IT Incident Management in Capital Markets

Exploratory study

March 1, 2023

AFM

Table of Contents

1 Introduction

Trading venues and proprietary traders have a legal obligation to notify the AFM of incidents. The AFM uses these incident notifications to proactively respond to signals and developments in the industry. As such, these incident notifications contribute to the adequate functioning of financial markets and individual financial institutions and are an important part of the AFM's risk-based supervision.

Based on these incident notifications, the AFM observes an increase in IT-related incidents occurring in the capital markets. Examples of IT-related incidents are trading system outages, connectivity issues and software bugs. Due to the high level of dependence on IT, these IT incidents could have adverse effects on the robustness of the capital market infrastructure or the fairness of trading practices.

Capital market institutions are expected to manage risks, which includes minimising the impact of IT-related events to ensure controlled and sound business operations. An IT-related event can cause (significant) financial or reputational loss and could become an incident that must be notified to the AFM. Therefore, it is important for the AFM to get more insight into the measures capital market institutions have taken to reduce the impact of IT-related events and (potential) IT-related incidents. In 2021/2022, the AFM performed an exploratory study into this topic at eight capital market institutions (operators of trading venues and proprietary traders). As part of this study, we asked the firms to perform a self-assessment of the maturity level of their incident management processes and to provide the AFM with supporting documentation. This self-assessment was based on the indicative criteria described in Appendix A.[1] Measures to prevent incidents from happening were not part of this study.

In 2025, the Digital Operational Resilience Act (DORA)[2] will come into force. This new European legislation will define a broad set of requirements for ICT Risk Management, which includes incident management, (cyber) incident response and incident reporting and notification. Proprietary traders and trading venues will have to comply with this new legislation.

2 Observations

2.1 Incident notification to the AFM

Most of the trading venues in scope of the exploratory study notified the AFM of incidents during the timeframe of the study. Most of the notified incidents related to market outages. All firms in scope were aware of the obligation to notify incidents to the AFM. The AFM stresses that IT-related events could also qualify as an incident that must be notified to the AFM. The AFM has published additional guidance on its website concerning the notification of incidents.[3]

2.2 Management of IT-related incidents and events

Capital market firms are highly and increasingly dependent on IT and as a result, the likelihood and impact of IT events and incidents are increasing. All firms in scope had procedures and processes in place to identify, document and manage IT-related events and incidents to minimise the impact. The firms in scope had a

[1] The maturity levels are based on COBIT - https://www.isaca.org/
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595
[3] https://www.afm.nl/nl-nl/nieuws/2020/december/oproep-melden-incidenten

maturity level between 2 and 4 and the average maturity level was 2.6. The AFM observed a clear correlation between the size of the firm and the maturity of processes to manage IT-related events and incidents. The observed maturity level of IT incident management at trading venues was slightly higher than at proprietary traders.

The AFM expects that capital market participants periodically assess the risks of IT incidents and whether improvements need to be made to controls to ensure controlled and sound business operations. In the study, the AFM identified examples of controls to reduce the impact of IT incidents that had been implemented by several capital market firms. These examples are described below.

DORA introduces a set of detailed requirements for ICT risk management, which includes IT incident management, IT incident response and IT incident reporting and notification. The AFM observed some gaps between the incident management processes in place and the DORA requirements. The AFM recommends starting a DORA compliance implementation programme in a timely manner to ensure compliance when DORA enters into force.

IT event categorisation and prioritisation

Firms categorise and prioritise IT-related events based on their impact. By prioritising events, firms can determine which event to focus on and how to dedicate resources. This ensures that events with a higher impact and urgency are resolved more quickly than events with a lower priority.

Security event response plan

The larger firms have set up an information security department, including a Security Operations Centre (SOC). As part of the SOC, they have implemented tools to identify cyber security events and a security event response plan to counter cyber threats.

Periodically review the incident management process

The firms regularly review the controls implemented to manage IT-related events to ensure that the process is adjusted to technological and regulatory changes and to ensure residual risks are within the firm's risk appetite. The second line and/or third line of defence function is involved in the review process.

Root cause analyses and definition of action plans

Most firms in the study perform root cause analyses of IT-related incidents and use standard templates to document incidents and action plans. The main benefit of a root cause analysis is that it helps to prevent a recurrence of incidents by identifying and eliminating the underlying cause of the incident.

Key performance indicators to measure the effectiveness of incident management.

Key performance indicators (KPIs) related to IT events and incidents are defined, measured and reported to management to determine whether goals are achieved. Examples of metrics are the number of events/incidents and average time to resolve them.

Outsourcing of the IT function

Many firms have outsourced (parts of) their IT function, including IT incident management, to an external IT service provider, or to a group IT function that is not part of the Dutch legal entity. To manage outsourcing risks, firms have implemented service level agreements with the relevant IT service providers, whereby these service providers report on KPIs related to IT events and provide incident reports.

3 Conclusions

The AFM performed an exploratory study of IT incident management at 8 capital market firms. As part of this study, the maturity of IT incident management was assessed. Measures to prevent incidents from happening were not part of this study. All firms in the study had procedures and processes in place to identify, document and manage IT-related events to minimise their impact. Capital market firms have a legal obligation to notify incidents to the AFM. All firms in scope were aware of this legal obligation. The firms in scope had a maturity level between 2 and 4 and the average maturity level was 2.6. The observed maturity level of IT incident management at trading venues was slightly higher than at proprietary traders.

The combination of increased digitalisation and increased cyber threats increases the risk of IT incidents, which could have a significant impact on the business. The AFM expects that capital market participants assess the risks of IT incidents to their business and whether improvements are needed to IT incident management to ensure controlled and sound business operations. The AFM has provided an overview of controls identified in this study that firms can implement to improve their IT incident management.

In 2025, the Digital Operational Resilience Act (DORA) will come into force and proprietary trading firms and trading venues will have to comply with this new European legislation. DORA introduces a set of detailed requirements for ICT risk management, which includes IT incident management, IT incident response and IT incident reporting and notification. The AFM observed some gaps between the incident management processes in place and the DORA requirements.

The AFM recommends starting a DORA compliance implementation programme in a timely manner to ensure compliance when DORA enters into force.

Appendix A: Maturity level and indicative criteria

Level	Definition	Indicative criteria
Level 0	Non-existent	
Level 1	Initial / Ad hoc	• The incident management (IM) process is ad hoc, not documented and manual
		• Execution is dependent on individual employees
Level 2	Repeatable but intuitive	• The IM process is standardised but not fully documented and informal
		• The IM process is partially supported by automated tools
		• The recording of incident-related information is incomplete
Level 3	Defined process	• There is a formal IM process supported by integrated IT tools
		• The IM process is based on a risk assessment
		• Responsibilities for IM are formally defined
		• The IM process has been approved by senior management
		• All incidents are recorded in a standardised way.
		• The operational effectiveness of the IM process is periodically reviewed and reported to management
		• Escalation criteria have been defined
Level 4	Managed and measurable	*In addition:* • The IM process is periodically evaluated and this evaluation is documented
		• KPIs are defined and measured for the incident management process
		• Metrics of the incident management process are periodically discussed with management
Level 5	Optimised	*In addition:* • Continuous evaluation and improvement of the IM process
		• Self-assessments and gap analyses are performed
		• The IM process is benchmarked with external standards and is 'best practice' compared to other companies
		• Self-healing systems
		• Automated alert routing

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

Telephone
+31 20 797 2000

www.afm.nl

Data classification
AFM - Publiek

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.