Updated TMPG Best Practice Recommendations Related to Operational Resiliency

III. MAINTAINING A ROBUST CONTROL ENVIRONMENT, RISK MANAGEMENT

Best Practice # 12 (formerly Best Practice #11). Market participants should recognize that in light of the interconnectedness of systems and operations, market participants have a shared interest in and responsibility to collaborate to mitigate and resolve cyber risk and disruption that could have a systemic impact on market participants, and/or their service providers, such as counterparties, funding providers, data providers, trading venues, or clearing and settlement services. Since external cyber risk is faced by all market stakeholders, market participants should engage with both industry and official sector efforts to mitigate and manage such risks. This includes, but is not limited to, participation in industry-wide testing initiatives, facilitating resumption of operations, certification of reconnection to cyber affected systems, and centralized communication with respect to the same. All market participants, including service providers, should develop written protocols to determine when it is appropriate to safely reconnect with those impacted by a cybersecurity incident. In addition, cyber risk is also an internal risk that market participants should address and mitigate based on the nature of their market operations and engagement, and market participants are encouraged to perform regular internal testing and periodic reviews of their respective systems to ensure alignment with operational and security procedures.

Best Practice # 13. Market participants should plan for a potential lack of access to service providers, such as counterparties, funding providers, data providers, trading venues, and clearing and settlement services, and manage the associated risk. All market participants, including service providers, should develop their own written contingency plans, given the potential loss of access to service providers. At a minimum, such contingency plans should consider single points of failure, alternative backup providers, concentration risk, and fourth-party downstream reliance, and should account for both potential sudden intraday loss of access and more extended disruptions and outages. Market participants are also encouraged to periodically test their contingency plans. All market participants should, in a manner commensurate with their level of risk and volume in the market, be aware of the potential for the loss of access to service providers, and understand their related contingency plans.

III. MAINTAINING A ROBUST CONTROL ENVIRONMENT, INTERNAL CONTROLS

Best Practice # 8. Market participants, including service providers, such as data providers, trading venues, and clearing and settlement services, should ensure that they employ a robust change control process for designing, testing, and introducing new trading technologies, algorithms, risk systems, order types, or other potentially impactful system features or capabilities. Changes to market participants' written processes and procedures should promote market integrity and should consider, prior to implementation, behavior and market impact that these changes may foster. Market participants, including service providers, should also evaluate the potential consequences of an operational disruption to their systems, including liquidity or credit counterparty exposures, that could result in a wide range of scenarios (both intraday and more extended) — especially if a trading counterparty relies on the high use of intraday liquidity and credit that is implicit in high-gross, low- net trading activity. Market participants, including service providers, should adopt written policies and procedures identifying the types of changes that must be vetted and ensuring that such changes are vetted with appropriate representatives from support areas such as compliance, risk, and operations. Such processes should be reviewed on a regular basis for ongoing compliance.