FMA

Finanzmarktaufsicht
Liechtenstein

FMA Guidance 2021/17 – Implementation of the ICT Security Guideline

Reference:	FMA Guidance 2021/17
Addressees:	– Management companies and undertakings for collective investment in transferable securities (UCITS) under the Liechtenstein Act on Certain Undertakings for Collective Investment in Transferable Securities (*Gesetz über bestimmte Organismen für gemeinsame Anlagen in Wertpapieren, UCITSG*) – Management companies and investment undertakings under the Liechtenstein Law on Investment Undertakings (*Investmentsunternehmensgesetz, IUG*) – Alternative Investment Fund Managers under the Liechtenstein Alternative Investment Fund Managers Act (*Gesetz über die Verwalter alternativer Investmentfonds, AIFMG*) – Asset management companies under the Liechtenstein Asset Management Act (*Vermögensverwaltungsgesetz, VVG*) – Insurance intermediaries under the Liechtenstein Insurance Distribution Act (*Versicherungsvertriebsgesetz, VersVertG*) – Pension schemes under the Liechtenstein Occupational Pensions Act (*Gesetz über die betriebliche Personalvorsorge, BPVG*) – Pension funds under the Liechtenstein Pension Funds Act (*Pensionsfondsgesetz, PFG*)
Concerning:	FMA Guideline 2021/17
Place of publication:	Website
Date of publication:	19 May 2021
Last amended on:	–

These Guideline explain the possibility for a graduated implementation of the ICT Security Guideline (ICT Guideline – FMA-GL 2021/3) under certain conditions. Financial intermediaries are permitted, after taking into account the degree of risk and the applicability of the individual specifications, to lower the requirements and apply the principle of proportionality for the purposes of ensuring that the requirements are implemented in a manner compliant with the Guideline.

1. General information

In order to address the risks associated with the rapidly increasing number of incidents in the area of ICT security, the FMA published the ICT Security Guideline (FMA GL 2021/3) on 19 May 2021. These ICT Security Guideline will not only help to increase the level of protection for clients but will also ensure the long-term stability and integrity of the of the Liechtenstein financial market. In this respect, the ICT Guideline are based on the principle of proportionality, whereby the manner of implementation depends on the size and complexity of the individual market operator. Financial intermediaries are therefore required to assess the adequacy of the implementation.

For those financial intermediaries (according to the group of addressees) which – due to their size and complexity – are exposed to lower levels of risk in certain circumstances, these Guideline are provided as an aid to help ensure that the requirements are fulfilled in an appropriate manner according to the principle of proportionality. Based on the categorisation of the requirements (Section 2), the financial intermediary must decide upon how to implement the individual requirements set out under individual paragraph numbers in the ICT Guideline in a manner that is appropriate for the risk structure. The minimum requirements specified in Appendix I must be taken into account when determining the graduated method of implementation.

2. Categorisation

If a graduated implementation is to be carried out, the financial intermediary must arrange for a person with appropriate specialist knowledge to assess the individual requirements of the ICT Guideline in terms of risk and applicability (e.g. by means of an IT risk assessment). The risk assessment must be brought to the attention of the management body. Categorisation is not necessary if the implementation conforms to the ICT Guideline. If a reduced or event-driven implementation is intended for individual requirements of the ICT Guideline, the relevant requirements must be assessed on the basis of the following factors:

- Risk: The risk level for the respective paragraph numbers is to be classified, in a manner that is clear for third parties, as “low”, “medium” or “high”. In this respect, the risk level refers to the potential negative impact that a graduated implementation might entail for the financial intermediary, its clients, contractors, third parties or the financial market.
- Applicability: The financial intermediary shall determine the extent to which the individual requirements are applicable and/or the frequency of their application.

If a graduated implementation will be carried out instead of an implementation that conforms to the ICT Guideline, the reasons for this must be recorded in writing.

3. Graduations in the implementation

For the purposes of implementing the ICT Security Guideline for financial intermediaries (according to the group of addressees), the implementation may, depending on the categorisation, include the following graduations.

a) Implementation in conformity with the ICT Guideline: The specifications in the ICT Guideline are complied with in conformity with the Guideline. If there is no graduation, it will not therefore be necessary to provide reasons for the grading. In principle, an implementation that conforms to the ICT Guideline is possible for all requirements. In cases where the risk level has been assessed as “medium” or “high” according to the categorisation, the requirements must always be implemented in conformity with the Guideline. A standardised implementation that is based on model documents (for example in the Organisation Manual (OM)) is permissible, provided that this does not compromise compliance with the specifications.

b) Reduced implementation: In the case of specifications for which a reduced level of implementation is permissible, formal implementation requirements are relaxed in particular. Implementation must still take place, but the requirements are lowered. A reduced implementation is permissible only for the paragraph numbers specified by the FMA in Appendix I. In addition, the risk level based on the categorisation must be rated as “low”. A reduced implementation must be documented and be justified in a manner that is clear for third parties. This graduation comprises, firstly, a relaxation of

the documentation requirements (e.g. process documentation) and, secondly, the control requirements may also be relaxed, provided that this will not lead to an increase in the risk level. A standardised implementation that is based on model documents (for example in the OM) is permissible, provided that this does not compromise compliance with the specifications.

c) Event-driven implementation: An event-driven implementation of specific requirements specified in the ICT Security Guideline shall be permissible only in cases where they are not applicable – and hence there are no foreseeable risks – due to the fact that the relevant activity is not being carried out. Their non-implementation must be documented and be justified in a manner that is clear for third parties. This form of graduation is permissible only insofar as it can be determined that there are no risks and that the relevant requirement does not apply.

An implementation that conforms to the ICT Guideline is always possible, even if one or more factors listed in Section 2 have been graded as “low”. The categorisation under Section 2 must be reviewed at least once annually and on an ad-hoc basis. The graduation must also be consistent with the minimum requirements set out in Appendix I.

4. Data protection

The FMA processes personal data exclusively in accordance with the general data processing principles of the General Data Protection Regulation (Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) and in line with applicable data protection law.

All information regarding the processing of personal data, including details about the purpose of processing, the data controller and the rights of data subjects can be found in the FMA Privacy Policy, accessible at: www.fma-li.li/en/fma/data-protection/fma-privacy-policy.html

5. Entry into force

These Guideline were approved by the FMA Executive Board on 11 May 2021 and shall enter into force on 1 January 2022.

Please contact the FMA for further information.

Securities and Markets Division
Supervision Department

FMA

Appendix I: Graduations according to paragraph numbers

Section	Heading	Para. no.	Max. graduation
1.	Principles and legal bases	1–5	n/a
2.	Definitions	–	n/a
3.	ICT strategy	6	Implementation conformant with GL
		7 a–c	Implementation conformant with GL
		8	Reduced
4.	ICT governance	9	Implementation conformant with GL
		10	Implementation conformant with GL
		11	Implementation conformant with GL, para. no. 4
5.	ICT and information security risk management		
5.1	Organisation and objectives	12	Implementation conformant with GL
		13	Implementation conformant with GL
		14	Reduced
		15	Reduced
		16 a–f	Reduced
		17	Implementation conformant with GL
5.2	Determination of functions, processes and ICT assets	18	Implementation conformant with GL
		19	Reduced
5.3	Criticality grading and risk assessment	20	Implementation conformant with GL
		21	Implementation conformant with GL
		22	Implementation conformant with GL
		23	Reduced
		24	Reduced
5.4	Risk reduction	25	Reduced

		26	Reduced
5.5	Reporting	27	Implementation conformant with GL
5.6	Internal auditing	28	Implementation conformant with GL, para. no. 4
		29	Reduced, para. no. 4
6.	Information security management		
6.1	Information security Guideline	30	Implementation conformant with GL
		31	Reduced
6.2	ICT monitoring and information security	32 a–c	Reduced
		33	Reduced
		34	Reduced
6.3	Inspection, evaluation and testing of information security measures	35	Implementation conformant with GL
		36	Reduced
		37 a–b	Reduced
		38	Reduced
		39	Reduced
		40	Reduced
		41	Reduced
6.4	Training and awareness raising in relation to information security	42	Implementation conformant with GL
7.	User authorisation management		
7.1	Logical security/access protection	43 a	Implementation conformant with GL
		43 b–g	Reduced
		44	Implementation conformant with GL
7.2	Physical security	45	Implementation conformant with GL
		46	Reduced
		47	Reduced
8.	ICT operational management	48	Reduced
		49	Implementation conformant with GL
		50	Reduced

		51	Implementation conformant with GL
		52	Reduced
		53	Reduced
		54	Reduced
		55	Implementation conformant with GL
		56	Implementation conformant with GL
8.1	ICT operations security	57 a–e	Reduced
		58	Reduced
8.2	Management of ICT incidents and problems	59	Reduced
		60 a–f	Reduced
9.	ICT projects and change management		
9.1	ICT project management	61	Reduced
		62	Reduced
		63	Reduced
		64	Reduced
		65	Reduced
		66	Reduced
9.2	Purchasing and development of ICT systems	67	Reduced
		68	Reduced
		69	Implementation conformant with GL
		70	Reduced
		71	Reduced
		72	Reduced
		73	Reduced
9.3	ICT change management	74	Reduced
		75	Reduced
10.	Outsourcing (including cloud)		
10.1	Principles	76	Implementation conformant with GL
		77 a–e	Reduced
		78	Reduced
		79	Reduced

		80	Reduced, para. no. 4
10.2	Outsourcing Guideline	81	Implementation conformant with GL
10.3	Important ICT services and/or ICT systems	82	Implementation conformant with GL
10.4	Risk assessment	83	Implementation conformant with GL
		84	Reduced
		85	Reduced
		86	Reduced
		87	Reduced
10.5	Due diligence auditing	88	Implementation conformant with GL
		89	Reduced
		90	Reduced
		91	Reduced
		92	Reduced
		93	Reduced
		94	Reduced
10.6	Conflicts of interest	95	Reduced
10.7	Register of outsourcing agreements	96	Reduced
10.8	Outsourcing agreement	97	Implementation conformant with GL
10.9	Sub-outsourcing	98	Implementation conformant with GL
		99	Implementation conformant with GL
		100	Implementation conformant with GL
10.10	Data security	101	Implementation conformant with GL
		102	Reduced
		103	Reduced
		104	Reduced
10.11	Data protection	105	Implementation conformant with GL
		106	Implementation conformant with GL

		107	Implementation conformant with GL
10.12	Access, information and auditing rights	108	Implementation conformant with GL
		109	Implementation conformant with GL
		110	Implementation conformant with GL
		111	Implementation conformant with GL
		112	Implementation conformant with GL
10.13	Monitoring	113	Implementation conformant with GL
		114	Reduced
		115	Reduced
		116	Reduced
10.14	Business continuity for outsourced ICT services and/or systems	117	Implementation conformant with GL
10.15	Exit strategies	118	Reduced
		119	Reduced
		120	Reduced
		121	Reduced
11.	Disaster recovery plan and business continuity management	122	Implementation conformant with GL
		123	Reduced
11.1	Business impact analysis (BIA)	124	Implementation conformant with GL
		125	Reduced
		126	Reduced
11.2	Business continuity planning (BCP)	127	Implementation conformant with GL
		128	Reduced
		129	Reduced
		130	Implementation conformant with GL
11.3	Response and recovery plans	131	Reduced
		132	Reduced
		133	Reduced

		134	Reduced
11.4	Testing of plans	135	Reduced
		136	Reduced
		137	Reduced
		138	Reduced
11.5	Crisis communication	139	Implementation conformant with GL
		140	Implementation conformant with GL
12.	Data protection	–	n/a
13.	Entry into force	–	n/a