2019 G20 Osaka Summit Interim Compliance Report

Prepared by
Sofia Lopez and the G20 Research Group
University of Toronto
Toronto
and
Irina Popova and the Center for International Institutions Research
Russian Presidential Academy of National Economy and Public Administration,
Moscow

From 30 June 2019 to 10 May 2020

14 October 2020

"The University of Toronto … produced a detailed analysis to the extent of which each G20 country has met its commitments since the last summit … I think this is important; we come to these summits, we make these commitments, we say we are going to do these things and it is important that there is an organisation that checks up on who has done what."

— *David Cameron, Prime Minister, United Kingdom, at the 2012 Los Cabos Summit*

Munk School of Global Affairs
Trinity College at the University of Toronto
1 Devonshire Place, Room 209N
Toronto, Ontario M5S 3K7
Canada
www.g20.utoronto.ca

G20 RESEARCH GROUP
@G20rg

Centre for International Institutions Research at
the Russian Presidential Academy of National
Economy and Public Administration
11 Prechistenskaya nabarezhnaya
Moscow, Russia 119034
www.ranepa.ru/eng/ciir

Contents

8. Crime and Corruption: Cyber Resilience

"We also continue to step up efforts to enhance cyber resilience."

G20 Osaka Leaders' Declaration

Assessment

	No Compliance	Partial Compliance	Full Compliance
Argentina		0	
Australia		0	
Brazil			+1
Canada	−1		
China		0	
France		0	
Germany			+1
India		0	
Indonesia			+1
Italy	−1		
Japan			+1
Korea		0	
Mexico			+1
Russia			+1
Saudi Arabia			+1
South Africa		0	
Turkey			+1
United Kingdom			+1
United States	−1		
European Union			+1
Average	+0.35 (68%)		

Background

The G20 has been dealing with issues relating to crime and corruption since the 2009 Pittsburgh Summit when members committed to cope with tax heavens, money laundering, corruption, terrorist financing and prudential standards.[1253] At the next summit in Toronto in 2010, the G20 committed to fully implement the United Nations Convention against Corruption (UNCAC).[1254] The same year the G20 Anti-Corruption Working Group (ACWG) was established.[1255] In 2010 in Seoul, the G20 endorsed the G20 Anti-Corruption Action Plan aimed at ratification and implementation of the UNCAC, fight against international bribery, money laundering prevention and the detection of transfers of proceeds of crime.[1256]

[1253] G20 Leaders' Statement: The Pittsburgh Summit. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2009pittsburgh/G20%20Leaders%20Statement.pdf
[1254] The G20 Toronto Summit Declaration. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2010toronto/g20_declaration_en.pdf
[1255] The G20 Toronto Summit Declaration. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2010toronto/g20_declaration_en.pdf
[1256] Annex III. The G20 Anti-Corruption Action Plan. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2010%20Korea/g20seoul-consensus.pdf

In 2012, the G20 approved the G20 principles for denying entry of corrupt officials, presented by the ACWG.[1257] At Los Cabos, G20 leaders also reiterated the necessity to implement the G20 Anti-Corruption Action Plan and UNCAC.[1258]

In 2013 at St. Petersburg, the G20 approved the High-Level Principles on Mutual Legal Assistance, the Guiding Principles on Enforcement of the Foreign Bribery Offence and the Guiding Principles to combat Solicitation.[1259] In 2014 at Brisbane, these principles were supplemented by the G20 High Level Principles on Beneficial Ownership Transparency.[1260]

In 2015 at Antalya three documents dealing with crime and corruption were approved by the G20: the G20 High-Level Principles on Integrity and Transparency in the Private Sector, G20 Anti-Corruption Open Data Principles and the G20 Principles for Promoting Integrity in Public Procurement.[1261] The following year, at the Hangzhou Summit in 2016, the G20 endorsed the G20 High Level Principles on Cooperation on Persons Sought for Corruption and Asset Recovery.[1262]

At Hamburg in 2017, G20 members agreed on four sets of High Level Principles. These four includes the High Level Principles on Organizing Against Corruption, the High Level Principles on the Liability of Legal Persons for Corruption, the High Level on Countering Corruption in Customs, and the High Level Principles on Combatting Corruption Related to Illegal Trade in Wildlife and Wildlife Products.[1263]

At Buenos Aires in 2018, G20 leaders agreed on the new Action Plan 2019–2021 and endorsed the Principles on Preventing Corruption and Ensuring Integrity in State-Owned Enterprises and on Preventing and Managing Conflicts of Interest in the Public Sector.[1264] In addition, the leaders committed to further explore "the links between corruption and other economic crimes and ways to tackle them, including through cooperation on the return of persons sought for such offences and stolen assets, consistent with international obligations and domestic legal systems."[1265]

In 2019 at Osaka, G20 leaders addressed cyber resilience for the first time in terms of the fight against corruption. They pledged to "step up efforts to enhance cyber resilience" following work by the Financial Stability Board (FSB) on the implications of decentralized financial technologies.[1266]

[1257] G20 Los Cabos Leaders' Declaration. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2012loscabos/G20%20Leaders%20Declaration%20-%20Los%20Cabos%2018-19%20June%202012.pdf

[1258] G20 Los Cabos Leaders' Declaration. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2012loscabos/G20%20Leaders%20Declaration%20-%20Los%20Cabos%2018-19%20June%202012.pdf

[1259] G20 St. Petersburg Leaders' Declaration. Access date: 22 December 2019. http://en.g20russia.ru/load/782795034

[1260] G20 Leaders' Communique Brisbane Summit. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2014brisbane/G20%20Leaders%E2%80%99%20Communiqu%C3%A9%20Brisbane%20Summit,%2015-16%20November%202014.pdf

[1261] G20 Leaders' Communique Antalya Summit. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2015Antalya/000111117.pdf

[1262] G20 Leaders' Communique Hangzhou Summit. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2016Hangzhou/G20%20Leaders%E2%80%99%20Communique%20Hangzhou%20Summit.pdf

[1263] G20 Leaders' Hamburg Summit Declaration. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2017hamburg/G20%20Hamburg%20leaders_%20communiqu%C3%A9.pdf

[1264] G20 Leaders' Buenos Aires Summit Declaration. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2018buenosaires/buenos_aires_leaders_declaration.pdf

[1265] G20 Leaders' Buenos Aires Summit Declaration. Access date: 22 December 2019. https://www.ranepa.ru/images/media/g20/2018buenosaires/buenos_aires_leaders_declaration.pdf

[1266] G20 Osaka Leaders' Declaration. Access date: 22 December 2019. https://www.ranepa.ru/images/News_ciir/Project/G20_new_downloadings/FINAL_G20_Osaka_Leaders_Declaration.pdf

Commitment Features

The main concept under this commitment is "cyber resilience." In the Osaka Declaration the G20 leaders do not give a clear definition of this term. A comprehensive guide on notions relating to the cyber resilience (including the term "cyber resilience" itself) was developed by the FSB in 2018 following the request from the G20 Finance Ministers and Central Bank Governors.[1267] Thus, the term "cyber resilience" refers to: "The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents."[1268]

The related concept of "cyber threats" refers to "a circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security."[1269]

The definition of "cyber incidents" means "a cyber event that: i. jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not."[1270] Thus, a "cyber event" implies "any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring."[1271] Another notion mentioned here is the "information system" that is a "set of applications, services, information technology assets or other information-handling components, which includes the operating environment."[1272]

"Vulnerability" implies "a weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats."[1273]

Finally, the term "asset" in this context refers to "something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation."[1274]

The G20 refers to the work done by the FSB on implications of the possible implications of decentralized financial technologies in the commitment's text as well as the recommendation presented by the Financial Action Task Force (FATF). However, the FATF recommendations on money laundering and terrorist financing prevention does not refer to "cyber resilience" under the FSB's definition.

The FSB noted that widening use of decentralized financial technologies could affect financial stability. It specified three dimensions affected by these technologies: risk taking, decision making and record keeping. It said:

[1267] Cyber Lexicon, Financial Stability Board, 18 November 2018. Access date: 08 April 2020. https://www.fsb.org/wp-content/uploads/P121118-1.pdf
[1268] Cyber Lexicon, Financial Stability Board, 18 November 2018. Access date: 08 April 2020. https://www.fsb.org/wp-content/uploads/P121118-1.pdf
[1269] Cyber Lexicon, Financial Stability Board, 18 November 2018. Access date: 08 April 2020. https://www.fsb.org/wp-content/uploads/P121118-1.pdf
[1270] Cyber Lexicon, Financial Stability Board, 18 November 2018. Access date: 08 April 2020. https://www.fsb.org/wp-content/uploads/P121118-1.pdf
[1271] Cyber Lexicon, Financial Stability Board, 18 November 2018. Access date: 08 April 2020. https://www.fsb.org/wp-content/uploads/P121118-1.pdf
[1272] Cyber Lexicon, Financial Stability Board, 18 November 2018. Access date: 08 April 2020. https://www.fsb.org/wp-content/uploads/P121118-1.pdf
[1273] Cyber Lexicon, Financial Stability Board, 18 November 2018. Access date: 08 April 2020. https://www.fsb.org/wp-content/uploads/P121118-1.pdf
[1274] Cyber Lexicon, Financial Stability Board, 18 November 2018. Access date: 08 April 2020. https://www.fsb.org/wp-content/uploads/P121118-1.pdf

There are a number of different types of decentralization in financial services. These vary in the degree to which they affect different segments of financial services, but generally take three broad forms:

- Decentralisation of decision-making. This involves a move away from a single trusted financial intermediary or infrastructure towards systems in which a broad set of users is able to make decisions about whether and how to undertake financial transactions.

- Decentralisation of risk-taking. This involves the shift away from the retention of risk (e.g., credit and liquidity risk) on the balance sheets of individual traditional financial intermediaries towards more direct matching of individual users and providers of financial services.

- Decentralisation of record-keeping. This involves a move away from centrally held data and records, towards systems in which the ability to store and access data is extended across broader consortia of users. Verification of such data and records may also be more distributed, for example via consensus mechanisms.[1275]

These forms of decentralization could raise new risks to financial stability:

- New forms of concentration risks may arise in what might appear to be decentralised systems. In addition to using similar technology, many activities in larger DLT [digital ledger technology] systems (e.g., ownership of the assets, control over source code, operation of the infrastructure, crypto-assets mining and code development) remain concentrated in a relatively small set of persons (e.g., software developers) or entities.

- Greater procyclicality could emerge, particularly in the supply of credit. For example, peer-to-peer (P2P) matching platforms may exhibit larger and sharper swings in their provision of credit than existing financial institutions. This may apply particularly where lending decisions are automated and/or rely on novel data or models whose performance remains untested in a downturn.

- Diffused or unclear responsibility and accountability may arise where the allocation of liability in a more decentralised financial system may be unclear. Such legal risk may be particularly problematic in systems that are permissionless or where participants remain anonymous, and around liabilities arising from smart contracts.

- Recovery and resolution challenges may arise, particularly where current approaches to the recovery and resolution of financial institutions are reliant on centralised recordkeeping and claims on market participants whose identity and location is known.[1276]

The FSB also identifies three areas for further assessment:

- Financial regulation and regulatory approaches: for example, by considering the appropriateness, applicability and effectiveness of current financial regulations for financial businesses and activities based on decentralised financial technologies, and exploring ways to address potential regulatory gaps and financial stability concerns. Some jurisdictions may consider new ways of administering or enforcing regulation. This might include embedding restrictions in computer code, the implications of which have yet to be explored under legal theory.

[1275] Decentralised financial technologies: Report on financial stability, regulatory and governance implications, Financial Stability Board, 6 June 2019. Access Date: 22 December 2019. https://www.fsb.org/wp-content/uploads/P060619.pdf
[1276] Decentralised financial technologies: Report on financial stability, regulatory and governance implications, Financial Stability Board, 6 June 2019. Access Date: 22 December 2019. https://www.fsb.org/wp-content/uploads/P060619.pdf

- Financial supervision: for example, by assessing how decentralised financial technologies could lead to gaps or overlaps in supervisory systems, and updating or modifying data reporting processes accordingly (such as with respect to supervising activities on distributed ledgers). New data could also provide supervisors with greater and timelier insights into potential systemic risks, through the real-time tracking of asset ownership and shifting of associated risks. That said, acquiring and analysing such data may prove to be resource intensive for both market participants and regulators.

- The proportional and consistent application of regulation of decentralised financial technologies: for example, by continuing to regulate decentralised financial technologies in a manner proportional to the risks they pose. In places, the application of decentralised financial technologies may present challenges to the technology-neutral approach to regulation taken by some authorities.[1277]

Thus, to achieve full compliance with the commitment on cyber resilience in financial matters, a G20 member should take actions in all three areas mentioned above.

Scoring Guidelines

−1	G20 member takes no action to improve cyber resilience in finance in any of three areas: financial regulation and regulatory approaches; financial supervision; or the application of regulation of decentralized financial technologies.
0	G20 member take actions to improve cyber resilience in finance in ONE or TWO of three areas: financial regulation and regulatory approaches; financial supervision; or the application of regulation of decentralized financial technologies.
+1	G20 member take actions in ALL three areas to improve cyber resilience in finance: financial regulation and regulatory approaches; financial supervision; and the application of regulation of decentralized financial technologies.

Centre for International Institutions Research

Argentina: 0

Argentina has partially complied with the commitment to enhance cyber resilience.

On 9 January 2020, Argentina's Central Bank released the instruction to fintech start-ups. Specifically, it instructed these startups to place their users' money in traditional banks so it may be under constant supervision by the corresponding supervising body. This regulation has a three-pronged purpose. First, it wants to protect users by supervising that startups don't mishandle a person's funds. Second, it mitigates tax evasions. And third, it ensures a level playing field between banking institutions and fintechs.[1278]

Argentina has taken only one action to improve ciber resilience in finance.

Therefore it receives a score of 0.

Analyst: Irina Popova

Australia: 0

Australia has partially complied with the commitment to enhance cyber resilience.

[1277] Decentralised financial technologies: Report on financial stability, regulatory and governance implications, Financial Stability Board, 6 June 2019. Access Date: 22 December 2019. https://www.fsb.org/wp-content/uploads/P060619.pdf
[1278] Argentina's government is honing in on fintechs, Contxto 21 January 2020. Access date: 20 May 2020. https://www.contxto.com/en/argentina/argentina-government-honing-fintechs/

On 25 November 2019, the Minister for Home Affairs Peter Dutton announced the creation of the 2020 Cyber Security Strategy Industry Advisory Panel. The Panel was to provide strategic advice on the development of the 2020 Strategy to replace the 2016 Cyber Security Strategy.[1279]

On 18 December 2019, the Australian Securities and Investments Commission issued a report Cyber resilience of firms in Australia's financial markets: 2018–19. The report provided an overview of the Commission's cyber resilience capabilities. According to the report "The cyber resilience of firms operating in Australia's markets has improved" since the publication of the previous edition, "with all firms recognising cyber risk as a strategic, organisation-wide issue that is attracting increasing investment." The report's purpose was also to identify new and emerging trends and challenges.[1280]

During the monitoring period Australia took action in one area of cyber resilience in finance — financial supervision.

Thus, it is awarded a score of 0 for partial compliance.

Analyst: Andrei Sakharov

Brazil: +1

Brazil has fully complied with the commitment to enhance cyber resilience.

On 5 December 2019, the Central Bank of Brazil (BCB) put public regulation proposals for open banking in the country under public consultation. The circular and resolution proposals intend to define, among other aspects, the minimum scope of participating institutions and data and services covered by open banking, as well as the requirements for sharing, responsibilities, the convention between the participants and the implementation schedule. Open banking consists of the standardized sharing of data and services by opening and integrating information systems platforms and infrastructures, using a dedicated interface for this purpose, by financial institutions and other institutions authorized to operate by the BCB.[1281]

On 3 January 2020, the Laboratory of Financial and Technological Innovations (Lift), developed by the Central Bank, announced launch of 17 new projects for innovation in the National Financial System (SFN). The 2019 edition selected 20 proposals and 17 completed the prototype development cycle. The resulting projects include blockchain technologies, artificial intelligence, payment models and new application models for technologies already established in the market.[1282]

On 5 February 2020, the BCB announced its BC# Agenda which combines activities in three major areas: instant payment, open banking and fintech. One of the focuses of the BC# Agenda is the adaptation of the SFN and the Brazilian Payment System to the modern technologies currently present in the sector. Innovation, interoperability and immediacy are the watchwords in the actions of the platform, which deals with the development and implementation of new and disruptive

[1279] Industry Panel meets to drive 2020 Cyber Security Strategy forward, Ministry of Home Affairs (Canberra) 25 November 2019. Access Date: 17 May 2019. https://minister.homeaffairs.gov.au/peterdutton/Pages/Industry-Panel-meets-to-drive-2020-Cyber-Security-Strategy-forward.aspx.
[1280] 19-362MR ASIC reports on cyber resilience assessments of financial markets firms, Australian Securities and Investments Commission (Canberra) 18 December 2019. Access Date: 17 May 2019. https://asic.gov.au/about-asic/news-centre/find-a-media-release/2019-releases/19-362mr-asic-reports-on-cyber-resilience-assessments-of-financial-markets-firms/.
[1281] BC põe em consulta pública regras para funcionamento do Open Banking, Central Bank of Brazil (Brasilia) 5 December 2019. Access date: 20 May 2020. https://www.bcb.gov.br/detalhenoticia/392/noticia
[1282] LIFT leva à criação de 17 novos projetos para inovação no SFN, Central Bank of Brazil (Brasilia) 3 January 2020. Access date: 20 May 2020. https://www.bcb.gov.br/detalhenoticia/401/noticia

systems. The technological infrastructures necessary for the operationalization of the systems are being developed. The issue has also been debated with market and consumer representatives. The launch of the first phase of three phases is scheduled for next November.[1283]

On 5 February 2020, the National Cybersecurity Strategy (E-Cyber) was approved by Decree 10.222. The idea of developing E-Cyber was born from the need for the country to modify, with the greatest possible urgency, the current Brazilian Cybersecurity scenario, characterized by the following aspects: increasing cyber threats; increasing rates of cybercrime, good cybersecurity initiatives, however fragmented, lack of macro-political and strategic alignment in cybersecurity actions; and low maturity of the society in cybersecurity. One of the goals of the strategy is the reduction of financial losses for citizens and national institutions, by increasing the culture in cybersecurity.[1284]

On 11 February 2020, the BCB participated in the world-wide Safe Internet Day and implemented public information campaign for the citizens to raise their awareness about risks in digital finance.[1285]

On 2 March 2020, the BC created a working group to propose open banking governance in Brazil. With the implementation of open banking, the entire financial market will operate based on a standardized technological model that will allow universal communication and data sharing between institutions. It will increase competition and expand the offer of financial products and services.[1286]

On 5 March 2020, testing of PIX's technological infrastructures, Brazil's instant payment system, started. Participating institutions are already testing the functionality of the addressing base, an infrastructure that will allow payment to be made in a more practical way, with the BCB. Communication between participants will take place in a secure environment using digital certificates for encryption and authentication. The National Financial System Network, which will be used to transmit payment orders, guarantees an adequate level of isolation to the most critical elements of the system.[1287]

Brazil has taken actions for improvement of cyber resilience in finance in all three priority areas.

Therefore it receives a score of +1.

Analyst: Irina Popova

Canada: −1

Canada has not complied with the commitment to enhance cyber resilience.

No government action in any of the three areas of cyber resilience in finance has been registered during the monitoring period.

[1283] Agenda BC# reforça ações de inovação no Sistema Financeiro Nacional, Central Bank of Brazil (Brasilia) 5 February 2020. Access date: 20 May 2020. https://www.bcb.gov.br/detalhenoticia/409/noticia
[1284] Estratégia Nacional de Segurança Cibernética / E-Ciber, Departamento de Segurança da Informação Gabinete De Segurança Institucional Da Presidência Da República (Brasilia) 11 February 2020. Access date: 20 May 2020. http://dsic.planalto.gov.br/noticias/estrategia-nacional-de-seguranca-cibernetica-e-ciber
[1285] Dia da Internet Segura: confira dicas para se proteger de frauds, Central Bank of Brazil (Brasilia) 5 February 2020. Access date: 20 May 2020. https://www.bcb.gov.br/detalhenoticia/412/noticia
[1286] Banco Central cria Grupo de Trabalho para propor governança do Open Banking no Brasil, Central Bank of Brazil (Brasilia) 2 March 2020. Access date: 20 May 2020. https://www.bcb.gov.br/detalhenoticia/415/noticia
[1287] BC testa infraestrutura tecnológica do PIX, Central Bank of Brazil (Brasilia) 5 March 2020. Access date: 20 May 2020. https://www.bcb.gov.br/detalhenoticia/419/noticia

Thus, Canada is awarded a score of −1.[1288]

Analyst: Andrei Sakharov

China: 0

China has partially complied with the commitment to enhance cyber resilience.

On 26 October 2019, China approved its first national law on encryption. The regulation came into force on the 1 January 2020. It broadens the current regulatory scope of encryption, liberalizes commercial encryption at national-law level and proposes a market-oriented regulatory regime for the commercial encryption industry.[1289]

On 19-20 December 2019, the 16th China International Finance Forum was held in Shanghai. The participants discussed urgent topics, including financial security risk prevention. The event was co-hosted by the main China's financial regulation authorities, major banks and local municipalities.[1290]

On 23 February 2020, the People's Bank of China issued the financial distributed ledger technology security specification (JR/T 0184-2020). New regulation specifies the security system of the mentioned technology including basic hardware and software, cryptographic algorithms, etc.[1291]

China is taking steps towards consistent application of regulation of decentralized financial technologies, but no actions aimed at improvement of financial regulation and financial supervision have been found.

Thus, China receives a score of 0.

Analyst: Alexander Ignatov

France: 0

France has partially complied with the commitment to enhance cyber resilience.

On 26 December 2019, the French Financial Markets Authority published new regulations concerning the licensing of digital assets providers. Licensed providers are required to have professional indemnity insurance or a minimum amount of reserve funds, at least one effective senior manager, resilient information technology systems, an internal control system, a claims handling procedure, an organization enabling it to avoid conflicts of interests and procedures to prevent money laundering and terrorist financing.[1292]

[1288] The website of the Canadian government as well as open sources were searched.
[1289] China Cybersecurity and Data Protection: China publishes first law on encryption, Lexology (London) 12 November 2019. Access date: 24 March 2020. https://www.lexology.com/library/detail.aspx?g=53282dfc-c7f6-4cef-8de6-8f180fed8b31
[1290] The 16th China International Finance Forum. Access date: 24 March 2020. http://www.ciff.org.cn/eng/
[1291] Financial distributed ledger technology security specification, China legislation standard (Beijing) 23 February 2020. Access date: 24 March 2020. http://www.cnstandards.net/index.php/financial-distributed-ledger-technology-security-specification/
[1292] Crypto Firms Can Now Apply for a License in France, Yahoo Finance 26 December 2019. Access date: 03 April 2020. https://finance.yahoo.com/news/crypto-firms-now-apply-license-170000940.html

On 14 November 2019, the French government signed a three-year cybersecurity pact with eight major national companies to step up security arrangements amid growing number of cybersecurity attacks.[1293]

France is taking steps towards consistent application of regulation of decentralized financial technologies and improvement of financial supervision, but no actions aimed at improvement of financial regulation have been found.

Thus, France receives a score of 0.

Analyst: Alexander Ignatov

Germany: +1

Germany has fully complied with the commitment to enhance cyber resilience.

On 11 September 2019, German federal ministry of finance and German Bundesbank launched TIBER-DE, a new programme that will strengthen the resilience of the entire financial system to cyber attacks. The TIBER-DE framework was developed together with the Federal Financial Supervisory Authority (BaFin) and the Federal Office for Information Security. Banks, insurance companies, financial market infrastructures and their most important service providers can use TIBER-DE to test their resilience against cyber attacks. Under the coordination of the Bundesbank, businesses interested in testing their systems hire ethical hackers to try to breach their security mechanisms and penetrate their information systems. These businesses can then close the vulnerabilities in their security systems and take preventive measures against actual hacking.[1294]

In March 2020, BaFin identified four overarching priority areas for its work in 2020, including digitalization, information technology (IT) risk and cyber risk. BaFin will particularly focus on the growing use of artificial intelligence, distributed ledger technology and crypto-assets based on these technologies. In the area of big data and artificial intelligence, BaFin will define the framework for action for supervised entities on the basis of five initiatives within the context of principle-based supervision. The objective is to provide greater legal certainty for the use of technologies involved in big data and artificial intelligence. In addition, BaFin's Insurance Supervision Sector will examine whether supervised undertakings are implementing Insurance Supervisory Requirements for IT.[1295]

Germany has taken actions for improvement of cyber resilience in finance in all three priority areas.

Thus, it receives a score of +1.

Analyst: Andrey Shelepov

India: 0

India has partially complied with the commitment to enhance cyber resilience.

[1293] French government forms cybersecurity pact with major French companies, Reuters 14 November 2019. Access date: 03 April 2020. https://www.reuters.com/article/us-france-cyber/french-government-forms-cybersecurity-pact-with-major-french-companies-idUSKBN1XO1HZ

[1294] TIBER-DE enhances the security of the German financial system, German Federal Ministry of Finance 11 September 2019. Access Date: 3 April 2020. https://www.bundesfinanzministerium.de/Content/EN/Pressemitteilungen/2019/2019-11-09-joint-release-with-bundesbank.html.

[1295] Supervisory priorities for 2020, Geramn Federal Financial Supervisory Authority March 2020. Access Date: 3 April 2020. https://www.bafin.de/SharedDocs/Downloads/EN/Broschuere/dl_Aufsichtsschwerpunkte2020_en.pdf?__blob=publicationFile&v=3.

On 2 September 2019, Steering Committee on Fintech related issues constituted by the Ministry of Finance, Department of Economic Affairs submitted its Final Report to Union Finance and Corporate Affairs Minister Nirmala Sitharaman. The report outlines the current landscape in the fintech space globally and in India, studies the various issues relating to its development and makes recommendations focusing on how fintech can be leveraged to enhance financial inclusion of micro, small and medium sized enterprises with a view to making fintech-related regulations more flexible and generate enhanced entrepreneurship. The committee report also identifies application areas and use cases in governance and financial services and suggests regulatory upgrades enabling fintech innovations. Given the rapid pace at which technology is being adopted primarily by private sector financial services, the committee recommends the Department of Financial Services work with public sector banks to bring in more efficiency to their work and reduce fraud and security risks. Significant opportunities can be explored to increase the levels of automation using artificial intelligence, cognitive analytics and machine learning in their back-end processes. The committee also recommends a comprehensive legal framework for consumer protection be put in place early keeping in mind the rise of fintech and digital services.[1296]

India is taking steps towards improvement of financial regulation and regulatory approaches, but no actions in other two key spheres indicated by the Financial Stability Board have been detected withing the monitoring period.

Thus, India receives a score of 0.

Analyst: Irina Popova

Indonesia: +1

Indonesia has fully complied with the commitment to enhance cyber resilience.

On 30 September 2019, Indonesia's Financial Services Authority (OJK) issued Regulation No. 23/POJK.01/2019 (POJK 23/2019), which amends several provisions of OJK Regulation No. 12/POJK.01/2017 on Implementation of Anti-Money Laundering and Prevention of Terrorism Funding in Financial Sector Programs. One change introduced by POJK 23/2019 is to allow banks to engage third party service providers to conduct their face-to-face on-boarding verification, whereas previously, banks could only use their own electronic facilities for face-to-face verification.[1297]

In October 2019, the Indonesian government issued Government Regulation No. 71 of 2019 on the Management of Electronic Systems and Transactions, which clarifies the distinction between public and private electronic system operators, which affects the applicability of Indonesia's data localization requirements. These regulations are generally applicable to data protection, and not specific to the financial services sector.[1298]

In October 2019, Bank Indonesia (BI) issued a regulation and circular letters allowing private companies to operate electronic trading platforms for money market and foreign exchange

[1296] Steering Committee on Fintech related issues submits its Final Report to Finance Minister, Press Information Bureau of Indian Government (Delhi) 2 September 2019. Access date: 19 May 2020. https://pib.gov.in/PressReleasePage.aspx?PRID=1583866

[1297] Digitalisation Trends in Indonesia's Financial Services Sector — Recent and Upcoming Developments 07 February 2020. Access date: 28 March 2020. https://www.mondaq.com/Finance-and-Banking/891136/Digitalisation-Trends-In-Indonesia39s-Financial-Services-Sector-Recent-And-Upcoming-Developments

[1298] Digitalisation Trends in Indonesia's Financial Services Sector — Recent and Upcoming Developments 07 February 2020. Access date: 28 March 2020. https://www.mondaq.com/Finance-and-Banking/891136/Digitalisation-Trends-In-Indonesia39s-Financial-Services-Sector-Recent-And-Upcoming-Developments

transactions in Indonesia. The maximum foreign ownership for these entities is 49%, and the single presence policy also applies to this sector. We have seen increasing interest in this space since then.[1299]

On 29 November 2019, BI issued a blueprint titled Bank Indonesia: Menavigasi Sistem Pembayaran Nasional di Era Digital (Bank Indonesia: Navigating the National Payment System in the Digital Era) as a follow-up to Indonesia's 2025 Payment System Visions (introduced in May 2019). The five initiatives will be implemented in parallel by five working groups under BI. Through the 2025 visions, BI intends to:[1300]

- Support the integration of national digital economy and finance;
- Support banking digitalization;
- Guarantee the interlink between fintech and banking;
- Ensure there is a balance between innovation, consumer protection and healthy business competition;
- Safeguard national interests in cross-border digital economy and finance.

The blueprint covers five initiatives to achieve the 2025 visions: (i) open banking, (ii) retail payment system, (iii) market infrastructure, (iv) data and (v) regulatory, licensing and supervision.

The introduction of Payment System Directive 2 in the European Union created opportunities for technology companies (including fintech players), and that will likely be the case in Indonesia too, once open banking is fully implemented.

Indonesia has taken actions for improvement of cyber resilience in finance in all three priority areas.

Thus, it receives a score of +1.

Analyst: Pavel Doronin

Italy: −1

Italy has not complied with the commitment to enhance cyber resilience.

No government actions in any of the three areas of cyber resilience in finance has been registered during the monitoring period.

Thus, Italy is awarded a score of −1.

Analyst: Andrei Sakharov

Japan: +1

Japan has fully complied with the commitment to enhance cyber resilience.

[1299] Digitalisation Trends in Indonesia's Financial Services Sector — Recent and Upcoming Developments 07 February 2020. Access date: 28 March 2020. https://www.mondaq.com/Finance-and-Banking/891136/Digitalisation-Trends-In-Indonesia39s-Financial-Services-Sector-Recent-And-Upcoming-Developments

[1300] Bank Indonesia Issues Blueprint for 2025 Payment System 29 November 2019. Access date: 28 March 2020. https://www.bakermckenzie.com/en/insight/publications/2019/11/bank-indonesia-2025-payment-system

On 18 July 2019, it was reported Japan's Financial Services Agency was considering 110 registration applications from crypto trading platforms, as part of the country's efforts to further strengthen crypto legislation to protect cryptocurrency investors and further integrate the crypto sector with traditional finance.[1301]

On 6 September 2019, Japan's Financial Services Agency held the second roundtable on supervisory oversight of crypto assets, which brought together relevant financial supervisors and international organizations, providing a useful opportunity to share experiences and discuss recent developments concerning crypto assets, including (1) recent technological developments and challenges with crypto-assets; (2) regulation and supervision of crypto-asset trading platforms; (3) investor protection and market integrity; and (4) international cooperation with multi-stakeholders involvement.[1302]

On 30 September 2019, Japan's Financial Services Agency issued draft guidelines for funds investing in crypto assets; the guidelines refer to the worrying investments as "non-specific assets" and advise funds to exercise caution when investing in assets outside the original objective of the trust and to evaluate potential risks, such as those relating to volatility and liquidity.[1303]

On 3-11 October 2019, Japan's Financial Services Agency held fourth financial sector industry-wide cybersecurity exercise Delta Wall, in which 120 financial sector entities took part (large, medium and small players); the scenarios of the exercises were designed with expert knowledge and examples of actual cyber attacks to allow participants to raise their awareness for weaknesses that they tend to fall into.[1304]

On 28 October 2019, Japan's Financial Services Agency published a report reflecting the current state and common issues of cybersecurity across the financial sector; the report notes that "with the progress of digitalization, the environment surrounding the financial sector is undergoing rapid changes, with financial institutions revamping their business models, non-financial players referred to as "platformers" entering the sector," Japan's Financial Services Agency "will take steps to find out about how digitalization is progressing at financial institutions, taking into account the sizes and characteristics of financial institutions … and will also be active in gathering information from various entities, including non-financial players, and proactively encourage the financial sector to take whatever steps are necessary to ensure cyber security."[1305]

On 4 December 2019, it was reported Japan's Financial Services Agency approved the remaining crypto exchange that was in business prior to the regulation of the crypto industry; exchanges in this category were allowed to continue operations while their registration applications were being reviewed; in total 21 crypto exchanges have been approved to operate in the country.[1306]

[1301] Japan's FSA considering over 100 new exchange applications, BNC 18 July 2019. Access date: 23 March 2020. https://bravenewcoin.com/insights/japans-fsa-considering-over-100-new-exchange-applications

[1302] The second Roundtable on Supervisory Oversight of Crypto-Assets –Toward a new Stage of International Cooperation, Japan's FSA 9 September 2019. Access date: 23 March 2020. https://www.fsa.go.jp/en/news/2019/201909/20190909.html

[1303] Japan's Financial Regulator Issues Draft Guidelines for Funds Investing in Crypto, Coindesk 3 October 2019. Access date: 23 March 2020. https://www.coindesk.com/japans-financial-regulator-issues-draft-guidelines-for-funds-investing-in-crypto

[1304] Financial Industry-wide Cybersecurity Exercise (Delta Wall IV), Japan's FSA 28 October 2019. Access date: 23 March 2020. https://www.fsa.go.jp/en/news/2019/20191028-4.html

[1305] Publication of a report on cybersecurity across the financial sector, Japan's FSA 28 October 2019. Access date: 23 March 2020. https://www.fsa.go.jp/en/news/2019/20191028-5.html

[1306] Japan Now Has 21 Approved Crypto Exchanges, Bitcoin.com 4 December 2019. Access date: 23 March 2020. https://news.bitcoin.com/japan-now-has-21-approved-crypto-exchanges/

On 24 December 2019, Bank of Japan released the summary of the main findings of the Report of the Study Group on Legal Issues regarding Central Bank Digital Currency (CBDC); the Report discusses what legal issues would arise within the Japanese legal framework if the Bank of Japan were to issue its own CBDC; whether or not CBDC can be regarded as legal tender; what would happen in the case of counterfeit or duplication under current private law; whether or not issuance of CBDC is consistent with the purposes of the Bank as currently specified by the Bank of Japan Act; whether the Bank can restrict the use of CBDC by certain individuals; the legal issues related to the acquisition of information with respect to Anti-Money Laundering and Counter-Terrorism Financing regulations; protecting personal information; and the penalties for counterfeiting/duplicating CBDC as Crimes of Counterfeiting of Currency under current criminal law.[1307]

On 24 December 2019, Japan's Financial Services Agency announced its plans to organize the "Blockchain Global Governance Conference" on 9-10 March 2020 (though it was later postponed due to the COVID-19 pandemic) to deepen the understanding of issues regarding the financial system based on decentralized financial technologies.[1308]

On 13 January 2020, it was reported Japan's Financial Services Agency had plans to impose the new rule in a revision to the Financial Instruments and Exchange Act to reduce the risk to cryptocurrency margin traders by cutting the permitted leverage to two times the deposit due to the crypto markets volatility.[1309]

On 10 March 2020, within the framework of the postponed "Blockchain Global Governance Conference," Japan's Financial Services Agency "BG2C — Special Online Broadcasting Panel Discussion"; the session announced the launch of "Blockchain Governance Initiative Network" (BGIN) aiming to (1) create an open, global and neutral platform for multi-stakeholder dialogue, (2) develop a common language and understandings among stakeholders with diverse perspectives, and (3) build academic anchors through continuous provision of trustable documents and codes based on an open source-style approach; Japan's Financial Services Agency stressed BGIN was formed under the guidelines set by Japan at the G20 on governance and regulatory frameworks for decentralized finance[1310].

Japan has taken significant efforts in all considered areas for enhancement of cyber resilience, including financial regulation and regulatory approaches; financial supervision; and the application of regulation of decentralized financial technologies.

Thus, Japan is awarded a score of +1.

Analyst: Pavel Doronin

Korea: 0

Korea has partially complied with the commitment to enhance cyber resilience.

[1307] Summary of the Report of the Study Group on Legal Issues regarding Central Bank Digital Currency, Bank of Japan 24 December 2019. Access date: 23 March 2020. https://www.boj.or.jp/en/research/wps_rev/lab/lab19e03.htm/

[1308] Financial Services Agency Japan: Blockchain Global Governance Conference [BG2C], Mondovsione 24 December 2019. Access date: 23 March 2020. https://mondovisione.com/media-and-resources/news/financial-services-agency-japan-blockchain-global-governance-conference-bg2c/

[1309] Japan's Financial Watchdog to Set Low Leverage Cap for Crypto Margin Traders: Report, Coindesk 13 January 2020. Access date: 23 March 2020. https://www.coindesk.com/japans-financial-watchdog-to-set-low-leverage-cap-for-crypto-margin-traders-report

[1310] Launch of a new global network for blockchain "Blockchain Governance Initiative Network" [BGIN], Japan's FSA 10 March 2020. Access date: 23 March 2020. https://www.fsa.go.jp/en/news/2020/20200310.html

On 20 January 2020, the government announced its intention to impose a 20 per cent tax on cryptocurrencies. The ordering to review taxation plan had been given to the Ministry of Economy and Finance.[1311]

On 11 May 2020, the Financial Services Commission launched the financial data exchange platform. The platform is said to establish a safe and secure marketplace for the distribution of financial big data. It will also foster new data-driven business opportunities for fintech start-ups and promote data convergence and utilization with non-financial data, which will lead to the development of new types of innovative services.[1312]

On 13 May 2020, the Financial Services Commission presented the development plan of MyData licensing program. By law, MyData business operators are required to have a minimum capital of KRW500million and adequate telecommunications facilities for safe data processing, while satisfying the major shareholder and feasibility of business plan requirements. MyData program aims at improvement of the productivity and competitiveness of the financial industry.[1313]

On 18 May 2020, the Financial Services Commission unveiled the 5th Plan for Financial Hub Policy for 2020–2022. he specific strategies include pursuing regulatory reforms to promote private sector-driven innovation, building infrastructure to continue innovative growth in the financial industry and adopting a "selection and concentration" approach to build global capacity with a particular attention paid to the markets in the Association of South East Asian Nations. Among the main pillars of the policy, the key factors are the development of the digital financial technologies and promotion of anti-money laundering framework.[1314]

Korea is taking steps towards improvement of financial regulation and regulatory approaches, but no actions in other two key spheres indicated by the Financial Stability Board have been detected withing the monitoring period.

Thus, Korea receives a score of 0.

Analyst: Alexander Ignatov

Mexico: +1

Mexico has fully complied with the commitment to enhance cyber resilience.

On 29 October 2019, Global Financial Innovation Network welcomed Mexican National Banking and Securities Commission as a member of the group. This network is made up of 50 authorities and international organizations committed to facilitating financial innovation, through a global regulatory sandbox in which coordination mechanisms are established for companies that want to test novel products, services or models in the respective sandboxes of the countries.[1315]

[1311] S. Korea considering imposing 20% tax on cryptocurrencies, the Korea Herald (Seoul) 20 January 2020. Access date: 18 May 2020. http://www.koreaherald.com/view.php?ud=20200120000204&np=61&mp=7

[1312] Financial Data Exchange Platform Launched, Financial Services Commission (Seoul) 11 May 2020. Access date: 18 Mau 2020. http://meng.fsc.go.kr/common/pdfjs/web/viewer.html?file=/upload/press1/20200511171544_32e3c243.pdf

[1313] FSC Announces Plans for MyData Businesses, Financial Services Commission (Seoul) 13 May 2020. Access date: 13 May 2020. http://meng.fsc.go.kr/common/pdfjs/web/viewer.html?file=/upload/press1/20200513154540_13b5d14f.pdf

[1314] FSC Unveils 5th Plan for Financial Hub Policy, Financial Services Commission (Seoul) 18 May 2020. Access date: 18 May 2020. http://meng.fsc.go.kr/common/pdfjs/web/viewer.html?file=/upload/press1/20200518111610_58dffdf1.pdf

[1315] 68/2019 La CNBV se suma a la Red Global de Innovación Financiera (GFIN), Mexican Government (Mexico City) 29 October 2019. Access date: 20 May 2020. https://www.gob.mx/cnbv/prensa/68-2019-la-cnbv-se-suma-a-la-red-global-de-innovacion-financiera-gfin

On 2 December 2019, the National Banking and Stock Commission made the Register of Novel Models available to the public. This temporary authorization space, known as the Regulatory Sandbox internationally, can be seen as an experimentation space, which allows companies to offer financial services to a limited number of clients, using innovative technological tools or means, in order to test them before offer them to the general public in bulk. The authorities obtain better tools to accommodate, in the regulatory framework they issue, the New Models that have the potential to generate benefits for users of financial services, the financial entities themselves or the financial system in your set.[1316]

On 17 December 2019, the Secretary of the Treasury and Public Credit, Arturo Herrera Gutiérrez, together with the Ambassador of the United Kingdom in Mexico, Corin Robertson, launched Officially, the Financial Services Program of the Prosperity Fund, which includes a contribution of GBP9.5 million by the United Kingdom government, which will be invested in cooperation for the development of the financial sector in Mexico. The objective of the Financial Services Program of the Prosperity Fund is to promote inclusive economic growth and development, through a modern financial system, on which three main lines of work have been proposed:

1. Improve the financial education of beneficiaries of some social programs;

2. Support the implementation and development of secondary regulation of the Financial Technology Institutions Law, based on international best practices,

3. Promote the adoption and use of digital financial services among the population and micro, small and medium-sized enterprises.[1317]

On 11 March 2020, Mexico adopted the National Policy for Financial Inclusion. It is a public policy tool that will pay for social mobility, economic growth and with it the well-being of the population. The main objectives of the Policy are:

- To facilitate access to financial products and services for people and micro, small and medium-sized enterprises.

- Increase digital payments among the population, businesses, companies and the three levels of government.

- Strengthen infrastructure to facilitate access and provision of financial products and services and reduce information asymmetries.

- Increase the economic-financial skills of the population.

- Strengthen access to information tools and financial protection mechanisms.

- Promote the financial inclusion of people in vulnerable situations, such as women, migrants, older adults, indigenous people and the rural population.[1318]

[1316] Registro de Modelos Novedosos), Mexican Government (Mexico City) 2 December 2019. Access date: 20 May 2020. https://www.gob.mx/cnbv/acciones-y-programas/registro-modelos-novedosos

[1317] Comunicado No. 104 La SHCP y la Embajada Británica en México presentan el Programa de Servicios Financieros del Fondo de Prosperidad, Mexican Government (Mexico City) 17 December 2019. Access date: 20 May 2020. https://www.gob.mx/shcp/prensa/comunicado-no-104-la-shcp-y-la-embajada-britanica-en-mexico-presentan-el-programa-de-servicios-financieros-del-fondo-de-prosperidad

Mexico has taken actions for improvement of cyber resilience in finance in all three priority areas.

Thus, it receives a score of +1.

Analyst: Irina Popova

Russia: +1

Russia has fully complied with the commitment on cyber resilience in finance.

On 16 September 2019, Bank of Russia adopted the Guidelines for the Advancement of Information Security in the Financial Sector for 2019-2021, which define priorities in the area for the near future. These include the creation of risk profiles for financial institutions and the transition to risk-based supervision; the introduction of requirements for the resilience and smooth operation of financial institutions in case of cyber risks materialization; the requirements for data management security and the prevention of data leaks from financial institutions; and the development of the cyber culture of the financial market.[1319]

Russia has taken actions for improvement of cyber resilience in finance in all three priority areas.

Thus, it receives a score of +1.

Analyst: Andrey Shelepov

Saudi Arabia: +1

Saudi Arabia has fully complied with the commitment on improvement of cyber resilience in finance.

On 10 November 2019, in a joint effort between the National Cybersecurity Authority (NCA) and the E-Commerce Council, NCA has issued two cybersecurity guidelines documents for sellers and consumers of e-commerce.[1320]

On 8 December 2019, NCA launched the Cybersecurity Toolkit, containing cyber security policies, standards and documents that can be used by various authorities as a reference for cybersecurity policies and standards with the objective to enhance the capabilities and readiness of national entities in cybersecurity.[1321]

On 30 January 2020, the Saudi Arabian Monetary Authority (SAMA) announces the launching of licenses for non-bank financial institutions (financial technology institutions), by announcing the issuance of the first license for an electronic wallet company and the first license for a payment services company in Saudi Arabia. The announcement comes as part of SAMA's efforts to achieve the objectives of the financial sector development program, which is one of the pillars of Vision 2030, in enabling financial institutions to support private sector growth by opening financial services

[1318] Comunicado No. 019 CONAIF y CEF presentan la Política Nacional de Inclusión Financiera (PNIF), Mexican Government (Mexico City) 11 March 2019. Access date: 20 May 2020. https://www.gob.mx/shcp/prensa/comunicado-no-019-conaif-y-cef-presentan-la-politica-nacional-de-inclusion-financiera-pnif

[1319] Guidelines for the Advancement of Information Security in the Financial Sector for 2019-2021, Bank of Russia 16 September 2019. Access Date: 15 May 2020. http://old.cbr.ru/Content/Document/File/103460/onrib_2021_e.pdf.

[1320] NCA Issues E-Commerce Guidelines in Conjunction with the E-Commerce Council, National Cybersecurity Authority of Saudi Arabia 10 November 209. Access date: 20 August 2020. https://nca.gov.sa/en/pages/news/news22.html

[1321] Cybersecurity tools, National Cybersecurity Authority of Saudi Arabia 8 December 2020. Access date: 20 August 2020. https://nca.gov.sa/pages/kit.html

to non-banking actors (payment services providers and financial technologies), supporting development of the national economy.[1322]

On 4 February 2020, the NCA launched a Global Cybersecurity Forum in Riyadh. It discussed five themes: cybersecurity industry, international cyber collaboration, cyber culture, cyber disruption, and cyber threats and resilience.[1323] It was stated that five memorandum's of understanding (MOUs) would be signed between the NCA and international organizations to strengthen international cybersecurity cooperation.

On 19 February 2020 NCA launched a public consultation on the Cloud Computing Cybersecurity Controls Draft Document to fulfill its rule in organizing and protecting the kingdom's cyberspace and engaging the stakeholders and the public in order to produce efficient policies and legislation.[1324]

On 25 February 2020, SAMA released additional licensing guidelines and criteria for digital-only banks operating in Saudi Arabia. Guidelines for digital-only banks include that applicants for licenses must be set up as a locally incorporated joint-stock company and maintain a physical presence in Saudi Arabia.[1325]

On 29 May 2019, the NCA introduced the Critical Systems Cybersecurity Controls. (CSCC -1 :2018) after conducting a comprehensive study of multiple national and international cybersecurity frameworks and standards.[1326]

Saudi Arabia has taken actions for improvement of cyber resilience in finance in all three priority areas.

Thus, Saudi Arabia receives a score of +1.

Analyst: Alexander Ignatov

South Africa: 0

South Africa has partially complied with the commitment on cyber resilience in finance.

On 17 April 2020, the Crypto Assets Regulatory Working Group consisting of several major financial institutions of South Africa including the South African Reserve Bank presented the Position Paper on Crypto Assets. The position paper provides specific recommendations for the development of a

[1322] SAMA Announces the Launching of Licenses for Non-Bank Financial Institutions, Saudi Arabian Monetary Authority (Riyadh) 30 January 2020. Access date: 30 March 2020. http://www.sama.gov.sa/en-US/News/Pages/news-399.aspx
[1323] Saudi Arabia's National Cybersecurity Authority Launches Today the Global Cybersecurity Forum in Riyadh, the Middle East Larges to Date Cybersecurity Event, Global Cyber Security Forum, Saudi Arabia National Cybersecurity Authority, 4 February 2020. Access Date: 24 September 2020. https://nca.gov.sa/en/pages/news/news27.html.
[1324] NCA Asks for the Public's Feedback Regarding the Cloud Computing Controls Draft Document, National Cybersecurity Authority of Saudi Arabia 19 February 2020. Access date: 20 August 2020. https://nca.gov.sa/en/pages/news/news32.html
[1325] Saudi central bank issues additional licensing guidelines for digital-only banksб Salaam Gateway 25 February 2020. Access date: 15 May 2020. https://www.salaamgateway.com/story/saudi-central-bank-issues-additional-licensing-guidelines-for-digital-only-banks
[1326] Cybersecurity controls for sensitive systems, National Cybersecurity Authority of Saudi Arabia 29 May 2020. Access date: 20 August 2020. https://nca.gov.sa/pages/cscc.html

regulatory framework for crypto assets, including suggestions on the required regulatory changes to be implemented.[1327]

South Africa is taking steps towards improvement of financial regulation, but no actions aimed at consistent application of regulation of decentralized financial technologies and improvement of financial supervision were detected.

Thus, South Africa receives a score of 0.

Analyst: Alexander Ignatov

Turkey: +1

Turkey has fully complied with the commitment on cyber resilience in finance.

On 14 November 2019, Turkey announced it would be fully complying with the European Union's revised Payment Services Directive (PSD2) starting from 1 January 2020.[1328] The PSD2 focuses on supporting innovation and competition in retail payments and enhances the security of payment transactions and protection of consumer data. The PSD2 is supplemented by regulatory technical standards on strong customer authentication and common and secure open standards of communication, as well as guidelines on incident reporting and guidelines on security measures for operational and security risks. The three documents were developed by the European Banking Authority in close cooperation with the European Central Bank and payment service providers must comply with all of them.

On 1 January 2020, the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institution entered into force and introduced major changes to the regulation and supervision of payment services and open banking service providers, such as:[1329]

- Within the scope of the law, the Payment and E-Money Institutions Association of Turkey is established. Simultaneously, payment and e-money institutions will be subject to independent audit;
- In accordance with the law, open banking products of payment initiation service providers and account information service providers are defined as payment services and be included in the scope of payment services. Payment service providers will be entitled to provide these services as well. The Central Bank of the Republic of Turkey (CBRT) is authorized to supervise these services;
- Open banking and payment services providers are required to apply to the CBRT to obtain the authorization for these services within one year of the entry into force of the law;
- Furthermore, depending on the limits to set forth by the CBRT, the marketplaces may need to establish their payment service provider subsidiaries or outsource the payment services to third party service providers;

[1327] IFWG Position Paper on Crypto Assets, South African Reserve Bank (Pretoria) 17 April 2020. Access date: 15 May 2020. https://www.resbank.co.za/Lists/News%20and%20Publications/Attachments/9867/IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf

[1328] Turkey paves the way for Open Banking 14 November 2019. Access date: 21 March 2020. https://www.finextra.com/newsarticle/34764/turkey-paves-the-way-for-open-banking

[1329] Turkey: Turkish PSD2: Open Banking Reform, Enacted! Marketplaces May Need Payment Services License 02 December 2019. Access date: 21 March 2020. https://www.mondaq.com/turkey/Finance-and-Banking/870432/Turkish-PSD2-Open-Banking-Reform-Enacted-Marketplaces-May-Need-Payment-Services-License

- The law brings major changes to the regulation and supervision of payment service providers and e-money issuers. The CBRT is authorized to regulate and supervise these institutions in lieu of the Banking Regulatory and Supervisory Authority (BRSA). The CBRT will also be entitled to supervise the third parties providing services to these institutions;

- Within the scope of the prevailing legislation, the services, which are not currently defined as payment services, are included in the category of payment services if they reach the limits to be set by CBRT;

- Pursuant to the law, if transactions used with closed loop payment instruments reach certain limits, they may become subject to the Payment Services and Electronic Money Law.

The law is the second and the most important step in terms of regulating open banking in Turkey. The BRSA had taken the first step by introducing the Draft Information Technology Systems Regulation to public review in 2018.

On 4 January 2020, it was reported that the Capital Markets Board, Turkey's financial regulatory and supervisory agency, is planning to develop guidelines to foster the adoption of blockchain technology responding to the increasing interest and usage of cryptocurrencies in the country.[1330]

On 15 March 2020, the BRSA published new Regulation on Information Systems of Banks and Electronic Banking Services, which enter into force on 1 July 2020. According to the regulation, banks' boards of directors are liable for conducting effective supervision to manage any risks arising from the use of information systems. The regulation sets out that the board of directors must approve and establish a strategic plan, establish a strategy committee and a guidance committee related to information systems.

The regulation sets forth the standards regarding the following points to control the information systems:[1331]

- Establishment of authentication mechanisms;

- Establishment of track record mechanism for transactions related to information systems;

- Establishment of network security control systems;

- Security configuration management;

- Security vulnerability management;

- Cyber-attack management and cyber information sharing;

- Creation of an information security awareness training program.

Turkey has taken actions for improvement of cyber resilience in finance in all three priority areas.

[1330] Kripto paralara SPK denetimi 04 January 2020. Access date: 23 March 2020. https://www.hurriyet.com.tr/ekonomi/kripto-paralara-spk-denetimi-41412081

[1331] Turkey: New Regulation On Bank IT Systems And Electronic Banking Services 30 March 2020. Access date: 30 March 2020. https://www.mondaq.com/turkey/Finance-and-Banking/907164/New-Regulation-On-Bank-IT-Systems-And-Electronic-Banking-Services

Thus, it receives a score of +1.

Analyst: Pavel Doronin

United Kingdom: +1

The United Kingdom has fully complied with the commitment on cyber resilience in finance.

On 3 July 2019, the Financial Conduct Authority (FCA) proposed rules to address harm to retail consumers from the sale of derivatives and exchange traded notes (ETNs) referencing certain types of cryptoassets. The FCA considered these products as ill-suited to retail consumers who cannot reliably assess the value and risks of crypto-derivatives, including due to the prevalence of market abuse and financial crime, such as cyber theft, in the secondary market for cryptoassets. Therefore the FCA proposed banning the sale, marketing and distribution to all retail consumers of all derivatives and ETNs that reference unregulated transferable cryptoassets by firms acting in, or from, the UK.[1332]

On 27 September 2019, the Bank of England published the findings of the financial sector cyber simulation exercise that took place on 9 November 2018. The exercise, commissioned by the Cross Market Operational Resilience Group jointly chaired by the bank and UK Finance, explored the sector's resilience to a major cyber incident impacting the UK. The exercise demonstrated that recommendations from the last sector exercise have been implemented and identified further opportunities for improvement.[1333]

In February 2020, the National Cyber Security Centre opened the Northern Ireland Cyber Security Centre. The new Centre will provide a centralised communications role for cyber security in Northern Ireland, and will help deliver the Cyber Security: A Strategic Framework for Action and the UK Cyber Security Strategy focusing on several major areas including finance.[1334]

The UK has taken actions for improvement of cyber resilience in finance.

Thus, it receives a score of +1.

Analyst: Andrey Shelepov

United States: −1

United States has not complied with the commitment to enhance cyber resilience.

On 12 December 2019, the Presidential National Infrastructure Advisory Council (NIAC) released a communication in response to the National Security Council's call, outlining risks and recommendations for the United States cyber security, including in the matters of finance. The NIAC recommended a two-track approach: to pursue solutions that address urgent, near-term cyber risks that have national security implications and that can be implemented rapidly using existing authorities

[1332] FCA proposes ban on sale of crypto-derivatives to retail consumers, UK Financial Conduct Authority 3 July 2019. Access Date: 3 April 2020. https://www.fca.org.uk/news/press-releases/fca-proposes-ban-sale-crypto-derivatives-retail-consumers.
[1333] Bank of England sector resilience exercise, Bank of England 27 September 2019. Access Date: 3 April 2020. https://www.bankofengland.co.uk/news/2019/september/boe-sector-resilience-exercise.
[1334] NCSC supports Northern Ireland's push to strengthen cyber security capabilities, UK National Cyber Security Centre 18 February 2020. Access Date: 3 April 2020. https://www.ncsc.gov.uk/news/northern-ireland-cyber-security-centre.

and design the ideal model for an assured measure of protection informed by an executive-driven public-private partnership.[1335]

However, no other government actions in any of the three areas of cyber resilience in finance has been registered during the monitoring period.

Thus, the United States is awarded a score of −1.

Analyst: Andrei Sakharov

European Union: +1

The European Union has fully complied with the commitment on enhancing cyber resilience in finance.

On 2 October 2019, the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (FISMA) and Deloitte co-hosted the event: "How can technology driven transparency fuel the Capital Markets Union?." Head of Sector Digital Building Blocks at European Commission's Directorate-General for Informatics Joao Rodrigues Frade introduced the European Financial Transparency Gateway pilot run by DG FISMA. The pilot experimented with blockchain technology to provide European citizens and investors with easier access to financial information on companies across the EU. He also presented the European Blockchain Services Infrastructure (EBSI) project, which will deliver a Europe-wide blockchain infrastructure offering numerous applications for public administrations in EU member states. The Commission is delivering EBSI in close collaboration with the member states through the European Blockchain Partnership, established in 2018 through the Connecting Europe Facility.[1336]

In December 2019, the European Commission started an open market consultation in preparation of the European Blockchain Pre-Commercial Procurement that is looking for novel, improved blockchain solutions for the future evolution of the European Blockchain Service Infrastructure. Interested market parties are invited to participate in the open market consultation activities.[1337]

In December 2019, 30 Recommendations on Regulation, Innovation and Finance were released by European Commission's Expert Group on Regulatory Obstacles to Financial Innovation. They cover all segments of the financial sector, all types of novel technologies, a wide range of business cases currently observed and all types of market players. They also span important policy areas, including the prevention of money laundering and terrorist financing, consumer protection, data sharing and use, and governance and operational resilience within the financial sector. Thus, our work has an extremely broad scope. The report explains that it is relevant to consider changes to the general regulatory framework (across multiple industry sectors), as well as the framework for the regulation of the financial services sector, which may require tailored responses in order to be able to realise the

[1335] Transforming the US Cyber Threat Partnership, Cybersecurity and Infrastructure Security Agency (Washington) 12 December 2019. Access Date: 17 May 2019. https://www.cisa.gov/sites/default/files/publications/NIAC-Transforming-US-Cyber-Threat-PartnershipReport-FINAL-508.pdf.

[1336] EU Blockchain Initiatives supporting financial transparency, European Commission (Brussels) 2 October 2019. Access date: 19 May 2020. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/10/09/EU+Blockchain+Initiatives+supporting+financial+transparency

[1337] Blockchain Technologies, European Commission (Brussels). Access date: 19 May 2020. https://ec.europa.eu/digital-single-market/en/blockchain-technologies

potential of specific opportunities and to take account of specific regulatory concerns in an already highly regulated environment.[1338]

On 2 December 2019, the Council of the EU adopted a first fundamental review of the functioning of the European system of financial supervision. The texts adopted review tasks, powers, governance, so as to adapt the authorities to the changed context in which they operate. The reform also includes provisions reinforcing the role of the EBA as regards risks posed to the financial sector by money laundering activities.[1339]

On 19 December 2019, European Commission launched a consultation process on the topic "Financial services — improving resilience against cyberattacks (new rules)." Through this consultation, the Commission services aim to gather stakeholders' views on the need for legislative improvements within the financial services acquis with a view to harmonise rules across the EU in a proportionate way to make the financial sector more secure and resilient while alleviating compliance and administrative burdens.[1340]

The EU has taken actions for improvement of cyber resilience in finance in all three priority areas.

Thus, it receives a score of +1.

Analyst: Irina Popova

[1338] Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG): 30 Recommendations on Regulation, Innovation and Finance, European Commission (Brussels) December 2019. Access date: 19 May 2020. https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf

[1339] Financial supervision: Council adopts a review of the supervisory framework for financial institutions, Council of the European Union (Brussels) 2 December 2019. Access date: 19 May 2020. https://www.consilium.europa.eu/en/press/press-releases/2019/12/02/financial-supervision-council-adopts-a-review-of-the-supervisory-framework-for-financial-institutions/

[1340] Financial services — improving resilience against cyberattacks (new rules), European Commission (Brussels) 19 December 2019. Access date: 19 May 2020. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation