European Securities and
Markets Authority

Annual peer review of EU CCP supervision

2021 Peer Review on CCPs' Business Continuity in Remote Access Mode

4 July 2022 | ESMA91-372-2064

Table of Contents

Acronyms used

CCP	Central Counterparty
EMIR	Regulation (EU) 648/2012 of the European Parliament and Council on OTC derivatives, central counterparties and trade repositories
ESMA	The European Securities and Markets Authority
NCA	National Competent Authority
RTS	Regulatory Technical Standards
RTS 153/2013	Commission Delegated Regulation (EU) No 153/2013 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on requirements for central counterparties

1 Executive Summary

Reasons for publication

In accordance with EMIR, the European Securities and Markets Authority (ESMA) shall, at least annually, conduct a peer review analysis of the supervisory activities of all competent authorities in relation to the authorisation and the supervision of CCPs.

Contents

This peer review assesses the overall functioning of CCP colleges and provides an in-depth analysis of supervisory activities of National Competent Authorities (NCAs) of CCPs with respect to requirements set out in EMIR related to CCPs' business continuity. This peer review is based on a specific methodology developed for mandatory peer reviews under EMIR. The review was conducted by the Peer Review Committee established by the CCP Supervisory Committee (CCPSC).

The peer review findings are based on information gained by ESMA staff through participation in CCP colleges, the responses by the NCAs to a predefined questionnaire, including, where relevant, tailored follow-up questions, and the findings from on-site visits at selected NCAs. The questionnaire and the findings of the peer review were discussed and agreed by the CCP Supervisory Committee of ESMA. Accordingly, this report provides an overview of the approaches followed by NCAs and presents ESMA's assessment of the degree of convergence reached by NCAs.

The review of the functioning of the colleges during the reporting period remains overall positive. Chairing NCAs continue to manage CCP colleges in compliance with EMIR requirements. However, CCP colleges continue following the trend, already noted in past peer reviews, of performing merely as fora for regular updates and exchange of information, where college members largely rely on chairing authorities' reporting and ESMA reviews.

Regarding the supervision of business continuity in remote access mode, the overall outcome of the peer review is that the NCAs participating in the current peer review have broadly met the supervisory expectations. The peer review showed that some aspects of business continuity in remote access mode were not always specifically assessed. In most cases, this is explained by the fact that at many CCPs remote working was already common practice or part of existing business continuity arrangements. In this context, remote working did not introduce any new major risks to be re-assessed. The following observations were noted:

a. NCAs could better clarify, when defining their risk-based approach, how operational risks related to remote access are addressed.

b. From a supervisory perspective, CCPs could better clarify the risk-based scope of penetration testing and how risks related to remote access are addressed as part of this.

c. BCM plans could in this context be improved by taking into account other extreme scenarios, where remote working arrangements could serve to ensure business continuity.

Moreover, the report highlights ten best practices that emerged from the NCAs' responses (see Box 1 below). Implementing these best practices would also address the three observations mentioned above. The table below provides an overview of the current level of implementation of these best practices, based on the information received during the peer review.

Best practices	Implementation frequency
1 Set up competence center	7
2 Apply proactive approach	5
3 Dedicated meetings	5
4 Request daily crisis updates	8
5 Use international cyber resilience guidance	11
6 Request penetration testing	6
7 Request awareness training	8
8 Request (more) extreme, relevant stress scenarios	5
9 Participate in BCP tests	2
10 Assess user-friendliness BCP	3

The maximum implementation frequency amounts to 11, equalling the total number of Member States with a CCP, as where a Member State had designated several NCAs under EMIR, the authorities from this Member State coordinated a single response and are counted as one.

Finally, while the new EU legislative proposal for Digital Operational Resilience Act (DORA) is going to establish a new regulatory framework applying also to CCPs, it could be considered whether there remain areas for improvement within the EMIR framework, in order to strengthen the enforcement of EMIR requirements with respect to business continuity (not addressed by DORA). This could be addressed via a review of the relevant RTS under EMIR.

Next Steps

ESMA will follow up on the findings listed in this report in order to identify, where relevant, the most appropriate tools to further enhance supervisory convergence with respect to the considerations included in this report. NCAs are expected to consider implementing the best practices.

Box 1: Best Practices

Best practice 1: NCAs could ensure that CCP supervisors are adequately supported by IT and cyber risk experts when reviewing the CCPs' IT and cyber resilience, in order to exploit best practices and continuously update knowledge across sectorial supervision, especially with regard to cyber risk management approaches. This could be achieved by establishing a "competence centre" shared by supervision across different sectors under the NCA supervisory mandate (FMIs, Financial firm, Banks…).

Best practice 2: NCAs could adopt a more 'pro-active' supervision of CCPs' operational and IT/cyber risk, relying less on the CCPs' reporting updates and taking control of the information provided by CCPs by issuing ad hoc requests for information and, where suggested by a risk-based approach, initiating desk-based reviews or on-site inspections.

Best practice 3: NCAs could have regular meetings with CCPs with a specific focus on operational resilience. The frequency of such meetings should be at least quarterly, while the need for more frequent meetings would be risk-based. Attendance of such meetings should involve operational experts from both NCAs' and CCPs' side. To be well prepared for such meetings, the NCAs could send scoping questions and/or request from the CCPs to receive well in advance of the meeting any relevant input, such as reporting on identified operational risks (risk self-assessment), risk controls in place, relevant policies and procedures. In preparation or as follow-up to such meetings, NCAs could perform desk-based reviews with specific focus on the CCPs' operational resilience.

Best practice 4: During extreme situations (e.g. a pandemic outbreak, increased cyber-attacks, unavailability of internet services or extensive power supply outages), NCAs could reinforce their regular supervision by increasing the frequency of interactions with the CCPs' management and operational staff. NCAs could request daily updates on operational availability, incidents and threats.

Best practice 5: Until the new regulation on Digital Operational Resilience for the financial sector (DORA) enters into force, NCAs could consider existing guidelines and expectations consistent with the CPMI-IOSCO guidance on cyber resilience, such as the Cyber Resilience Oversight Expectations (CROE), the CIS18 Controls (Center for Internet Security - Critical Security Controls) and, to the extend applicable to CCPs, the EBA Guidelines on ICT and security risk management and relevant guidelines by (inter)national Cyber Security Centres.

Best practice 6: NCAs could request CCPs to test their cyber security and cyber resilience by performing regular penetration tests, and to consider changing over time the external service providers supporting them with the penetration testing, as this contributes to gaining new insights on cyber security. The frequency of such tests should be risk-based reflecting the CCPs' risk profile and complexity. The TIBER framework could be used as a best practice for an extensive threat intelligence-based red teaming test.

Best practice 7: NCAs could request CCPs to perform regular awareness campaigns, covering the (security) risks related to remote working, in order to reduce employee vulnerability.

Best practice 8: Besides the regular review of BCM policies and tests, NCAs could also request CCPs to take specific extreme scenarios into account during their annual review of BCM policies, including e.g. a pandemic outbreak, increased cyber-attacks, unavailability of internet services or extensive power supply outages. The formulation of extreme scenarios should be risk-based, as they are very dependent on each CCP's specific critical processes and (cyber) threats. Testing of (extreme) scenarios should be done at least annually, but it should also be possible to perform ad hoc tests if material risks are foreseen.

Best practice 9: NCAs could participate as an observer in (some of) the CCPs' BCM tests. This could provide the NCAs with a better understanding of the CCPs' decision-making capability, good practices and points for improvement.

Best practice 10: When reviewing the CCPs' business continuity plans and crisis management plans, NCAs could also consider the 'user friendliness' of such plans as an important element of their effectiveness. In extreme situations it could prove to be vital for new employees or temporary external employees to be able to easily and clearly find in the plan what to do during a crisis. A very comprehensive but difficult-to-use BCM plan is typically less user friendly or effective.

2 Introduction

1. Article 24a(7)(a) of Regulation EU No 648/2012 (EMIR) requires ESMA to conduct at least annually a peer review analysis of the supervisory activities of all competent authorities in relation to the authorisation and the supervision of CCPs in accordance with Article 30 of Regulation (EU) No 195/2010 (ESMA Regulation).

2. The ESMA Board of Supervisors approved the methodology for mandatory peer reviews in relation to CCPs' authorisation and supervision under EMIR (the methodology),[1] whereby the review is conducted by the CCP Supervisory Committee (CCPSC) through delegation to a Peer Review Committee (PRC) composed of the Chair and the two independent members of the CCPSC. Each peer review will assess the overall functioning of CCP colleges and provide an in-depth analysis of a specific topic, to be determined within the scope set by EMIR.

3. In March 2021, the ESMA Board of Supervisors agreed with the CCPSC proposal to change the topic that was initially proposed for the 2021 CCP peer review into "business continuity in remote access mode", covering also the relevant cybersecurity aspects.

4. In May 2021, the ESMA Board of Supervisors approved the mandate for the 2021 CCP peer review, as developed by the PRC and validated by the CCPSC.

5. In accordance with its mandate, this peer review aimed to assess the effectiveness of supervisory practices put in place by competent authorities to assess CCP compliance with the provisions of Article 26 of EMIR on general provisions on organisational requirements and Article 34 of EMIR on business continuity and the related Articles of RTS 153/2013 (i.e. Article 4 on risk management and internal control mechanisms, Article 9 on Information Technology (IT) systems, and Articles 17-23 on business continuity). The review also assessed whether competent authorities in doing so are complying with the relevant provisions of the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) and the CPMI-ISCO guidance on cyber resilience.

6. The peer review covered the relevant National Competent Authorities (NCAs) of CCPs authorised under EMIR as of 1 July 2021. On this date, 13 CCPs were authorised under EMIR in the EU. The Peer Review thus was intended to cover the NCAs of the 11 Member States where the above mentioned 13 CCPs are established, namely: DE, EL, ES, FR, IT, HU, NL, AT, PL, PT, SE.

7. The peer review considered the NCAs' supervisory activities conducted from January 2020 to June 2021 (the reporting period), with respect to the assessment of a CCP's compliance with the requirements in Articles 26 and 34 of EMIR and related RTS, in connection with: a) the monitoring of the CCP activities under remote working arrangements activated during the Covid-19 pandemic, and b) the yearly review (performed during this period) of the CCP's compliance with the requirements in the scope of the current peer review, pursuant to Article 21 of EMIR.

8. While the overall functioning of CCP colleges has been assessed on the basis of ESMA staff's experience in the participation in CCP colleges, in line with the methodology, the PRC also developed a self-assessment questionnaire (the questionnaire – see Annex

[1] See ESMA70-151-3061 Methodology for mandatory peer reviews in relation to CCPs

1). This provided the PRC with detailed information on each NCA’s supervisory activities, practices and approaches related to the assessment of CCPs’ business continuity.

9. On 25 June 2021, the covered NCAs were invited to answer the questionnaire by 15 September 2021. Where a Member State had assigned several NCAs under Article 22 of EMIR, the authorities from this Member State coordinated a single response to the questionnaire representing the coordinated view of all relevant competent authorities in that Member State.

10. Answers to the questionnaire were generally thorough and provided evidence of the supervisory actions. In a few cases ESMA sent some follow-up questions to NCAs, which were promptly addressed.

11. In February 2022, the PRC conducted three on-site visits to the NCAs supervising Nasdaq Clearing, Eurex Clearing and LCH SA (i.e. respectively, Finansinspektionen, BaFin and the Deutsche Bundesbank,[2] and Banque de France, ACPR and AMF). Given the travelling restrictions due to the pandemic, on-site visits were organised via videoconference.

12. The findings of the peer review are presented in this report, which does not intend to provide an exhaustive representation of all responses submitted by the NCAs, but to provide an overview of the approaches followed by the majority of NCAs. The report is intended to highlight any emerging divergences in an effort to identify potential opportunities for further supervisory convergence, best practices and, where applicable, identify possible cases of non-compliance. Section 3 assesses the overall functioning of CCP colleges. Section 4 presents a general overview of NCAs’ supervisory activities conducted in the reporting period with respect to business continuity and organisational set-up. Section 5 presents the outcome of the peer review of specific supervisory activities on business continuity in remote access mode. Section 6 summarises the conclusions drawn from this peer review.

3 Overall functioning of CCP colleges

13. The review finds that the functioning of the colleges during the reporting period remains overall positive. Important findings are, in particular, that chairing NCAs aim to meet previous best practices and expectations, as well as the new guidelines issued in 2021, and that they updated the colleges on the recent market developments related to the Russian invasion of Ukraine, including the impact on CCPs’ risk management and operations.

14. Overall, chairing NCAs continue to manage CCP colleges in compliance with EMIR:

    a. All colleges adopted a revised written agreement in 2021 in line with the respective new guidelines.[3] The composition of all colleges was also reviewed

[2] BaFin is the sole competent NCA under EMIR for the supervision of the two CCPs established in Germany. On several supervisory topics, including operational and cyber risk resilience, BaFin cooperates with the Deutsche Bundesbank which is together with BaFin the supervisor of the two CCPs under the banking regulatory framework. Although the peer review would strictly cover the supervisory activities of BaFin, the on-site visits included in scope both BaFin and Bundesbank to better understand the supervisory activities conducted under this cooperation

[3] “Guidelines on written agreements between members of CCP colleges under Article 18 of EMIR” published by ESMA on 01 July 2021.

in 2021, which saw UK authorities leaving several CCP colleges at the end of the Brexit transition period. Most chairing authorities have published on their websites the list of the members of the college, in compliance with Article 18(2) of EMIR. ESMA is following up with the chairing authorities that have not yet published that list, so that ESMA can also publish on its website the list of the members of all colleges.

b. Most colleges held at least one meeting in 2021, where the NCAs reported on their annual review under Article 21 in line with the respective new guidelines,[4] as well as the outcome of their supervisory activities and their next supervisory workplan. Given the restrictions adopted in several countries across the Union in relation to the Covid-19 pandemic, college meetings were organised via videoconferences. For two colleges, annual meetings were postponed to Q1 2022, resulting in a delay of more than 24 months from the previous meeting, which is not in line with the college written agreements requesting at least an annual meeting. One NCA has not yet presented its CCP annual review under Article 21 of EMIR.

c. Not all chairing NCAs tested the colleges' communication procedures for emergency situations, through simple reachability and connectivity tests.

15. Concerning the CCPs' initiatives for new services and activities or changes to risk models and parameters, pending the adoption of new RTS under Articles 15 and 49 of EMIR, the chairing NCAs continued applying the framework developed by ESMA for the identification of new services and activities requiring an extension of the authorisation pursuant to Article 15 of EMIR or significant changes for the purpose of Article 49 of EMIR (see ESMA Opinion[5] published on 15 November 2016) and ensured a timely process for adopting the related college opinion.

16. Overall, the level of engagement by college members can be considered satisfactory once an Article 15 or 49 procedure was triggered, although most college members continue to rely on the review by the chairing NCA and the scrutiny by ESMA. In most cases, college opinions took into account conditions and/or recommendations resulting from the review by the CCPSC under Article 23a of EMIR or ESMA validations under Article 49 of EMIR, and in some cases included additional recommendations. Where past authorisations under Article 15 of EMIR or validations under Article 49 of EMIR, and related college opinions and/or CCPSC reviews, included conditions and/or recommendations, in two cases the chairing authority has not yet reported a follow-up to the college.

17. Besides the context of college opinions, colleges continue following the trend, already noted in past peer review, of performing merely as fora for regular updates and exchange of information, where college members largely rely on chairing authorities' reporting and ESMA reviews.

[4] "Guidelines on common procedures and methodologies on supervisory review and evaluation process of CCPs under Article 21 of EMIR" published by ESMA on 24 February 2021.

[5] See https://www.esma.europa.eu/sites/default/files/library/2016-1574_-_opinion_on_significant_changes_for_ccps.pdf.

4 General overview of NCAs' activities in relation to business continuity in remote access mode

18. EMIR requires NCAs to assess and review the compliance of CCPs with the EMIR requirements, including those in Articles 26 and 34 of EMIR and related RTS under 1) Article 17(4) with respect to authorisations provided under Article 15 and 2) Article 21 with respect to regular reviews under on-going supervision, including at least an annual review. The NCAs were asked to provide responses to a number of questions on their supervisory approach and practices with respect to the above supervisory activities, as well as on their organisational set-up.

19. Overall, NCAs reported that they conducted supervisory activities covering several aspects of CCP operational resilience. Several NCAs closely monitored the unprecedented shift to remote working arrangements throughout the Covid-19 pandemic via continuous reporting and regular meetings. Table 1 provides an overview of the supervisory activities conducted by NCAs.

Table 1: Overview of the NCAs' supervisory activities

	YES	*NO*
Annual review	*10*	*1*
Desk based review	*11*	*0*
On-site inspections/ on-site visits/ audits	*5*	*6*
Ongoing Supervision and monitoring *- Regular calls* *- Regular (daily, weekly, bi-weekly and monthly) reports* *- reports to Risk Committee, Audit Committee, Supervisory Board*	*9*	*2*

Yes/No reflects the number of NCAs that conducted the various activities

Annual review under EMIR Article 21

20. Most NCAs reported that they included the review of the CCPs' operational resilience in the scope of the annual reviews under Article 21 of EMIR conducted within the reporting period (both in 2020 and/or in 2021).

21. In particular, several NCAs referred to the use of specific supervisory activities on the CCPs' compliance with Articles 26 and 34, as input to the annual review under Article 21.

    a. Three NCAs reported having conducted a desk-based review of the CCP compliance with the same requirements in the context of an extension of authorisation under article 15 of EMIR.

    b. Several NCAs referred to desk-based review of the CCP's IT and cyber risk profile and operational risk management framework, in some cases including aspects relating to outsourcing, business continuity management (e.g. reviews of BCM procedures or tests), preparedness to the pandemic scenarios and remote working arrangements. Some NCAs reported the use of ad hoc reviews of the CCP's cyber resilience against the PFMI and the *related* guidance on cyber resilience or the Eurosystem Cyber Resilience Oversight Expectations

(CROE). Some NCAs also reviewed the CCP performance in the context of the CPMI-IOSCO IMSG Level 3 assessment on cyber resilience and/or in the ECB survey on cyber resilience and/or conducted their own survey on the FMI/CCP operational and cyber resilience. Another NCA reported having reviewed the CCP against the framework developed by the Center for Internet Security (CIS),[6] identifying 20 key controls (known as CIS20) that an organisation should do to defend themselves against cyber-threats.

c. Four NCAs conducted dedicated on-site inspections or visits on IT and cyber risk matters, while another NCA commissioned an IT audit to an external consultant.

Ongoing Supervision and Monitoring

22. Several NCAs reported about the use of regular meetings and on-site visits as tools to discuss operational and cyber resilience topics with CCPs, covering also remote working arrangements, as well as regular reporting on such topics.

23. In particular, at the beginning of the Covid-19 pandemic, all NCAs implemented a daily reporting from CCPs based on a template developed by ESMA and approved by the CCPSC, which included prudential risk indicators as well as business continuity management aspects such as the CCP's implementation of remote working arrangements. Moreover, upon invitation by the CCPSC, all NCAs promoted fire-drills under remote working arrangements to test the ability of the CCPs and involved external stakeholders to deal with default management procedures (including default auctions) under the unprecedent circumstances during the pandemic.

24. In particular, one NCA predominantly relied on monitoring the CCP's reporting updates, without performing during the reporting period a thorough review of the CCP's operational risk under remote working arrangements.

NCAs organisational set-up and resources

25. In total, 14 NCAs in 11 EU Members States have a direct supervisory responsibility to assess the EU CCP's compliance with Articles 26 and 34 of EMIR and related RTS:

- In France, three NCAs have shared responsibilities for the supervision of CCPs (ACPR, AMF and BdF), which jointly assess compliance with EMIR Articles 26 and 34 and related RTS.

- In Italy, two NCAs have shared responsibilities for the supervision of CCPs (BdI, Consob).

- In the Netherlands, the responsibilities regarding the supervision of CCPs are divided between AFM and DNB, whereby DNB is the sole responsible authority for EMIR Articles 26 and 34 and related RTS.

[6] The CIS is a US-based non-profit organization established by hundreds of IT security professionals representing governmental agencies, the military, large corporations, conglomerates, and academic institutions.

- In Germany, BaFin is the sole NCA for the supervision of CCPs. However, due to national legislation (German Banking Act) BaFin works in close cooperation with the Deutsche Bundesbank.

- In Austria, although the FMA is the sole NCA for CCP, the latter has established a close cooperation with the OeNB, in particular in matters of information technology systems and business continuity management.

- In Portugal, CMVM is the sole NCA for the supervision of CCPs. However, following the notification of OMIClear as operator of essential services, in August 2019, under the national law implementing the EU Directive on Network and Information Security (NIS), OMIClear is currently subject to the security and notification requirements set out by the Portuguese National Cybersecurity Centre (CNCS).

26. The number of Full-Time Equivalent (FTE) staff members assigned to the supervision of a CCP (not only to the assessment of compliance with Articles 26 and 34 of EMIR and related RTS) is on average about 3 FTEs per supervised CCP at each NCA, ranging overall between one and six FTEs. These figures are proportional to the importance and the complexity of supervised CCPs.

27. However, one NCA indicated to have no operational risk expertise within the supervisory team, therefore, it commissioned an external auditor to perform an IT audit on the CCP's policies and procedures related to the regulatory compliance of the CCP to the articles 26 and 34 of EMIR. Another NCA postponed planned in-depth analyses regarding cyber and business continuity plans, beyond the focus of this peer review, due to resourcing issues, which are going to be resolved by the introduction of an internal IT risk competence centre.

28. With respect to the supervisory handbook, some NCAs shared internal supervisory guidance on business continuity and on IT and cyber resilience, others pointed to the PFMI and the CPMI-IOSCO guidance on cyber resilience as a guiding supervisory handbook or to the Eurosystem's CROE, whereas others refer to national legislation imposing additional operational and cyber resilience requirements for Financial Market Institutions and Infrastructures, including CCPs.

29. Regarding the supervision of CCPs with a banking licence, it was noted that the requirements applying to credit institutions, which such CCPs are equally subject to, are largely consistent with the requirements under EMIR but also more detailed, which may result more effective in terms of enforcement.

4.1 Main general findings

30. Most NCAs reviewed the CCPs' operational resilience in the scope of the annual reviews under Article 21 of EMIR conducted within the reporting period, and topics related to business continuity and operational and cyber resilience were monitored and discussed in regular supervisory meetings with the CCPs. In some cases, NCAs conducted on-site inspections and specific desk-based reviews, also addressing the specific risks related to the wider use of remote working arrangements during the Covid-19 pandemic.

31. More specifically, for most NCAs, supervisory activities related to the compliance with Articles 26 and 34 of EMIR and related RTS involve supervisory team members (on

average, approximately 1 FTE per CCP), which have sufficient supervisory skills to review e.g. the CCPs' policies and procedures and the respective governance. In several cases, CCP supervisors are supported by IT experts when conducting specific, technical reviews and IT and cyber resilience assessments. Such experts can be external consultants or more commonly staff members with IT expertise from other departments within the NCA's organization or, where cooperation arrangements are in place, from the respective national central bank, acting as an overseer or, with respect to CCPs with banking licence, as a supervisor.

32. The following best practices emerged from the general overview of NCAs' supervisory practices:

    Best practice 1: NCAs could ensure that CCP supervisors are adequately supported by IT and cyber risk experts when reviewing the CCPs' IT and cyber resilience, in order to exploit best practices and continuously update knowledge across sectorial supervision, especially with regard to cyber risk management approaches. This could be achieved by establishing a "competence centre" shared by supervision across different sectors under the NCA supervisory mandate (financial market infrastructures, financial firms, banks…).

    Best practice 2: NCAs could adopt a more 'pro-active' supervision of CCPs' operational and IT/cyber risk, relying less on the CCPs' reporting updates and taking control of the information provided by CCPs by issuing ad hoc requests for information and, where suggested by a risk-based approach, initiating desk-based reviews or on-site inspections.

33. Finally, while the new EU legislative proposal for Digital Operational Resilience Act (DORA) is going to establish a new regulatory framework applying also to CCPs, it could be considered whether there remain areas for improvement within the EMIR framework, in order to strengthen the enforcement of EMIR requirements with respect to business continuity (not addressed by DORA). This could be addressed via a review of the relevant RTS under EMIR.

5 Review of NCAs' supervisory practices on business continuity in remote access mode

34. Article 26 of EMIR and related RTS (namely Article 4 on risk management and internal control mechanisms and Article 9 on Information Technology (IT) systems of RTS 152/2013) set out the general provisions on organisational requirements. Article 34 of EMIR and related RTS (namely Articles 17-23 on business continuity of RTS 152/2013) set out the business continuity requirements.

35. This section reflects the level of details provided by the NCAs in their answers to the targeted set of questions in the peer review questionnaire aimed to determine which supervisory activities are most frequently used to assess business continuity in remote access mode. It presents current practices on how the NCAs ensure compliance of the CCPs' implementation of business continuity in remote access mode with the relevant requirements. It also assesses whether competent authorities' practices are complying with the relevant provisions of the PFMI (in particular, Principle 17 thereof) and the CPMI-IOSCO guidance on cyber resilience.

5.1 Overview of NCAs’ practices

Operational risk management policies and procedures

36. The authorities were invited to describe their supervisory activities in relation to the CCPs’ review of their risk management policies and systems to ensure they satisfy the requirement of Art 4 of RTS 153/2012 and Principle 17 of the PFMI with respect to remote working arrangements.

37. Most NCAs reported that the issues addressed in the questionnaire were covered by their generic risk-based supervisory approach. Some NCAs also provided additional details on specific practices. These are described below.

Table 2: NCAs’ approaches to review of operational risk management policies and procedures

	Generic approach	*Generic approach and/or Specific practices*
Supervisory activities on operational risk management policies and procedures	*8*	*3*
Review of risk management policies and procedures	*3*	*8*
Identification and monitoring of the risks before the Covid-19 pandemic	*11*	*0*
Assessment and monitoring of the risks during the Covid-19 pandemic	*5*	*6*
CCPs’ review and adaptation of risk management policies, procedures, and processes to remote working arrangements	*2*	*9*
NCAs’ review of the CCPs’ remote working arrangements	*9*	*2*
Access to relevant information for the risk management function	*9*	*2*
Access to relevant information for the NCAs	*11*	*0*

38. NCAs have generally addressed the CCPs’ review of operational risk management policies and procedures, including specific risks from remote working, through their regular supervisory activities. These activities generally included a) regular supervisory meetings with CCPs’ management and operational staff, b) the annual review under Article 21 of EMIR (and/or the Supervisory Review and Evaluation Process – SREP due under the banking regulation for CCPs with a banking licence) including against the requirements on IT systems and business continuity, and c) the monitoring of major incidents and changes to the CCPs’ policies and IT systems.

39. NCAs also indicated that remote working was already implemented as a daily practice for most CCPs. Consequently, CCPs did not have to make large changes to their risk management policies and procedures when the pandemic started.

40. Some NCAs employ specialized IT and/or cyber expert teams from within their respective organisations for assessing operational and/or IT risks at the CCPs. This enables them to go into more focused conversations with the CCPs’ operational staff.

Review of risk management policies and procedures

41. Authorities were asked how they supervise the CCPs' risk management policies and procedures (including those for crisis management).

42. Generally, the NCAs indicate that to supervise the CCPs' risk management policies and procedures, they performed regular and ad hoc supervisory meetings with the CCPs' management and staff. Especially during the Covid-19 crisis NCAs had more frequent (in some instances even daily) meetings on the developments and consequences for the CCPs.

43. Furthermore, some NCAs performed specific inspections aimed at operational risk and crisis management related to remote working arrangements. This included on-site and off-site inspections, review of CCPs' answers to relevant questionnaires and surveys. Issues often found were related to the use of staff private devises (Bring Your Own Devise - BYOD risks), security of the remote workspace and sound documentation of crisis management procedures.

44. Three NCAs reviewed the CCPs' answers to questionnaires specifically targeting operational risk in remote working situations. These questionnaires were developed by these NCAs specifically for this cause.

45. Two NCAs noted that while performing a more comprehensive assessment on the CCPs' extension of clearing services, they also assessed the CCPs' risk management policies and procedures.

46. One NCA also reviewed the meeting notes of the CCPs' operational risk committee meetings, while another NCA attended as an observer the CCP's supervisory board meetings during the time of the Covid-19 outbreak.

Identification and monitoring of the risks before the Covid-19 pandemic

47. Authorities were asked how their activities addressed the risks posed by remote working arrangements during a 'business as usual' situation (before the Covid-19 pandemic).

48. The majority of the NCAs indicated that, before the pandemic, they addressed the CCPs' risks by performing their regular supervisory activities on operational risks heavily relying on the CCPs' risk reporting, including change and incident reporting and internal audit reports.

49. Most NCAs indicated that remote working arrangements were already part of CCPs' business continuity plans or business as usual arrangements. The CCPs' control measures mitigating risks related to remote working had already been in place and tested well before the pandemic.

Assessment and monitoring of the risks during the Covid-19 pandemic

50. Authorities were asked how they checked the CCPs' assessment and monitoring of the risks posed by remote working arrangements during the Covid-19 pandemic.

51. Generally, the NCAs supervised the CCPs through their regular supervisory activities, such as monitoring the regular risk reporting by the CCPs. The CCPs were, however,

requested by most NCAs to provide specific risk assessments related to the pandemic and remote working (e.g. related to contingency tests[7] and VPN tests). Also, the NCAs indicated that they had frequent meetings with the CCPs regarding the developments during - and impact due to - the Covid-19 crisis.

52. NCAs also mentioned the ESMA-initiated fire drills regarding default management process under remote working conditions.

53. Two NCAs indicated that their CCPs are also credit institutions and therefore are subject to banking regulation, which is more stringent e.g. when it comes to operational risk scenario requirements.

CCPs' review and adaptation of risk management policies, procedures, and processes to remote working arrangements

54. Authorities were asked how they supervised the CCPs' review and adaptation of their risk management policies, procedures, and processes to company-wide remote working arrangements.

55. The majority of the NCAs have addressed this topic with their regular supervisory activities, such as the annual review under Article 21 of EMIR and analysis of CCPs' major changes to policies and IT systems. NCAs indicated that no major adaptations to the CCPs' risk management policies, procedures and processes were deemed necessary as a consequence of the extended use of remote working arrangements.

56. Two NCAs performed a desk-based review based on the CCPs' answers to a tailored questionnaire and related background documentation. No major issues were identified.

Main points identified by the NCAs' review of the CCPs' remote working arrangements

57. Authorities were asked what the main points identified were following their review of the CCPs' company-wide remote working arrangements.

58. Generally, the NCAs have identified no major issues specific to the CCPs' remote working arrangements, as such arrangements were already in place at the CCPs before the pandemic. The assessments of such arrangements were mainly positive, while a few points for improvement were identified.

59. For instance, one NCA mentioned a CCP's VPN capacity that had to be enhanced. Another NCA mentioned that a CCP implemented a split of teams (e.g. "team A" and "team B") to cope with the pandemic-related risks. The teams altered between working in the office and remotely.

[7] Contingency tests are focussed on long term solution for an unfortunate event

Access to relevant information for the risk management function

60. Authorities were asked how they have checked whether access to all relevant information for the CCPs' risk management function was assured during remote working situations.

61. Generally, the NCAs indicated they have checked this topic with their regular supervisory activities (mostly by monitoring the regular risk reporting updates by the CCPs), while two NCAs performed an on-site visit to check on the CCP's switch to remote working. No major issues were found.

Access to relevant information for the NCAs

62. Authorities were asked whether they encountered any issues related to gaining access to the CCPs' information during the remote working situation.

63. Generally, no issues were raised by the NCAs related to access to the CCPs' information during remote working arrangements.

IT systems reliability and security

64. The authorities were invited to describe their supervisory activities in relation to the CCPs' review of their IT systems, policies and procedures with respect to remote working arrangements, to ensure they satisfy the requirements of RTS Art 9 and the CPMI-IOSCO guidance on cyber resilience.

65. Most NCAs reported that the issues addressed in the questionnaire were covered by their generic risk-based supervisory approach. Some NCAs also provided more additional details on specific practices. The details are described in the subsections below.

Table 3: NCAs' approaches to review of IT systems reliability and security

	Generic approach	***Generic approach and/or Specific practices***
IT systems reliability and security	11	0
Operational risk policies and procedures dealing with cyber security	8	3
Addressing of cyber risks stemming from remote working	9	2
Identified cyber risks and issues related to remote working arrangements	7	4
Changes in the IT systems	10	1
Differences in remote working	10	1
Cyber security incidents related to remote working	8	3
Monitoring and assurance of IT systems reliability and security	8	3
Review of policies, procedures and processes	11	0

66. Generally, the NCAs relied on their regular supervisory activities for addressing the CCPs' IT risk management. These activities consisted of regular supervisory meetings with the CCPs' management and/or staff, where CCPs' major changes to their policies

or IT systems are discussed. In addition, NCAs mentioned as well on-site inspections, reviews of audit reports, ESCB cyber resilience surveys and TIBER tests.

67. In terms of specific requirements or guidelines, there is no obvious standard that is used by all NCAs to address IT and/or cyber risk at the CCPs. Rather, multiple standards and/or guidelines are used to draw inspiration from when addressing cyber risk. The CROE was mentioned as an important guideline by several NCAs within the euro area. NCAs also mentioned the PFMI, ISO27001 and the EBA Guidelines on ICT and security risk management. The DORA regulation, which is currently still in development, is mentioned as a possibility to introduce a new EU standard for supervising cyber risk.

Operational risk policies and procedures dealing with cyber security

68. Authorities were asked how they supervised the CCPs' operational risk policies and procedures dealing with cyber security.

69. A majority of the NCAs addressed the policies and procedures dealing with cyber security as part of their overall risk-based supervision approach. In general, this risk-based approach is based on identifying possible risks and mitigate them with supervisory action. For identification of the cyber risk at CCPs, NCAs made use of desk-based reviews based on the CCPs' responses to surveys on cyber resilience[8], (internal and/or external) audit reports and self-assessment reports on cyber resilience. The outcomes of such reviews and follow-up were discussed during regular meetings with the CCPs.

70. One NCA conducted ad hoc on-site inspections on cyber security before and after the reporting period. Another NCA reviewed the yearly (ICT) SREP assessment. Finally, another NCA also implemented the TIBER framework, while other NCAs are in the process of implementing it.

71. Some NCAs indicated an improvement of the CCPs' cyber resilience capabilities, according to the results of the mentioned surveys. No decline in cyber capabilities was mentioned by any NCA. Attention was also given to the monitoring of the CCPs' recovery time objective (RTO).

Addressing of cyber risks stemming from remote working

72. Authorities were asked how they addressed the cyber risks stemming from remote working.

73. A majority of the NCAs answered that specific attention was paid during regular meetings regarding the cyber risks stemming from the remote working situation, but that no specific actions were initiated. They indicated that the reason was because remote working (and mitigating related risks) was already a common practice at the CCPs before the pandemic situation. Control measures for remote working situations were already tested and implemented well before the pandemic, e,g. secure VPN connections, awareness campaigns and multi-factor authentication.

[8] NCAs referred to the ESMA Cyber Questionnaire, the Eurosystem Cyber Resilience Survey, the CPMI-IOSCO Survey on cyber resilience of FMI's and/or ECB/SSM cyber surveys

74. One NCA mentioned that it followed up on major incidents and alerts at other FMIs that could have (potentially) been linked to - and may have had impact on – a CCP.

Identified cyber risks and issues related to remote working arrangements

75. Authorities were asked which cyber risks and issues were identified related to remote working arrangements.

76. A majority of the NCAs answered that employee vulnerabilities (e.g. social engineering, data leakage, phishing) was the most urgent cyber risk related to remote working. Some NCAs mention ransomware and VPN issues as other significant cyber risks.

77. One NCA mentioned that a CCP reviewed its communication tools for adequate decision-making while working remotely. Three NCAs mentioned that their CCPs conducted security education campaigns in 2020 with a focus on remote working to reduce employee vulnerability.

Changes in the IT systems

78. Authorities were asked how they supervised changes made to the IT systems of the CCPs as a consequence of remote working facilities.

79. A majority of the NCAs answered that no major changes were required for the IT systems as a consequence of remote working facilities. Indeed, remote working was already a common practice or part of the BCM procedures, well before the pandemic situation. The NCAs relied on their regular supervisory activities for monitoring any (major) changes made at the CCPs, e.g. based on change reports and by organizing periodic calls with the CCPs' management on the topic.

80. One NCA also reviewed the CCP's change management process.

Differences in remote working

81. Authorities were asked if there was a difference between remote working as a usual business arrangement and as a part of the business continuity arrangements during the Covid-19 pandemic.

82. Generally, the NCAs report no major differences in the CCPs' setup of remote working arrangements.

Cyber security incidents related to remote working

83. Authorities were asked if CCPs reported (major) cyber security incidents to the NCAs related to remote working.

84. Generally, the NCAs indicated that no major incidents were identified. Some NCAs made report of minor DDoS threats or attacks, with no impact on the CCPs' functionality.

Monitoring and assurance of IT systems reliability and security

85. Authorities were asked how they supervised the CCPs' monitoring and assurance of its IT systems reliability and security under the remote working arrangements, including cyber resilience.

86. A majority of the NCAs relied on the business-as-usual supervisory activities: regular supervisory calls and the monitoring (and follow-up) of incident reports, operational risk reports, audit reports and resilience testing exercises.

87. Some NCAs participated in the CCPs' periodic supervisory board meetings. One NCA indicated to have monitored a CCP's teleworking test. Another NCA participated in regular cross-market working groups with CCPs.

Review of policies, procedures and processes

88. Authorities were asked how they supervised the CCPs' review of their policies, procedures and processes related to cyber security and reliability to adapt to company-wide remote working arrangements.

89. Generally, the NCAs report no real need to change the policies and procedures and therefore no need for a separate review. In case of any changes made to policies, the NCAs would monitor those changes in their regular supervisory meetings with the CCPs.

Business continuity plan, policies and procedures

90. Authorities were invited to describe their supervisory activities in relation to the CCPs' review of their business continuity plan, policies or procedures to ensure they satisfy the requirement of EMIR Art 34 and related RTS Art 17-23 and Principle 17 of PFMI, with respect to remote working.

91. Most NCAs reported that the issues addressed in the questionnaire were covered by their generic risk-based supervisory approach. Some NCAs also provided more additional details on specific practices. The details are described in the subsections below.

Table 4: NCAs' approaches to review of business continuity plan, policies and procedures

	Generic approach	***Generic approach and/or Specific practices***
Supervisory activities on business continuity plan, policies and procedures	11	0
Supervision of business continuity policies and procedures	11	0
Fitness of the CCPs' remote working arrangements related to business continuity	11	0
Review of the CCPs' business continuity policies and procedures	10	1
Review or testing of (extreme) risk scenarios	10	1
Review or testing of crisis management and communication procedures	10	1
Access to critical locations	7	4

92. Generally, the NCAs indicated that their supervisory activities during the reporting period were not very different from their regular supervisory activities consisting of. the regular (annual) review of the CCPs' BCM policies, and the review of testing reports, (internal/external) audit reports and (major) changes and incidents.

93. To assess compliance with EMIR Art 34 and related RTS Art 17-23, NCAs used various standards and/or guidelines when reviewing the CCPs' BCM policies, such as: PFMI Principle 17 – Operational Risk, ISO 22301:2019 Security and resilience -Business continuity management systems, and COBIT - DSS04 Managed Continuity.

Supervision of business continuity policies and procedures

94. Authorities were asked how they supervised the CCPs' business continuity policies and procedures.

95. Generally, the NCAs reported they reviewed the business continuity framework as part of the regular annual review. Two NCAs noted that they attended as observers the CCP's BCM tests, which provided them with valuable insights into the CCP's decision-making capability and good practices during the BCM test.

96. This means no differentiation during the reporting period compared to the pre-pandemic (business-as-usual) situation. The remote working arrangements seemed to have had no significant impact on the business continuity of the CCPs' critical operations.

Fitness of the CCPs' remote working arrangements related to business continuity

97. Authorities were asked how they supervised the fitness of the CCPs' remote working arrangements related to the business continuity.

98. A majority of the NCAs reported that the remote working arrangements were already used at the CCPs well before the pandemic outbreak and were already part of the regular BCP and/or Disaster Recovery (DR) tests. No major shortcomings or concerns about the CCPs' remote working arrangements were mentioned by the NCAs.

Review of the CCPs' business continuity policies and procedures

99. Authorities were asked how they supervised the CCPs' review of business continuity policies and procedures following the remote working arrangements during the Covid-19 pandemic. They were invited to share lessons learned and and/or updates made to the documents after the CCPs' review.

100. Generally, the NCAs reported that no major adjustments were needed for the business continuity policies and procedures in relation to the remote working arrangements.

Review or testing of (extreme) risk scenarios

101. Authorities were asked how they checked whether the CCPs had reviewed or tested the (extreme) risk scenarios, including remote working arrangements, related to a pandemic such as the Covid-19 pandemic. They were invited to share their lessons learned and/or updates made to the documentation after the CCPs' review.

102. A majority of the NCAs reported that they had monitored and analysed the CCPs' annual review of BCPs and extreme scenarios. No specific findings emerged.

103. One NCA recommended a CCP to improve their testing procedures so that findings and lessons learned would be included in a more consistent and clearly documented way.

Review or testing of crisis management and communication procedures

104. Authorities were asked how they checked whether the CCP reviewed or tested the crisis management and communication procedures addressing the remote working arrangements related to a pandemic. They were invited to share their lessons learned and/or updates made to the documentation after the CCPs' review.

105. Generally, the NCAs reported that they made use of their regular supervisory activities to the CCPs' review of crisis management and communication procedures. These activities mainly consisted in reviewing the CCPs' internal (risk) reports and (annual) BCM testing reports.

106. As mentioned above, one NCA observed the CCP's BCM tests during remote working arrangements.

Access to critical locations

107. Authorities were asked how they supervised whether the CCP is certain of (physical) access to their critical locations during these extreme scenario's.

108. A majority of the NCAs reported that they were in regular contact with the CCPs' management during the remote working situations. The topic of access to critical locations was discussed by most NCAs during these conversations. No issues were mentioned in this respect.

109. Some NCAs reported that (physical) access to critical locations was already part of CCPs' BCM testing scenarios before the Covid-19 pandemic. This meant that no additional action was needed.

5.2 Main findings

110. Overall, answers to the questionnaire were thorough and provided clarification of the various supervisory actions. NCAs reported that they applied a risk-based approach to the supervision on business continuity in remote access mode. Risk management requirements related to operational risk, including cyber risks, and business continuity requirements were often discussed in supervisory meetings with the CCPs. In some cases, NCAs conducted on-site inspections and specific desk-based reviews, also addressing the specific risk related to the wider use of remote working arrangements during the Covid-19 pandemic.

111. The responses to the peer review show a high degree of convergence of the supervisory approaches in the supervisory practices on business continuity in remote access mode.

112. On the basis of the responses to the peer review questionnaire and the annexed documentation, the responses to and follow-up questions, and the evidence from the

on-site visits, the PRC considers that, overall, the NCAs participating in the current peer review broadly met the supervisory expectations as listed in the peer review mandate.

113. Nevertheless, the following three observations can be drawn:

a. As remote access is covered in general as part of operational risk. it is not always clear which specific considerations were taken into account regarding the risk-based approach of remote working arrangements. NCAs could better clarify, when defining their risk-based approach, how operational risks related to remote access are addressed.

b. Regarding cyber resilience, it is generally indicated that CCPs perform regular penetration testing. Remote access is implicitly taken into account during these tests. From a supervisory perspective, CCPs could better clarify the risk-based scope of penetration testing and how risks related to remote access are addressed as part of this.

c. Although in general remote working arrangements were already part of business-as-usual arrangements or part of the BCM plans, the scope of usage during the pandemic was in general unforeseen. BCM plans could in this context be improved by taking into account other extreme scenarios where remote working arrangements could serve to ensure business continuity.

114. Moreover, the peer review identified the following specific supervisory best practices on business continuity in remote access mode with respect to risk management, IT systems reliability and security, and business continuity:

Best practice 3: NCAs could have regular meetings with CCPs with a specific focus on operational resilience. The frequency of such meetings should be at least quarterly, while the need for more frequent meetings would be risk-based. Attendance of such meetings should involve operational experts from both NCAs' and CCPs' side. To be well prepared for such meetings, the NCAs could send scoping questions and/or request from the CCPs to receive well in advance of the meeting any relevant input, such as reporting on identified operational risks (risk self-assessment), risk controls in place, relevant policies and procedures. In preparation or as follow-up to such meetings, NCAs could perform desk-based reviews with specific focus on the CCPs' operational resilience.

Best practice 4: During extreme situations (e.g. a pandemic outbreak, increased cyber-attacks unavailability of internet services or extensive power supply outages), NCAs could reinforce their regular supervision by increasing the frequency of interactions with the CCPs' management and operational staff. NCAs could request daily updates on operational availability, incidents and threats.

Best practice 5: Until the new regulation on Digital Operational Resilience for the financial sector (DORA) enters into force, NCAs could consider existing guidelines and expectations consistent with the CPMI-IOSCO guidance on cyber resilience, such as the Cyber Resilience Oversight Expectations (CROE), the CIS18 Controls (Center for Internet Security - Critical Security Controls) and, to the extend applicable to CCPs, the EBA Guidelines on ICT and security risk management and relevant guidelines by (inter)national Cyber Security Centres.

Best practice 6: NCAs could request CCPs to test their cyber security and cyber resilience by performing regular penetration tests, and to consider changing over time the external service providers supporting them with the penetration testing, as this contributes to gaining new insights on cyber security. The frequency of such tests should be risk-based reflecting the CCPs' risk profile and complexity. The TIBER framework could be used as a best practice for an extensive threat intelligence-based red teaming test.

Best practice 7: NCAs could request CCPs to perform regular awareness campaigns, covering the (security) risks related to remote working, in order to reduce employee vulnerability.

Best practice 8: Besides the regular review of BCM policies and tests, NCAs could also request CCPs to take specific extreme scenarios into account during their annual review of BCM policies, including e.g. a pandemic outbreak, increased cyber-attacks, unavailability of internet services or extensive power supply outages. The formulation of extreme scenarios should be risk-based, as they are very dependent on each CCP's specific critical processes and (cyber) threats. Testing of (extreme) scenarios should be done at least annually, but it should also be possible to perform ad hoc tests if material risks are foreseen.

Best practice 9: NCAs could participate as an observer in (some of) the CCPs' BCM tests. This could provide the NCAs with a better understanding of the CCPs' decision-making capability, good practices and points for improvement.

Best practice 10: When reviewing the CCPs' business continuity plans and crisis management plans, NCAs could also consider the 'user friendliness' of such plans as an important element of their effectiveness. In extreme situations it could prove to be vital for new employees or temporary external employees to be able to easily and clearly find in the plan what to do during a crisis. A very comprehensive but difficult to use BCM plan is typically less user friendly or effective.

6 Conclusions

115. The review of the functioning of the colleges during the reporting period remains overall positive. In particular, ESMA appreciated the efforts of chairing NCAs to meet previous best practices and expectations as well as the new guidelines issued in 2021, and to update the colleges on the recent market developments related to the Russian invasion of Ukraine- and their impact on CCPs' risk management and operations. Overall, chairing NCAs continue to manage CCP colleges in compliance with EMIR. However, CCP colleges continue following the trend, already noted in past peer review, of performing merely as fora for regular updates and exchange of information, where college members largely rely on chairing authorities' reporting and ESMA reviews.

116. Regarding the NCAs supervisory activities on business continuity in remote access mode the overall outcome of the peer review is that the NCAs participating in the current peer review broadly met the supervisory expectations.

117. NCAs reported that they applied a risk-based approach to the supervision on business continuity in remote access mode. Overall, NCAs reported supervisory activities covering several aspects of CCP operational resilience during the reporting period and several NCAs closely monitored the unprecedent shift to remote working

arrangements throughout the Covid-19 pandemic via continuous reporting and regular meetings.

118. In particular, NCAs reviewed the CCPs' operational resilience in the scope of the annual reviews under Article 21 of EMIR conducted within the reporting period, and topics related to business continuity and operational and cyber resilience were discussed in regular supervisory meetings with the CCPs. In some cases, NCAs conducted on-site inspections and specific desk-based reviews, also addressing the specific risks related to the wider use of remote working arrangements during the Covid-19 pandemic.

119. The Covid-19 crisis and consequent wide use of remote working arrangements was a specific point of attention during supervisory meetings and no major issues were identified and no major incidents were reported regarding remote working in the review period.

120. However, the peer review showed that the assessment of some areas on business continuity in remote access mode was not always being evidenced specifically. In most cases, this is explained by the fact that at many CCPs remote working was already common practice or part of business continuity arrangements. In this context, remote working in general did not introduce new major risks.

121. Nevertheless, the following three observations were noted:

a. NCAs could better clarify, when defining their risk-based approach, how operational risks related to remote access are addressed.

b. From a supervisory perspective, CCPs could better clarify the risk-based scope of penetration testing and how risks related to remote access are addressed as part of this.

c. BCM plans could in this context be improved by taking into account other extreme scenarios, where remote working arrangements could serve to ensure business continuity.

122. Moreover, ten best practices emerged from the review of NCAs' supervisory activities and approaches with respect to business continuity in remote access mode (see Box 1 above). Implementing these best practices would also address the three observations mentioned above.

123. The table below provides an overview of the current level of implementation of the best practices found in this Peer Review. The results reflected in this overview are based on the information received during the peer review.

124. Finally, while the new EU legislative proposal for DORA is going to establish a new regulatory framework applying also to CCPs, it could be considered whether there remain areas for improvement within the EMIR framework, in order to strengthen the enforcement of EMIR requirements with respect to business continuity (not addressed by DORA). This could be addressed via a review of the relevant RTS under EMIR.

Table 5: Overview of implementation of best practices

Best practices	Implementation frequency
1 Set up competence center	7
2 Apply proactive approach	5
3 Dedicated meetings	5
4 Request daily crisis updates	8
5 Use international cyber resilience guidance	11
6 Request penetration testing	6
7 Request awareness training	8
8 Request (more) extreme, relevant stress scenarios	5
9 Participate in BCP tests	2
10 Assess user-friendliness BCP	3

The maximum implementation frequency amounts to 11, equalling the total number of Member States with a CCP, as where a Member State had designated several NCAs under EMIR, the authorities from this Member State coordinated a single response and are counted as one.

Annex 1 – Survey Questionnaire

1. General Information

1.1 Information on CCPs and supervisory activities

1. Please indicate in the table below the CCPs you supervise, and the dates of any supervisory review or activity (such as desk-based investigations or on-site inspections) conducted in the reference period which addresses the CCPs' operational resilience under remote working arrangements, also covering the relevant cybersecurity aspects. Also indicate the current status of these activities (E.g. closed, ongoing, planned, continuous).

CCP(s)	Supervisory Activity	Date	Description	Reference EMIR/RTS Article	Status

Please, attach to your answer any related NCAs' report documenting the outcome of the respective supervisory review or activity (where available in English, otherwise in the participating authority's working language[9]).

1.1.1 Organizational setup of the relevant Competent Authority(-ies)10

2. Please, indicate in the table below the competent authorities that have direct supervisory responsibilities to assess the CCPs' operational resilience under remote working arrangements on the basis of EMIR Article 26 and 34 and related RTS. Please specify the internal department in charge of the supervisory activities and the number of Full-Time-Equivalent staff members (FTEs) assigned to such activities, and whether internal procedures, guidelines or other tools have been developed to help staff dealing with these supervisory activities related to "business continuity in remote access mode". (If yes, please describe them and provide a copy of the relevant documentation).

[9] A translation in English could be requested by ESMA staff in follow-up interactions.

[10] According to Article 30(a) of ESMA regulation, the peer review shall inter alia include an assessment of the adequacy of resources and governance arrangements of the competent authority […].

Competent Authority	**Internal Department**	**N. of FTEs**	**Reference EMIR/RTS Article**	**Internal procedures/ handbook/guidelines/ other tools**

Please, explain and provide a copy/extract of the relevant competent authority's organizational chart or a list of staff members involved in the supervisory activities related to operational resilience under remote working arrangements, also covering the relevant cybersecurity aspects. Also give an indication of their title, seniority and background. If more than one competent authority has shared responsibility in conducting supervisory activities related to operational resilience under remote working arrangements, please explain how cooperation between authorities is ensured and how the relevant activities are coordinated. If applicable, provide any relevant cooperative arrangement (e.g. MoU, information sharing agreement) related to such activities.

1.2 Supervisory activities on business continuity in remote access mode

Competent authorities should assess whether CCPs comply with the regulatory provisions as detailed in the mandate and specifically:

a. General provisions on organisational requirements as set out in Article 26 of EMIR and related RTS (namely Article 4 on risk management and internal control mechanisms and Article 9 on Information Technology (IT) systems of RTS 152/2013)

b. Business continuity as set out in Article 34 of EMIR and related RTS (namely Articles 17-23 on business continuity of RTS 152/2013).

In accordance with the Guidelines on the implementation of the CPSS-IOSCO Principles for Financial Market Infrastructures in respect of Central Counterparties (ESMA/2014/1133), while reviewing compliance with the above requirements, the competent authorities should also take into account the relevant provisions of the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) (in particular, Principle 17 thereof) and the CPMI-IOSCO guidance on cyber resilience.

When a competent authority reports that it checks a specific point, it should specify how this is performed. Is this done through off-site supervision (i.e. considering documents provided by the CCP as a proof of the implemented methodology) or by checking directly during an on-site inspection if the documents provided reflect the actual practice, if possible during the Covid-19 pandemic.

Q1: Operational risk management policies and procedures

The NCA is invited to describe their supervisory activities in relation to the CCPs' review of their risk management policies and systems to ensure they satisfy the requirement of Art 4 of RTS 153/2012 and Principle 17 of the PFMI with respect to remote working arrangements.

Please give a description of what has been done by the NCA in this respect:

Please answer the following questions.

1. How did the NCA supervise the CCPs' risk management policies and procedures (including those for crisis management) e.g. on-site / off-site inspections, specific meetings or investigations?

2. How did the NCA supervise the CCPs' identification and monitoring of the risks posed by remote working arrangements during business as usual (before the Covid-19 pandemic)?

3. How did the NCA check the CCPs' assessment and monitoring of the risks posed by remote working arrangements during the Covid-19 pandemic? Where applicable, please describe how the CCPs' risk assessments addressed the following topics:
   a. Identification of the business functions and processes impacted by the remote working situation during the Covid-19 pandemic

   b. Identification of risks related to the situation of remote working during the Covid-19 pandemic

   c. Controls specific for the remote working situation

   d. Monitoring the well-functioning of remote working facilities

   e. Incident response planning in case of unavailability of remote working facilities

   f. Contingency planning during the remote working situation

   g. Testing of the resilience of the remote working facilities

4. How did the NCA supervise the CCPs' review of their risk management policies, procedures, and processes to adapt to company-wide remote working arrangements? Where applicable, please describe how the CCPs' review addressed the following topics:

   a. Risk assessments related to remote working as company-wide remote working arrangements

b. Policies, procedures, and processes related to remote working as company-wide remote working arrangements

5. What were the main points identified by the review of the company-wide remote working arrangements? If applicable, how are these points addressed?

6. Did the NCA check whether access to all relevant information for the risk management function was assured during the remote working situation? If applicable, please explain.

7. Did the NCA have any issues related to access to the CCPs' information during the remote working situation? If applicable, please explain.

Q2: IT systems reliability and security

The NCA is invited to describe their supervisory activities in relation to the CCPs' review of their systems, policies, and procedures to ensure they satisfy the requirement of RTS Art 9 and the CPMI-IOSCO guidance on cyber resilience, with respect to remote working arrangements.

Please give a description of what has been done by the NCA in this respect:

Please answer the following questions.

8. How did the NCA supervise the CCPs' operational risk policies and procedures dealing with cyber security, e.g. on-site / off-site inspections, specific meetings, participation in cyber surveys (ESCB/CPMI) and/or in the TIBER-EU framework?

9. How did the NCAs' activities address the cyber risks stemming from remote working? Where applicable, please describe how these activities addressed the following topics:

    a. Risks related to phishing, ransomware, vulnerabilities in remote working applications (such as Citrix), and Distributed Denial of Service (DDoS) attacks in the situation of remote working during the Covid-19 pandemic?

    b. Controls specific for the remote working situation such as VPN connections, managed laptops, remote desktops, other?

    c. Monitoring of remote working facilities to detect anomalous activities and events?

    d. Specific cyber security awareness training regarding remote working?

   e. Consequences for identity and access management of remote working?

   f. Testing the cyber-resilience of remote working facilities?

10. Which cyber risks and issues were identified related to remote working arrangements? If applicable, how have these been addressed?

11. How did the NCA supervise changes in the IT systems of the CCP as a consequence of remote working facilities?

12. Was there a difference between remote working as a usual business arrangement and as a part of the business continuity arrangements during the Covid-19 pandemic? If applicable, what were the differences?

13. Did the CCP report cyber security incidents to the NCA related to remote working? E.g. DDoS attacks, ransomware, vulnerabilities in the remote working facilities. If applicable, how were these issues addressed by the NCA?

14. How did the NCA supervise the CCPs' monitoring and assurance of its IT systems reliability and security under the remote working arrangements, including cyber resilience?

15. How did the NCA supervise the CCPs' review of their policies, procedures and processes related to cyber security and reliability to adapt to company-wide remote working arrangements?

Q3: Business continuity plan, policies, and procedures

The NCA is invited to describe their supervisory activities in relation to the CCPs' review of their business continuity plan, policies, or procedures to ensure they satisfy the requirement of EMIR Art 34 and related RTS Art 17-23 and Principle 17 of PFMI, with respect to remote working.

Please give a description of what has been done by the NCA in this respect:

The NCA is requested to answer the following questions:

16. How did the NCA supervise the CCPs' business continuity policies and procedures? Please elaborate on the NCAs' supervisory activities such as onsite/offsite inspections, specific meetings on this topic or participation by the CCP in relevant surveys (ESCB/CPMI).

17. How did the NCAs' activities address the fitness of the CCPs' remote working arrangements related to business continuity? Where applicable, please describe how the

NCAs’ activities covered remote working scenarios within the CCPs’ business continuity plans in relation to:

a. the preservation of the CCPs’ functions
b. the timely recovery of operations
c. the fulfilment of the CCPs’ obligations

18. How did the NCA supervise the review of the CCPs’ business continuity policies and procedures following the remote working arrangements during the Covid-19 pandemic? What were the lessons learned and/or updates made to the documents after this review?

19. How did the NCA check whether the CCP reviewed or tested the (extreme) risk scenarios addressing the remote working arrangements related to a pandemic such as the Covid-19 pandemic? (E.g. scenario’s for the remote access of critical functions or large scale illness of critical employees). What were the lessons learned and/or updates made to the documents after this review?

20. How did the NCA check whether the CCP reviewed or tested the crisis management and communication procedures addressing the remote working arrangements related to a pandemic? What were the lessons learned and/or updates made to the documents after this review?

21. How did the NCA supervise whether the CCP is certain of (physical) access to their critical locations during these extreme scenario’s? For example, access to data centres or (outsourced) secondary sites