Guidelines compliance table

EBA/GL/2019/04

(Update: 04 April 2023) Issue date: 28 November 2019; Application date: 30 June 2020

Guidelines on ICT and security risk management

The following competent authorities* comply or intend to comply with the EBA's Guidelines on ICT and security risk management:

		Competent authority	Complies or intends to comply	Comments
Member State				
BE	Belgium	National Bank of Belgium	**Complies**	Complies as of notification date, i.e. 3 March 2021. The National Bank of Belgium (NBB) is compliant with the EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04). To this end, an NBB circular was approved by the Board of Directors on the 16th of June 2020 which became applicable on the 30th of June 2020 (NBB_2020_23)(https://www.nbb.be/doc/cp/eng/2020/20200616_nbb_2020_23en.pdf). This circular integrates the Guidelines in the NBB's policy framework for credit institutions, stockbroking firms, payment institutions and electronic money institutions governed by Belgian law (as well as for branches of such institutions that are established in Belgium but governed by the law of a non-EEA Member State, and for

		Competent authority	Complies or intends to comply	Comments
				financial holding companies and mixed financial holding companies governed by Belgian law). Furthermore, methodologies for on-site and off-site supervision are brought in-line with the Guidelines, amongst others by building upon the work that has been accomplished in this regard in the context of the Single Supervisory Mechanism.
BG	Bulgaria	Bulgarian National Bank	**Complies**	Complies as of notification date, i.e. 15 June 2020.
CZ	Czech Republic	Czech National Bank	**Complies**	Complies as of notification date, i.e. 11 February 2020.
DK	Denmark	Finanstilsynet	**Complies**	Complies as of notification date, 20 September 2022. Please note that the Danish FSA has been compliant with "EBA/GL/2019/04 – GLs on ICT and security risk management" since June 30, 2020. In the period from June 20, 2020 to June 10, 2021 the guidelines acted as a basis for interpretation under the existing rules at the time. See link for press release: https://www.finanstilsynet.dk/Nyheder-og-Presse/Sektornyt/2020/EBA_retningslinjer_IKT. On June 11, 2021 the guidelines where formally incorporated into Danish law in Annex 5 to the "Executive Order on the Management and Control of Banks, etc." Therefore, Denmark can be considered compliant as of June 30, 2020.
DE	Germany	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	**Complies**	As of date of notification, i.e. 10.11.2021. Rundschreiben 10/2021 (BA) vom 16.08.2021, Mindestanforderungen an das Risikomanagement – MaRisk https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschr

		Competent authority	Complies or intends to comply	Comments
				eiben/2021/rs_1021_MaRisk_BA.html Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021 Bankaufsichtliche Anforderungen an die IT (BAIT) https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=11
EE	Estonia	Finantsinspektsioon	**Complies**	Complies as of notification date, i.e. 25 March 2020.
IE	Ireland	Central Bank of Ireland	**Complies**	Complies as of notification date, i.e. 1 May 2020.
EL	Greece	Bank of Greece	**Intends to comply****	Intends to comply when necessary legislative or regulatory proceedings have been completed.
HR	Croatia	Hrvatska narodna banka (Croatian National Bank)	**Complies**	Date of notification: 03/04/2023. Complies as of the date of this notification. From 1 June 2021 (based on the HNB circular letters sent to all credit institutions and payment services providers), the Guidelines applies and present supervisory expectations to all credit institutions and other payment service providers. Furthermore, Decision on Adequate Information Systems Management (Official Gazette 110/2022; hereinafter: the Decision) was updated/published in September 2023 and it started to apply from 1 April 2023. Decision is fully aligned with the Guidelines and applies to all credit institution. Intends to comply when necessary legislative or regulatory proceedings have been completed.

		Competent authority	Complies or intends to comply	Comments
				The HNB intends to comply with the Guidelines by 1 June 2021. The HNB has issued (on 4 March 2021) a circular letter to all credit institutions stating that the Guidelines present supervisory expectations and that the HNB expects all credit institutions to apply the Guidelines by 1 June 2021. Such circular will be sent to other payment service providers as well, with the same date of application. Background information: The Decision on Adequate Information Systems Management (Official Gazette 37/2010; hereinafter: the Decision) governs the obligations of credit institutions relating to their information systems management. Since 2007 (when the first version of the Decision was published), all credit institutions must be compliant with the Decision. The subject matter of the Decision and a significant number of provisions are aligned with the Guidelines. However, significant changes to the Decision are necessary to achieve full alignment with the Guidelines. Since the Decision is a sublegal act (L2 regulation) under the Credit Institutions Act (L1 regulation), changes to the Decision can only be made in line with the prescribed legal process. Because of the nature (extent) of the changes of the Decision, this process entails extensive communication with

		Competent authority	Complies or intends to comply	Comments
				credit institutions and public consultations. The initial plan (as stated in our Compliance form from 28 April 2020) was to perform the necessary changes and adjustments to the Decision and complete it in the first half of 2021. However, because of unforeseen events (prolonged COVID-19 pandemic, several earthquakes in Croatia and related changes in supervisory priorities), this process cannot be completed in the initially planned timeframe. Therefore, the HNB decided to apply the Guidelines directly, as supervisory expectations.
ES	Spain	Banco de España	**Complies**	As of notification date, i.e. 08.03.2021. Clarification with regards Competente Authority: Banco de España, as the Spanish competent authority responsible for monitoring compliance with the Spanish legislation transposing Directive 2013/36/EU (CRD IV) for LSIs when providing services other than payment services.
FR	France	Banque de France	**Intends to comply****	Intends to comply by such time as necessary legislative and regulatory proceedings have been completed.
IT	Italy	Bank of Italy	**Complies**	Complies as of date of notification, 16/11/2022. The GLs apply to banks from the 4th of November 2022 (please refer to the 40th update of Circular 285/2013) and to Payment institutions and E-money institutions from the 12th of November 2022 (see Banca d'Italia's Regulation of 2/11/2022 amending the Provisions for Payment institutions and E-money institutions of 20 June 2012).

		Competent authority	Complies or intends to comply	Comments
CY	Cyprus	Central Bank of Cyprus	**Intends to comply****	The matter of ICT and security risk with respect to Credit Institutions is currently addressed by the Central Bank of Cyprus (CBC) in its Directive on Governance and Management Arrangements in Credit Institutions of July 2014. The said Directive is currently under revision. Once the revision is completed, the CBC will be fully compliant with the subject Guidelines. With respect to the Payment and Electronic Money Institutions, they have been instructed to directly apply the subject EBA Guidelines, hence the CBC is fully compliant.
		Cyprus Securities and Exchange Commission	**Complies**	Complies as of the date of this notification: 12/10/2023. https://www.cysec.gov.cy/CMSPages/GetFile.aspx?guid=0d4d5d10-9eca-4080-8aa3-3d69607616e3
LV	Latvia	Financial and Capital Market Commission	**Complies**	Complies as of notification date, i.e. 08.03.2021. https://likumi.lv/ta/id/317384-informacijas-tehnologiju-un-drosibas-risku-parvaldibas-normativie-noteikumi
LT	Lithuania	Bank of Lithuania	**Intends to comply****	Intends to comply by application date, i.e. 30 June 2020.
LU	Luxembourg	Commission de Surveillance du Secteur Financier (CSSF)	**Complies**	Complies as of notification date, i.e. 05.03.2021. https://www.cssf.lu/wp-content/uploads/cssf20_750eng.pdf
HU	Hungary	Central Bank of Hungary	**Does not comply and does not intend to comply****	Hungary has provided a full explanation of the extent of non-compliance together with full reasons for this, as well as other details of the partial compliance. Central Bank of Hungary generally complies with most of the recommendations of the EBA ICT Guideline in the Guideline No. 7/2017 (VII.05) of the Central Bank of Hungary on the protection of the IT system. This national GL collects, details and explains all of the recommendations (governance, regulations, risk analysis and management, BCP and DRP,

		Competent authority	Complies or intends to comply	Comments
				training, ICT operations management, change management, ICT systems acquisition and development ,incident handling and communication) that Undertakings must follow in Hungary regarding their IT systems and services. This Guideline is under review, and during the revision Central Bank of Hungary could include and implement all of the recommendations that was missing or differ from the GL compared to the EBA ICT GL; for example, the recommendations for project management). The revised version of the Guideline No. 7/2017 (VII.05) of the Central Bank of Hungary on the protection of the IT system will be published only in January of 20201 because of the current pandemic situation. Furthermore, the recommendations regarding the PSP-s can be found in Guideline No.26/2018 (VIII.16.) of the Central Bank of Hungary on security measures relating to the operational and security risks of payment services. Reasoning for the partial implementation: - According to the EBA ICT Guideline Section 20, risk assessment must be carried out annually. In Hungary the Government Decree No. 42/2015. (III. 12.) on the protection of the IT systems of financial institutions, insurance and reinsurance undertakings, investment firms and commodity exchange service providers regulates this question in 2§ (2). According to the latter, risk assessment must be reviewed and tested if needed because of any change or at least in every two years. According to the Bank's experience, these requirements together

		Competent authority	Complies or intends to comply	Comments
				ensure the necessary requirements for updating the risk assessments. Tightening these requirements would mean unnecessary and not risk proportionate recommendation for our undertakings. - EBA ICT Guideline in Section 78 recommends that the BCPs of the critical business functions, supporting processes, information assets of the Undertakings must be tested annually. In Hungary, the Guideline No. 7/2017 (VII.05) of the Central Bank of Hungary on the protection of the IT system defines the rules for BCPs and its testing in section 11.2.5 point g.). According to this, BCPs must be tested in case of an incident, in case of any change in business- or service processes, IT processes, technology or in the legal environment or at least during the risk analysis (that must be done at least in every two year). According to the Bank's experience these requirements together ensure the necessary testing for BCPs. Tightening this requirements would mean unnecessary and not risk proportionate recommendation for undertakings of the Central Bank of Hungary.
MT	Malta	Central Bank of Malta	**Complies**	Complies as of notification date, i.e. 3 March 2021. On 11 December 2020, the Malta Financial Services Authority issued its principle-based, cross-sectorial guidelines, entitled MFSA Guidance on Technology Arrangements, ICT and Security Risk management and Outsourcing Arrangements. This is applicable to credit institutions licensed under the Banking Act and Financial Institutions licensed in terms of the Financial Institutions

		Competent authority	Complies or intends to comply	Comments
				Act. Title 4 of the MFSA Guidance implements the EBA Guidelines on EBA/GL/2019/04. Annex 2B to Banking Rule BR/12 and Financial Institutions Rule FIR/02 were also amended in order to ensure that credit institutions and financial institutions refer to the MFSA Guidance and ensure adherence thereto. Link to MFSA Guidance: https://www.mfsa.mt/wp-content/uploads/2020/12/Guidance-on-Technology-Arrangements-ICT-and-Security-Risk-Management-and-Outsourcing-Arrangements.pdf
NL	Netherlands	De Nederlandsche Bank N.V. (DNB)	**Complies**	As of notification date, i.e. 11.03.2021
AT	Austria	Austrian Financial Market Authority	**Intends to comply****	Intends to comply by application date, i.e. 30 June 2020. The implementation of the Guidelines requires only minor updates to the current administrative practices in relation to the existing national legal basis (Articles 25 and 39 of the Austrian Banking Act (BWG; Bankwesengesetz); the Regulation on Credit Institution Risk Management (KI-RMV; Kreditinstitute-Risikomanagementverordnung) and Articles 85 and 86 of the Austrian Payment Services Act 2018 (ZaDiG 2018; Zahlungsdienstegesetz 2018).
PL	Poland	Komisja Nadzoru Finansowego	**Intends to comply****	Intends to comply by application date, i.e. 30 June 2020.
PT	Portugal	Banco de Portugal	**Complies**	Complies as of notification date, i.e. 09 March 2021. A Circular Letter was published informing all credit institutions, investment firms, payment and e-money institutions under the direct supervision of Banco de Portugal that they are required to comply with the Guidelines from their date of application of 30/06/2020 onwards.

		Competent authority	Complies or intends to comply	Comments
				(https://www.bportugal.pt/cartacircular/cc202000000029). These Guidelines were incorporated into internal procedures and are taken into account as a reference by Banco de Portugal in the supervision of LSI, payment and e-money institutions, namely in performing on-site inspections on IT Risk and other IT Risk assessments (SREP, horizontal analyses).
RO	Romania	National Bank of Romania	**Complies**	Complies as of notification date, i.e. 10 July 2020.
SI	Slovenia	Bank of Slovenia	**Complies**	Link to the measures published in the relevant jurisdiction (Uradni list RS, št. 52/2020, 15 April 2020 - 786. Sklep o uporabi Smernic o upravljanju tveganj, povezanih z IKT in varnostjo - https://www.uradni-list.si/_pdf/2020/Ur/u2020052.pdf)
SK	Slovakia	Národná banka Slovenska	**Intends to comply****	Intends to comply after the application date, on 30 June 2021.
FI	Finland	Finanssivalvonta (FIN-FSA)	**Complies**	Complies as of notification date, i.e. 8 April 2021. The FIN-FSA complies with the guidelines in practice already. GLs will be included in the FIN-FSA Regulations and guidelines 8/2014: ‘ Management of operational risk in supervised entities of the financial sector’ in the next update of the Regulations and guidelines.
SE	Sweden	Finansinspektionen (Swedish Financial Supervisory Authority)	**Complies**	Complies as of notification date, i.e. 5 May 2020.

EU Institutions – Agencies

ECB	European Central Bank		**Complies**	As of notification date, i.e. 12.01.2021. Significant Institutions as defined in Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning

		Competent authority	Complies or intends to comply	Comments
				policies relating to the prudential supervision of credit institutions.

EEA – EFTA State

IS	Iceland	Fjármálaeftirlitíð (Financial Supervisory Authority, Iceland)	**Intends to comply****	Intends to comply by application date, i.e. 30 June 2020.
LI	Liechtenstein	Financial Market Authority Liechtenstein (FMA)	**Intends to comply****	Intends to comply after the application date, on 1 January 2021.
NO	Norway	The Financial Supervisory Authority of Norway	**Complies**	Complies as of date of notification, i.e. 7 May 2020.

*The EEA States other than the Member States of the European Union are not currently required to notify their compliance with the EBA's Guidelines. This table is based on information provided from those EEA States on a voluntary basis.

** Please note that, in the interest of transparency, if a competent authority continues to intend to comply after the application date, it will be considered "non-compliant" unless (A) the Guidelines relate to a type of institution or instruments which do not currently exist in the jurisdiction concerned; or (B) legislative or regulatory proceedings have been initiated to bring any national measures necessary to comply with the Guidelines in force in the jurisdiction concerned.

Notes

Article 16(3) of the EBA's Regulations requires national competent authorities to inform us whether they comply or intend to comply with each Guideline or recommendation we issue. If a competent authority does not comply or does not intend to comply it must inform us of the reasons. We decide on a case by case basis whether to publish reasons.

The EBA endeavour to ensure the accuracy of this document, however, the information is provided by the competent authorities and, as such, the EBA cannot accept responsibility for its contents or any reliance placed on it.

For further information on the current position of any competent authority, please contact that competent authority. Contact details can be obtained from the EBA's website www.eba.europa.eu.