrastructure are implemented in a way that the risk of information security incidents does not increase, where possible reducing this risk.

During the implementation and maintenance of systems, the agility of the ICT infrastructure is taken into account. This is to avoid the creation of dependencies on systems that can no longer be replaced.

The ICT network is divided into segments corresponding to the security classification of the information and data available in a specific segment. Technology standards are applied to every ICT component in every segment. Any deviation is explicitly approved, based on an analysis of the risks it will entail.

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

5.5 Principle 8 – 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 ones, for example, restrictions on the access to facilities and equipment. Such physical measures are adopted in accordance with an analysis of the risks relating to external factors (natural disasters for example), human factors (unauthorised access for example) and crisis situations (resulting from a power cut for example).

Information security risks associated with facilities and equipment are mitigated in conformity with the information security policy. The effectiveness of the measures is tested regularly in line with the risks inherent to the facility and/or equipment. Tests of this are also conducted in combination with the information security measures adopted by the firm.

6. Response and Recovery

The measures deriving from the application of the principles in this document are intended to reduce the probability of an information security incident occurring. Incidents of this nature can happen nevertheless, for example, owing to ineffective measures or threats as yet undetected. For these situations, firms implement response and recovery mechanisms to limit the impact.

6.1 Principle 9 – Response and Recovery

The firm is prepared for information security incidents. If such an incident occurs, the firm takes effective response and recovery measures in time to limit the impact of the incident.

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

Assessments are conducted during and after the recovery activities. The knowledge gained is fed into the information security policy, the existing processes and systems, and the communication to employees, as well as into their training.

7. Impact of external parties on the firm's information security

A firm is connected with external parties. Examples of such links are communication channels with customers, or the outsourcing of activities to suppliers. As a result, a firm may be influenced by the information security of the parties it is connected with.

7.1 Principle 10 – Chain Perspective

The firm takes an integrated chain approach[8] when determining information security risks and the necessary measures for mitigating these risks. The firm factors in its position in the chain, as well as its dependencies on other chain parties.

As baseline, the firm assumes that other firms in the same sector and/or part of the same chain are partners as regards protecting the sector against external cyber risks. A weakness at one chain party could have implications for other parties in the same chain. To identify the associated risks, the firm participates, where possible and relevant, in information and cyber security tests organised by the authorities for sectors or chains.

The firm determines the added value of exchanging information with the other parties in the chain, as well as between itself, its customers and the relevant authorities. The purpose of exchanging information in this context is to obtain a reliable picture of the threats within the chain. It concerns information security measures and existing threats, as well as incidents.

Based on insight into chain dependencies, the firm strives to cooperate with chain partners to improve information security of the whole chain. This includes reaching agreements on limiting the impact of a large-scale incident on the firm affected and on the chain as a whole. If such agreements do not exist, the firm assumes that no measures have been adopted for information security by chain partners and will adopt measures itself to limit the risk.

7.2 Principle 11 – Outsourcing

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

A group firm that outsources processes or ICT systems to another firm in the same group or to a party external to the group remains responsible for the information security of these activities and systems. Prior to outsourcing ICT infrastructure and/or processes to a supplier, the firm conducts a due diligence investigation into the information security of the supplier concerned. As

[8] An integrated chain approach means the firm is aware of the dependency of chain parties in ensuring information security of its own ICT environment. The chain comprises many links in the form of internal and external parties, among them being customers and supervisory authorities.

part of the investigation, the information security risks entailed by the outsourcing are considered, as well the opportunity to professionalise the information security.

The firm is aware of the implications of the outsourcing for the roles and responsibilities concerned, risk management and chain integration. Regular updating of the related risk-factors is carried out by the firm. The firm determines the effect of outsourcing on the availability, confidentiality and integrity of data and systems, adopting suitable measures as necessary.

The firm is expected to enter into contracts covering the collaboration and objectives relating to information security. Control measures can also be part of such contracts, such as the right to audit the supplier. Arrangements are made not just for the initial stage of the collaboration. It is important for the parties concerned to look ahead and consider all stages of the entire outsourcing cycle, irrespective of whether a short or long collaboration is involved.

8. Dynamics of information security

Information security is not static. Technology and threats, external or otherwise, are constantly evolving, which leads to the emergence of new risks. A firm is therefore compelled to constantly improve its information security.

8.1 Principle 12 – Continuous Improvement

The firm is constantly improving its information security, based on up-to-date insight into existing threats and developments in the field of information security.

Changes to the internal and external operating environment of the firm are identified, and the potential impact of these changes on information security is evaluated. The firm takes steps to ensure that these changes have no adverse effect on its information security.

Appendix 1 – Scope of the Principles for information security

At the time of publication, the scope of the Principles for information security was as follows:

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

Appendix 2 – Principles: new statement of policy from the AFM

The AFM publishes principles to supplement existing policy statements, specifically the policy regulation, the interpretation and the guideline. In this document, we explain what principles are, why the AFM is publishing them, what part the principles play in supervision, and what this means for firms under supervision by the AFM.

What are Principles?

Principles express what the AFM expects from firms for a specific policy area. Firms determine themselves how to meet these expectations. It may concern new areas or areas for which unclarity exists in the sector. Principles are not new rules. Instead, they elaborate on the spirit of the law, based on the legal framework that defines the AFM's supervisory mandate. The principles are formulated at a relatively abstract level. For those subjects for which standards and/or frameworks are generally accepted, the principles will take a more concrete form. The principles apply irrespective of the type of firm.

Why have Principles?

To provide clearer expectations for a wider area, the AFM takes the initiatives by drawing up a set of principles. With this approach, the AFM aims to create a picture of what consumers and other end-users in the financial and audit sector can expect from firms falling within these policy areas. The principles the AFM formulates are based on multiple legal standards. Often these are open standards that the AFM in its role as supervisor interprets given a certain context. For example, the AFM supervises compliance with the regulations applying to the duty of care, advice, honest and controlled business operations and product development.

Leveraging firms' knowledge and capacity

By issuing principles, the AFM provides guidance for a particular area without being prescriptive. Principles do not prescribe how firms have to meet a particular standard. Instead, they outline the expectations that the AFM has for the results. Firms make their own choices in applying the principles to their own situation. The AFM expects to increase the efficiency of supervision by leveraging the firm's knowledge and capacity.

Room for customisation

The principles allow for customisation to cater for the large diversity in firms that are under its supervision, as such giving them a more active role. It is a firm's own responsibility to apply the principles to their products, services and business operations. How the principles are interpreted can differ from firm to firm, depending on size and types of services, and kinds of products provided.

How do principles differ from a guideline?

With principles, the AFM states the more general outcomes it expects for a broader subject covered by multiple legal standards. Principles resemble guidelines, as both provide guidance for the sector. With a guideline, the AFM specifies its expectations in respect of a specific legal standard.

What does the AFM expect from firms?

For its supervision, the AFM assumes that firms take note of the contents of the principles and apply the expectations reflected in the principles. Firms apply the principles themselves to their products, services, disclosure of information, policy and business operations. In this way, they interpret the principles in terms that are suitable for their firms. The AFM reviews the justifications for the choices that firms make and will enter into dialogue with firms based on firms' interpretations.

What can firms expect from the AFM?

The AFM determines which areas require the issuance of principles, and draws up such principles in consultation with the sector. As such, the AFM takes the initiative for further development of the sector in these areas, increasing the predictability of the supervision at the same time.

Principle based supervision

Over the next few years, the AFM will hold a dialogue with firms and the sector as whole on drawing up and implementing principles. Pursuant to these discussions, the AFM will as necessary publish good practices or further explanations.

Firms can rest assured that the AFM will act in accordance with its published principles. Principles in themselves are not enforceable. If required, the AFM will fall back on the underlying legal standards for enforcement.

The Dutch Authority for the Financial Markets
T +31(0)20 797 2000 | F +31(0)20 797 3800
PO Box 11723 | 1001 GS Amsterdam
www.afm.nl

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.