DTCC
Securing Today. Shaping Tomorrow.®

55 Water Street
New York, NY 10041
United States of America

+1 (212) 855-1000

9 August 2019

Australian Securities and Investments Commission
Level 5, 100 Market Street
Sydney, NSW 2000
Australia

Att'n: Mr. Andrew McPherson, Senior Specialist
Market Infrastructure

Re: Response to Consultation Paper 314 – Market integrity rules for technological and operational resilience

Dear Mr. McPherson,

The Depository Trust and Clearing Corporation[1] (DTCC) welcomes the opportunity to provide its views on Consultation Paper 314 on Market integrity rules for technological and operational resilience.

We are strongly supportive of ASIC's efforts to improve market integrity, as well as technological and operational resilience. We are heartened by the consideration given to the global efforts in other jurisdictions, as well as to the developments likely to result from technological advancement.

We agree that the resilience of market operators and market participants are essential to the integrity of the securities and futures markets and the financial services sector as a whole. DTCC also acknowledges the focus of the Australian Securities and Investments Commission (ASIC) on outsourcing, change management, and international coordination. We address these topics through the answers provided to the questions in the Consultation Paper presented in the Annex, but we would like to highlight the following views:

[1] The Depository Trust and Clearing Corporation ("DTCC") is a major post-trade market infrastructure provider for the global financial services industry. From operating facilities, data centers and offices in 15 countries including Australia, DTCC, through its subsidiaries, automates, centralizes and standardizes the processing of financial transactions, mitigating risk, increasing transparency and driving efficiency for thousands of broker/dealers, custodian banks and asset managers. Industry owned and governed, the firm simplifies the complexities of clearing, settlement, asset servicing, data management, data reporting and information services across asset classes, bringing increased security and soundness to financial markets.

Outsourcing Critical Systems

Many Market Operators and Market Participants have increased their use of third-party service providers by outsourcing certain operational functions or the development of new products and services. This expansion of the supply chain allows these firms to optimize costs and provides an opportunity to introduce new and innovative solutions to the marketplace. DTCC agrees that market operators and market participants should manage their outsourced relationships in a manner that is consistent with the impact that a service may have to its critical business services[2] and the consequential potential to affect the integrity of the markets. The management of outsourcing risks should be commensurate to the level of risk presented by the outsourcing arrangement that may have a significant impact on the market operator and market participant's financial condition, is essential to its core business services, involves the use of sensitive customer information, or poses a material risk of contagion to the financial services sector.

DTCC agrees that the provisions as proposed are aligned with current international guidance on outsourcing arrangements with the exception of the proposals contained in B3(d)(iv) and B3(d)(v). This level of disclosure may have the unintended consequence of firm vulnerabilities being distributed across the sector as market operators and market participants request this information from their providers. In the worst-case scenario, the disclosure of details of a compromise to the system integrity of a market operator or market participant may lead to the exposure of vulnerabilities within the supply chain which in turn could ultimately lead to additional successful attacks across the sector. Secondly, while providing detailed vulnerability information could provide the supervisor with greater transparency into how the financial services sector is managing its risks, the detailed reporting requested in these statements would create a central point of such data which in turn could become a target of malicious attacks which could ultimately result in more severe consequences to a wider segment of the financial services sector. We therefore recommend that reporting obligations be weighed against the potential risk of such an extreme but plausible circumstance.

It is also recommended that market operators and market participants have a level of oversight commensurate with the aforementioned risks that the service provider may have to the firm, consumer, or market integrity. In the proposed B3(f), DTCC believes it may be in the interest of the market to articulate the purposes of this rule. While the collection of critical outsourcing arrangements may provide the supervisor with visibility into concentration risk within the financial services sector, this can be achieved after the outsourcing arrangements have been instituted.

[2] The definition of **Business Services** may be found in the UK Bank of England Discussion Paper, Building the UK Financial Sector's Operational Resilience at: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf

Change Management and Business Continuity of Critical Systems

As part of their normal operations, Market Operators and Market Participants introduce change in their technology environments in order to maintain, renew, and develop their product and service offerings. Such changes are typically carefully managed; yet issues with change management was the number one root cause of operational incidents[3] reported to the UK Financial Conduct Authority in 2017. Given the speed of technological changes and digitalization within the financial services sector, it is imperative that market operators and market participants focus on their change management processes and that these arrangements are proportional to the resilience, reliability, integrity, and security of its critical business services.

International Coordination

DTCC fully supports ASIC's efforts to promote certainty in the financial markets by encouraging market operators and their participants to adopt best practices regarding market integrity and resiliency. We have in the past advocated for the public sector to play a role when support is necessary to implement industry-wide efforts, both in terms of providing incentives and helping resolve roadblocks related to misaligned internal and external frameworks.

In that regard, we encourage ASIC and other global financial market regulators to continue work on coordinating regulatory expectations, including IOSCO and the FSB. This helps ensure that the regimes, frameworks and guidance remain compatible and, to the extent possible, aligned across multiple jurisdictions. Specifically, DTCC would like to point to the work that the FSB conducted, together with the financial services sector, in publishing the Cyber Lexicon[4] in November 2018. Given the public-private partnership used to develop this lexicon and its global applicability, we suggest that ASIC refer to this Lexicon in its definition of cybersecurity terms and align its use of these terms with the objectives of any additional guidance or rule-making. This will help reduce the difficulty of advancing the resilience agenda caused by subtle changes in the usage of terminology. Commonly used terms such as risk, threat, vulnerability, event and incident have consistently been used interchangeably and has slowed progress to develop rules and practices to address cybersecurity and cyber resilience risks.

We urge ASIC to continue to proactively engage the industry on these matters, as firms continue to balance operational and technological risk management objectives with their compulsory regulatory and supervisory obligations. This balance is particularly difficult to achieve for firms who operate across multiple jurisdictions, and who must meet different regulatory expectations – including ASIC's. Compliance with the expectations will require different and varying degrees of effort among the different firms. It is important that ASIC understand the complexity of implementation for the differently impacted firms when determining the appropriate transitional period.

[3] The UK FCA ***Cyber and Technology Resilience: Themes for cross sector survey 2017 -2018*** can be found at: https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf

[4] The Financial Stability Board's ***Cyber Lexicon*** can be found at: https://www.fsb.org/2018/11/cyber-lexicon/

We applaud ASIC's efforts to acknowledge not only technological developments to date, but also the rapid progress of new solutions. We believe that innovation should be encouraged on a level playing field that guarantees the safety and integrity of the market. Setting regulatory expectations from the outset is a fundamental step toward this goal, including the consideration given in the consultation to fair access to market operator products, data, and services.

We fully agree with ASIC that, where appropriate, there should be consistency in the regulatory approach between market operators and market participants. We also appreciate the value that the proposed rules serve as guidance of what ASIC considers to be best practice with regard to other licensed activities and would encourage further harmonization of the standards among all the regulated community.

DTCC welcomes the opportunity to further discuss these comments. If you are interested in doing so, or would like a clarification on this response and any related matters, please feel free to contact me at awdouglas@dtcc.com or Mr. Jean-Remi Lopez, Director of Government Relations APAC at jrlopez@dtcc.com.

Yours sincerely,

Andrew Douglas
Managing Director, Government Relations

Annex – DTCC responses to the Consultation Paper Questions

- **B1Q1: Do you agree with the definition of 'critical systems' and 'critical systems arrangements'? In your response, please give detailed reasons for your answer.**

  - No, we do not agree. Whilst we acknowledge ASIC's intent to "exclude systems, functions, infrastructure and processes which are non-essential to the operation of the market or a market participant's capacity to deliver market services to its clients" as articulated in Paragraph 45 of the consultation paper. we are concerned that the current drafting of explanatory Note 1 of the definition of 'Critical System' (Definitions section (8B.1.2)) appears to prescribe that all "functions, infrastructure, processes and systems that deliver or support order acceptance, routing and entry, clearing and settlement of transactions, payments and deliveries of financial products and funds, accounting for or reconciling client money, trust accounts, securities and funds, confirmations and regulatory data reporting" form part of 'Critical Systems' for a Participant. This seems to be a very broad definition that could encompass all Market Participant and Operator systems in all jurisdictions. In order to both give guidance to the firms when exercising their judgement as to what constitutes Critical Systems and maintain the intention to exclude non-essential components, we suggest the rules retain Note 1 in an illustrative rather than enumerative form (e.g. "Critical Systems referred to in this definition **may** include…"). ASIC could also consider explicitly incorporating into the Proposed Rules the regulatory expectations on the perimeter of Critical Systems as it does in paragraph 45 of the Consultation Paper.

- **B1Q2: Do you agree that market participants and market operators should have rules that require them to have in place adequate arrangements for critical systems?**
  - Yes, DTCC believes that the complexity of the financial services industry, the interconnectedness of its participants, and the introduction of new and innovative technologies further heighten operational and technology risks that must be properly understood and managed. [5]
  - Given the global nature of the financial markets, it is imperative that the rules be carefully calibrated to ensure a minimum standard for all participants; they encourage appropriate cooperation within the industry; and promote adopting the most appropriate measures based on each player's unique profile.
  - As is the case with setting all regulatory expectations, consideration must be given to the possible effects of national regulations on cross-jurisdictional operations. We therefore applaud and support ASIC's continuing efforts of coordination at IOSCO and other appropriate multilateral standard setting bodies.

[5] DTCC has shared some of these concerns with the industry in its whitepaper ***Cyber Risks: The Threats Of The New Frontier*** which can be found at: http://www.dtcc.com/dtcc-connection/articles/2019/may/20/cyber-risks-the-threats-of-the-new-frontier

- We urge ASIC to allow sufficient time for implementation of rules, especially when these may involve significant procedural, legal, or technical changes.

- **B1Q3 Do you agree with the types of arrangements that market participants and market operators should have to ensure the continued reliability of their critical systems?**

  - Yes; we agree with ASIC's broad intention of transferring resilience from a systems-centric view to a services-centric point of view, so that financial institutions consistently provide products and services to the marketplace in a manner that maintains the safety, soundness and integrity of the markets and limits consumer impact. In order to accomplish this goal, relevant entities and systems within the supply chain for critical economic functions and business services must be resilient.

- **B1Q4 Do you see any challenges for institutions in complying both with the proposed rules and other obligations they may be subject to including, for example, under Basel II or the Financial Stability Standards? In your response, please give detailed reasons for your answer.**

  - [No response.]

- **B1Q5 How will these proposed rules affect your business? If you are a market operator or market participant, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on your current critical systems arrangements.**

  - [No response.]

- **B2Q1 Do you agree that market participants and market operators should have rules that require them to have in place adequate arrangements for change management of critical systems?**

  - Yes, we agree.

- **B2Q2 Do you agree with our proposed rule? If you disagree, please give detailed reasons why.**

  - Yes, we agree although we encourage the incorporation of proportionality considerations as described in our cover letter.

- **B2Q3 How will this proposed rule affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your current expenditure on arrangements for change management of critical systems.**

    - [No response.]

- **B3Q1 Do you agree with our proposed rule that requires market operators and market participants to have outsourcing arrangements? If not, please give detailed reasons why you disagree.**

    - Yes, we agree. As stated in the Consultation Paper, the overall responsibility for the services and the data reside with the market operators and market participants, so the governance, such as policy definition, management (including contracts, service levels, and monitoring), SLA reviews and control audits, all continue to be owned completely by the such operators and participants.

- **B3Q2 Do you agree with the definition of 'outsourcing arrangement'? In your response, please give detailed reasons for your answer.**

    - No we do not agree. We would encourage the drafting of a definition of Outsourcing Arrangements in terms which do not imply a relationship with a critical system. We believe it is desirable to establish such a definition as it would enable setting, where necessary, regulatory expectations on all outsourcing arrangements. We also suggest it may be valuable to define a term such as or phrase that separately designates those relationships which provide, operate, or support Critical Systems.

- **B3Q3 Do you consider that the definition of 'outsourcing arrangement' covers the provision of services provided by all third-party service providers and not just those that may have been performed by the entity itself? If not, what if any risks do you see in relation to the provision of services by these entities?**

    - Yes, the current state of the definition of 'outsourcing arrangement' does cover the provision of services well beyond those that may have been performed by the entity itself; yet, as stated above, the current proposed rules may unintentionally capture functions which are non-essential to the operation of the market or a market participant's capacity to deliver market services to its clients.

- **B3Q4 Do you agree with the specific outsourcing arrangements proposed?**

  - We partially agree. The overall responsibility for the services and the data reside with the market participants and operators so governance such as policy definition, management (including contracts, service levels, and monitoring), SLA reviews and control audits, should continue to be owned completely by such market participants.
  - We believe that all outsourcing arrangements should be properly identified; that market operators and participants should conduct due diligence to an extent commensurate with the importance of the service to be provided; and that the arrangements be documented appropriately in a legally binding written contract as described in Proposal B3 (c). We further agree that regulatory expectations must be met, as described in paragraph (e) "in a manner appropriate to the nature, complexity, risks and materiality of the outsourcing arrangement; and in determining whether the service provider has the ability and capacity to provide the outsourced services, consider the extent to which the service provider is providing the same or similar services to other market operators or market participants". We believe that this proportionality measure should be applied to all outsourcing arrangements.
  - However, in some instances the outsourcing arrangements may not incorporate a provision requiring approval to be sought by the service provider before "outsourcing any of the services already outsourced to them to another party and before making any other material change to the manner in which the services covered by the outsourcing arrangement are provided" as described in paragraph (ii) of the proposal. It should be left to the Operators and Participants to decide whether it is appropriate for them to require these or similar terms to be incorporated into the contract. It may also not be appropriate or feasible for all outsourcing arrangements to incorporate provisions for the orderly transfer of services as described in paragraph (c)(iii) of Proposal B3, as some services may not be transferable.
  - Market operators and participants have a responsibility to monitor their service providers' ongoing performance and capability to deliver contracted services; identify and manage conflicts of interest; and at all times ensure they maintain their ability to comply with the Corporations Act and market integrity rules. However, it may not be appropriate or feasible in all cases for a Participant, an Operator, or its auditors to, as described in paragraphs (d)(iv) have prompt access to "books, records, and other information relating to the critical systems". Instead, the regulated entities should be allowed to put in place appropriate control and oversight mechanisms which might include the stated provisions or achieve a substantially equivalent outcome, As discussed previously, there should be also be a proportionality measure to ensure that oversight efforts are commensurate with the importance of the service provided relative to the critical system – including whether they justify being subject to confirmation and attestation by the board and senior management. In order to ensure that senior management and boards devote appropriate attention to the most relevant services, we suggest that rather than subjecting each outsourcing

arrangement to a confirmation and attestation procedure by the board and senior management as described in paragraph (d)(vi), they be mandated, as part of their oversight responsibilities, to be aware of the risks that are outside of the Market Operator or Market Participant risk appetite and track the mitigation and resolution actions.

- Whilst we acknowledge that ASIC needs to be able to effectively and efficiently discharge its supervisory and enforcement duties, we would like to highlight that in some cases it would be impractical or unfeasible to contractually subject a service provider to the oversight of ASIC as set out in paragraph (d)(v) of proposal B3, especially when the service provider may operate its systems from one or several other foreign jurisdictions; the difficulty might be exacerbated when such service provider may itself be subject to such jurisdictions' oversight framework, including for example that of a home jurisdiction privacy or securities regulator. Subject to the materiality threshold already discussed, it may be more appropriate for ASIC to set the expectation that an effective mechanism allowing it to exercise appropriate regulatory oversight must be in place for all outsourcing arrangements.

- **B3Q5 Do you consider that the risks associated with outsourcing to the cloud warrant a rule specific to that outsourcing arrangement? In your response, please give reasons for your answer.**

  - No. DTCC believes that regulation should be technologically agnostic, and we regard the use of a cloud vendor as similar to any third-party vendor and raises many of the same issues[6]. While the responsibility of the use of any third-party vendor resides with the regulated party, we believe that whether incorporated in a specific ruleset or incorporated in others, in determining what is the best regulatory approach for the use of cloud, we encourage ASIC to take into consideration the following factors:
    - Data protection and sensitivity. Market operators and participants' security policy for outsourcing and cloud services must ensure adequate safeguards to protect the confidentiality of data. Among the issues the policy needs to cover is whether the cloud adequately protects and/or encrypts sensitive data and encryption key management concerns. Market operators and participants must recognize that, regardless of the rigor of a cloud vendor's data security, it holds complete responsibility for ownership and protection of its data.
    - Data integrity. Market infrastructures must take steps to ensure data integrity to prevent data from being altered or destroyed under extreme circumstances. The market infrastructure must be able to establish procedures to validate and verify the integrity of its outsourced and cloud hosted data, in addition to controlling data retention periods.

[6] *See Moving Financial Market Infrastructure to the Cloud, http://perspectives.dtcc.com/downloads/whitepaper/moving-financial-markets-infrastructure-to-the-cloud.*

- Continuity of Service. Market operators and participants must ensure that data is available when needed. The cloud vendor must have adequate plans to respond to disasters and provide continuous service and pledge to make available essential communications links. It is incumbent on the market operators and participants to develop formal policies related to redundancy and the availability of backup data.
- Auditing issues. The compliance function of market operators and participants should require that cloud vendors have familiarity complying with the demands of regulated entities and can contractually meet current requirements, particularly related to required reporting and safeguarding of sensitive information. The regulated market operators and participants should use appropriate audit tools to ensure that the cloud vendor's internal controls are adequate.

- **B3Q6 How will these proposed rules affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on your current outsourcing arrangements.**

  - [No response.]

- **B4Q1 Do you agree with the proposed rules? If not, please give detailed reasons why you disagree.**

  - Yes, DTCC is a vocal proponent of public sector involvement in addressing challenges in both cyber-resilience and data management.
  - We broadly agree on the intent of the proposed rules. However, cyber-threats may justify a more comprehensive regulatory framework which should be applicable to the broader market, not only Market Participants and Operators. We encourage ASIC to consider leveraging the body of work developed by the international regulatory community, as well as engaging the industry when developing a comprehensive framework that includes collective response and recovery plans, outlining key response and recovery requirements; and which consider contingent service arrangements[7].

[7] *See Large-Scale Cyber-Attacks on the Financial System,* http://perspectives.dtcc.com/downloads/whitepaper/large-scale-cyber-attacks-on-the-financial-system.

- **B4Q2 Should the proposed requirement for market operators to notify ASIC of any unauthorised access to or use of their critical systems and market-sensitive, confidential or personal data be extended to market participants? Please provide detailed reasons for your answer.**

    - Yes. We believe that sharing information on breaches in a structured fashion among market participants is an important component in strengthening collective resilience. ASIC, being informed of the attacks, can play a crucial role in the context of cross-industry coordination on response and recovery mechanisms to mitigate the systemic consequences of a large-scale cyber-attack. We would highlight IOSCO's recommendation to draw from existing, prominent Cyber frameworks developed by experts in this space. This approach ensures consistency and avoids overlap, duplication, and conflict between Cyber frameworks, all of which can impede progress in this area.

- **B4Q3 How will these proposed rules affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on your data protection arrangements.**

    - [No response.]

- **B5Q1 Do you agree with the definition of 'incident' and 'major event'? In your response, please give detailed reasons for your answer.**

    - [No response.]

- **B5Q2 Do you agree with our proposed rule that requires market operators and participants to have plans for dealing with an incident or major event? If not, please give detailed reasons why you disagree.**

    - [No response.]

- **B5Q3 Do you agree with the frequency of reviewing and testing incident management and business continuity plans?**

    - [No response.]

- **B5Q4 Do you agree with the specific arrangements required in an incident management plan or business continuity plan?**

  - [No response.]

- **B5Q5 How will these proposed rules affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on incident management and business continuity arrangements.**

  - [No response.]

- **B6Q1 Do you agree with our proposal to introduce this rule to ensure adequate governance arrangements and resourcing? If you do not agree, please provide detailed reasons why you disagree.**

  - [No response.]

- **B6Q2 How will these proposed rules affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on governance arrangements.**

  - [No response.]

- **B7Q1 Do you agree with our proposal to introduce this rule to ensure fair access to the market? If you do not agree, please provide detailed reasons why you disagree.**

  - DTCC strongly supports this proposal. We believe that this will benefit the Australian market. Our clearing and settlement subsidiaries are subject to a requirement to establish, implement, maintain and enforce written policies and procedures reasonably designed to establish objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access[8]. We believe these rules have served to promote a highly efficient, competitive, dynamic, and innovative securities market in the United States and believe they could have a similar effect in Australian markets.
  - We are very encouraged by the forward-looking nature of the rule, especially as it anticipates its scope of application to new market operators, regardless of their technology platform. Regulations applicable to market operators of traditional securities should also be

[8] See Rule 17Ad-22(e)(18) of the Standards for Covered Clearing Agencies, https://www.govinfo.gov/content/pkg/FR-2016-10-13/pdf/2016-23891.pdf

applicable to innovative platforms. We would encourage ASIC to further consider the legal and other requirements applicable to innovative market operators based on the functions they may intend to perform and the risk they may pose. These risks may include custody risk, principal risk, and operational risk. Regulatory principles developed by international standard setting bodies, such as the "Principles for financial market infrastructures," or PFMIs, may serve as useful guidance. These principles can help market participants and other stakeholders identify the relevant responsibilities[9].

- **B7Q2 How will this proposed rule affect your business? If you are a market operator, please provide an estimate of the time and costs to implement this fair access rule.**

  - [No response.]

[9] See Guiding Principles for the Post-Trade Processing of Tokenized Securities, http://www.dtcc.com/~/media/Files/Downloads/WhitePapers/Crypto-Asset-Whitepaper-2019.pdf