AFM

Information Security of Capital Markets

Exploratory study

AFM

Table of Contents

1 Introduction

Background
In 2022, the AFM investigated the IT security of capital market firms. This investigation was based on the information security good practice methodology of De Nederlandsche Bank (DNB)[1]. This methodology includes 58 control measures to mitigate information security risks. As part of this investigation, the AFM asked capital market firms (operators of trading venues and proprietary traders) to self-assess the maturity of their IT security controls[2]. No supporting documentation was requested by the AFM.

In 2023, the AFM performed a follow-up investigation for nine selected controls of the information security good practice methodology. Five capital market firms (trading venues and proprietary traders) were selected. We only selected firms where the maturity level of controls based on the internal self-assessment was at least level 3 ("defined") based on the maturity levels of the information security good practice methodology. A control is "defined" when it is documented and executed in a structured and formal manner.

To gain a better understanding of the actual maturity of IT security controls, the AFM asked the selected firms to provide supporting evidence. This consisted of policies and procedures, a registry of risk assessments, service level reports, business continuity plans and test results. The AFM assessed whether the received documentation was in line with a maturity level of at least level 3 ("defined"). To further challenge the self-assessments, the AFM also interviewed compliance, IT risk and security functions of the selected firms. The AFM did not perform process walkthroughs or controls effectiveness testing.

The nine selected controls for this investigation are an important, but non-exhaustive, foundation for the requirements in the Digital Operational Resilience Act (DORA), which will apply from January 17, 2025. However, compliance or non-compliance with DORA was not part of the scope of this review. For all capital market firms, the AFM recommends starting a DORA compliance implementation programme in a timely manner.

Conclusion
During our investigation we found no evidence that the selected control measures had a maturity level lower than 3 ("defined"). We nonetheless identified three main recommendations for improvement.

- Each selected firm maintained IT risk registers/profiles. However, the quality of those risk registers/profiles differed. Some risk registers only contained a high-level risk assessment of inherent and residual risks, while others only contained a log of open residual risks but did not have a complete overview of inherent risks. This made it challenging for the AFM to determine whether the executed risk assessments were complete and sufficient. Additionally, not all firms assessed whether residual risks were within their 'risk tolerance' and key risk indicators were not always defined and reported on to local management.

- Although each selected firm had implemented measures to prevent and respond to cyberattacks and performed vulnerability scanning and pentests, cybersecurity scenarios were not always part of the annual business continuity test. This is an important control to ensure that the firm can recover from cybersecurity attacks, such as a ransomware attack.

[1] DNB - Good Practices Information security 2019-2020
[2] Capital markets sector vulnerable to cyber attacks; AFM makes recommendations

- Several of the selected firms are part of an international group and outsource significant parts of their IT intragroup. These intragroup arrangements can be complex if services of different group functions are used and in the case of sub-outsourcing (for example to a cloud service provider). The AFM identified that service level management of intragroup outsourcing was in certain cases less formalised than external outsourcing arrangements.

2 Detailed results

2.1 Introduction

As part of this investigation, nine controls of the IB good practices framework were selected for assessment. These nine controls are shown below.

Element	Control measure	
Governance	1	Define an information security plan
	1.1	Information security plan
Risk management cycle	4	Assess and manage (IT) risks
	4.1	IT risk management framework
	4.2	Risk assessment
	4.3	Maintenance and monitoring of a risk action plan
Organisation	5	Information security organisation
	5.1	Responsibility for risk, security and compliance
Processes	11	Continuity management
	11.1	IT continuity plans
	11.2	Testing of the IT continuity plan
Outsourcing	14	Manage third-party and supplier services
	14.1	Monitoring and reporting of SLAs
	14.2	Supplier risk management

In this chapter, our main observations during this investigation are described for each control measure.

2.2 Governance: define an IT information security plan

Control 1.1: Information security plan

Requirements regarding the availability, integrity and confidentiality of information are based on business objectives, operational processes, risk and compliance and are translated into an information security policy and, consequently, an information security plan. The information security policy addresses the firm's resilience against cyberthreats.

Observations
Each firm had an information security policy and the policy had been recently reviewed. The information security policy was often based on frameworks like COBIT, NIST and ISO 27001, but it was not always clear which framework was used. The information security policies contained both organisational and technical

principles to improve information security and cyber resilience. Some of the investigated firms adopted the information security policies and procedures of the group. It was not always clear whether the Dutch entities had reviewed whether these policies and procedures complied with local regulations.

All firms had implemented a variety of technical measures to increase cyber resilience. These include:

- Network segmentation to reduce the impact of a cybersecurity attack, including a segregation of production, development, test and office automation environments;
- Security software and tooling from external vendors, including firewalls, end point detection and response software, e-mail gateway software and SIEM tooling;
- Security vulnerability scanning and pentesting;
- Patching procedures.

Some firms are using the NIST cybersecurity framework to self-assess the maturity of their information security every year and identify areas for improvement.

2.3 Risk management cycle: assess and manage (IT) risks

Control 4.1: IT risk management framework

Capital market firms have defined an IT risk management policy and an IT risk management framework. Capital market firms have established their risk tolerance.

Observations
The selected firms had defined an IT risk management policy and an IT risk management framework. Some of the investigated firms adopted the risk management policies of the group. It was not always clear whether the Dutch entity had reviewed the group policies' compliance with local regulations. Not all firms seem to have defined a clear risk tolerance, so it was not clear whether open risks were within the risk tolerance of the firm. We have addressed this as the first main recommendation in the *Introduction*.

Control 4.2: Risk assessment

Capital market firms periodically carry out IT risk analyses. They create an overview of the opportunities and impacts associated with the inherent risks and residual risks related to information security.

Observations
Each selected firm had performed an IT risk assessment, although the approach and depth of the IT risk assessments differed. Some risk assessments were high-level. Others contained a detailed overview of open risks but did not include an overview of inherent risks and controls and had not defined IT risk categories. This makes it more challenging to determine that the risk assessment is complete and that all significant risks are addressed. We have addressed this as the first main recommendation in the *Introduction.*

Most operational risk management functions did not test the operational effectiveness of controls. The group internal audit functions of some of the selected firms tested the operational effectiveness of controls. In addition, the selected firms relied on external audits and pentests to obtain assurance that information security controls were effective. Some group IT functions were ISO 27001-certified. In some cases, it was challenging to determine that the effectiveness of all key IT controls of the Dutch entity had been tested.

Not all the selected firms had defined key risk indicators or reported key risk indicators to management. Examples of key risk indicators that were defined include:

- availability of critical IT systems;
- number and severity of IT incidents;
- findings based on audits and/or control testing;

- number of attempted cyberattacks.

Control 4.3: Maintenance and monitoring of a risk action plan

Risk action plans are drafted for unacceptable risks and detail the response to these risks. The follow-up of the implementation of the risk action plans is monitored.

Observations
The capital market firms had defined risk action plans but used different approaches to implement, plan and monitor the progress of the improvement actions. Some firms had defined a detailed security plan, including an overview and the status of information security projects. Other firms used the IT risk register to identify action plans to improve information security.

In the case of intragroup outsourcing of the IT security function, the service level reports were also used to report on the progress of IT security projects and IT security action plans. However, it was not always clear who was responsible for signing off the action plans or accepting the risk. Some firms had implemented GRC tools to monitor the status of risk mitigation.

2.4 Organisation: information security organisation

Control 5.1: Responsibility for risk, security and compliance

Ultimate responsibility for managing information security and cybersecurity risks rests with the institution's highest management level. Responsibilities for IT risk management and IT security are formalised.

Observations
Each capital market firm had an information security function, but this function was often outsourced to a centralised group function. Most of the selected firms had implemented a three lines of defence model. Each firm had a compliance function within the Dutch entity with an AFM licence. Each firm had a risk management function, but this function was sometimes shared with the group, entailing a potential risk of conflicts of interest. Most of the selected firms used a group internal audit function as a third line of defence.

2.5 Processes

Control 11.1: IT continuity plans

Capital market firms have prepared a continuity plan to limit the impact of a major disruption on the key operational functions and processes. Alternative processing and recovery options for critical IT functions are available. The IT continuity plans include cyberattack scenarios.

Observations
Each capital market firm had a business continuity plan and had performed a business continuity test less than a year ago. Business impact analyses were part of the business continuity plan to identify critical systems. Often, the disaster recovery plans were specified for specific markets or processes. Cyberattack scenarios were also included in the business continuity plans.

Control 11.2: Testing of the IT continuity plan

Capital market firms regularly test the IT continuity plan to ensure effective recovery of IT systems, resolution of shortcomings and continued relevance of the plan. The resilience against cyberattacks is tested.

Observations
Each firm had performed business continuity testing. The scope of these tests differed. Trading venues tested whether the trading platform could be run from the back-up data centre and whether crisis management procedures and communication protocols were working. Proprietary traders performed tests to determine whether trading could be resumed from other offices or from home if the office was not available. In addition, fail-over and recovery tests were performed to verify that systems could be recovered from back-ups.

Although the information security policies and business continuity plans included measures to prevent and recover from a cyberattack, cyberattack simulations were not always part of annual business continuity tests. We have addressed this as the second main recommendation in the *Introduction*.

2.6 Outsourcing: manage third-party and supplier services

Control 14.1: Monitoring and reporting of SLAs

Capital market firms have agreed specific quantitative and qualitative performance criteria with their service providers that report on these. Reports from service providers are analysed to identify both positive and negative trends and developments.

Observations
The capital market firms had outsourced significant parts of their IT. Often, this outsourcing was part of an intragroup arrangement. The main reason for organising IT as a shared service model was efficiency and standardisation of procedures, including cybersecurity.

The capital market firms in scope had contracts and service level agreements in place for both internal and external outsourcing of IT services. In addition, service level reporting of actual service levels was in place. These service level reports contained for example:

- Availability of critical IT systems;
- Status of patching of cybersecurity vulnerabilities;
- Status of security projects;
- Number and overview of cybersecurity events;
- Number of incidents;
- Overview of IT risks;
- Key risk performance indicators.

The amount and depth of information provided as part of service level reporting varied. In addition, it appeared that controls regarding internal outsourcing to group functions was often less formalised compared to outsourcing arrangements with external service providers. We have addressed this as the third main recommendation in the *Introduction*.

Control 14.2: Supplier risk management

Risks regarding the continuous and reliable provision of service by service providers are identified and mitigated.

Observations
Capital market firms used a wide range of external software and tools to manage IT and IT security. Capital market firms used third-party risk management procedures and checklists to assess the cybersecurity controls of IT service providers and to verify that these controls were sufficient.

The supply chain could potentially create backdoors that could be exploited by hackers. Capital market firms had implemented third-party risk management procedures to perform risk assessments of third-party service providers, which included:

- Information security;
- Financial position;
- Business continuity;
- Regulatory compliance.

To gain confidence that the IT vendor had adequate information security controls in place, capital market firms assessed whether the vendor could provide external assurance, such as an ISO 27001 certification or SOC2 statement. Most capital market firms indicated that there was no business case for third-party certification of intragroup IT service providers unless IT services were provided to external customers.

The Dutch Authority for the Financial Markets
PO Box 11723 | 1001 GS Amsterdam

Telephone
+31 20 797 2000

www.afm.nl

Data classification
AFM - Public

Follow us: →

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.