FMA

Finanzmarktaufsicht
Liechtenstein

FMA Communication 2018/3 – Dealing with cyber risks

Communication concerning the FMA's expectations in dealing with cyber risks

Reference:	FMA Communication 2018/XX
Addressees:	- Banks under the BankG
	- Investment firms under the BankG
	- E-money institutions under the EGG
	- Payment institutions under the ZDG
	- Insurance undertakings under the VersAG
	- Insurance intermediaries under the VersVermG
	- Pension schemes under the BPVG
	- Pension funds under the PFG
	- Management companies and UCITS under the UCITSG
	- Management companies and investment undertakings under the IUG 2015
	- Alternative investment fund managers under the AIFMG
	- Trustees and trust companies under the TrHG
Applicability:	Financial intermediaries must comply with the obligations set out in this Communication from 01.10.2018
Publication:	Website
Issued:	25.09.2018
Entry into force:	01.10.2018
Last change:	25.09.2018
Legal basis:	Article 4 FMAG

Landstrasse 109 • Postfach 279 • 9490 Vaduz • Liechtenstein
Telefon +423 236 73 73 • Telefax +423 236 73 74 • www.fma-li.li • info@fma-li.li

1. Starting point and purpose

The Liechtenstein financial market is increasingly dependent on the use of technologies and IT systems. This creates opportunities, but inevitably also special risks. These include above all cyber risks – mainly operational risks related to possible losses due to cyber attacks.[1]

Against this backdrop, the FMA considers cyber risks to be a central component of internal company risk management. The FMA therefore expects cyber risks to be included in comprehensive internal risk management. This Communication sets out the FMA's expectations of financial intermediaries in dealing with cyber risks. The FMA emphasizes that the comprehensive management of cyber risks besides the technical defensive measures also includes appropriate organisational arrangements, employees and the management body.

2. Legal basis

This Communication is based on Article 4 FMAG. Its purpose is to protect the Liechtenstein financial market and clients. The FMA may provide additional, more specific rules for individual sectors or may declare European guidelines to be applicable on a supplementary basis.

3. Scope of application

- Banks under the BankG
- Investment firms under the BankG
- E-money institutions under the EGG
- Payment institutions under the ZDG
- Insurance undertakings under the VersAG
- Insurance intermediaries under the VersVermG
- Pension schemes under the BPVG
- Pension funds under the PFG
- Management companies and UCITS under the UCITSG
- Management companies and investment undertakings under the IUG 2015
- Alternative investment fund managers under the AIFMG
- Auditors and audit firms
- Trustees and trust companies under the TrHG

4. Expectations in dealing with cyber risks

Specifically, the FMA expects financial intermediaries to consider cyber risks as part of IT risk management. Financial intermediaries must cover the following aspects through their risk management and ensure effective implementation through appropriate processes and a clear distribution of tasks, roles, and responsibilities.

a. Financial intermediaries ensure identification of the institution-specific potential threats posed by cyber attacks, especially in regard to critical and/or sensitive data and IT systems. This includes carrying out regular vulnerability analyses[2] and penetration testing[3] to check security gaps and to protect critical and/or sensitive data and IT systems.

[1] Attacks from the internet and comparable networks targeting the integrity, availability, and confidentiality of the technology infrastructure, especially in relation to critical and/or sensitive data and IT systems.
[2] Analyses for identifying currently existing security gaps in the IT infrastructure and software vulnerabilities to cyber attacks.
[3] Targeted testing and exploitation of software vulnerabilities and security gaps in the technology infrastructure to gain unauthorised access to such infrastructure.

b. Financial intermediaries ensure the protection of business processes and technology infrastructure against cyber attacks, especially in regard to the confidentiality, integrity, and availability of critical and/or sensitive data and IT systems. This includes the timely performance of security-relevant software updates and necessary configuration changes.

c. Financial intermediaries ensure the timely detection and recording of cyber attacks by systematically monitoring the technology infrastructure.

d. Financial intermediaries ensure a response to cyber attacks through timely and targeted measures and, in the event of major cyber attacks, the maintenance of normal business operations in coordination with Business Continuity Management.

e. Financial intermediaries take appropriate measures to ensure the timely restoration of normal business operations following cyber attacks.

f. The FMA also expects the financial intermediaries to inform the FMA within 14 days of detection of any serious or operationally disruptive cyber attacks.[4]

The above expectations apply irrespective of whether the financial intermediaries themselves carry out relevant activities and processes or whether they outsource them or otherwise obtain them from external providers.

5. Final provisions and entry into force

This Communication was approved by the FMA Executive Board on 25.09.2018 and enters into force on 01.10.2018.

4 Serious or operationally disruptive incidents of a cyber attack may include, for example, the loss or unintentional disclosure of client data or financial and reputational damage following a cyber attack. Financial damage includes extortion payments, unauthorised transactions, and non-availability of transactions and other processes. The notification should contain sufficient information to fully trace the cyber attack and to assess its impact. If there is not enough information available at the time of the report, such information can be submitted as it becomes available. Information on traceability includes, but is not limited to:

- the nature and course of the attack
- the nature and number of affected systems and data
- the number of affected employees and clients
- the time of the attack and its detection
- classification and prioritisation
- potential risks for other financial intermediaries
- measures taken and planned

Submission of the notification does not have to be in any particular form.