office@ccp12global.com

5F No.55
Yuanmingyuan Rd.
Huangpu District,
Shanghai, China

CCP BEST PRACTICES THIRD-PARTY RISK MANAGEMENT

-

A CCP12 POSITION PAPER

July 2019

TABLE OF CONTENTS

ABOUT CCP12

CCP12 is a global association of 37 members who operate more than 60 individual CCPs globally across EMEA, the Americas and the Asia-Pacific region. CCP12 aims to promote effective, practical and appropriate risk management and operational standards for CCPs to ensure the safety and efficiency of the financial markets it represents. CCP12 leads and assesses global regulatory and industry initiatives that concern CCPs to form consensus views of its members and seeks to actively engage with regulatory agencies and industry constituents through consultation responses, forum discussions and position papers

In an effort to share with the broader industry the lessons learned, CCP12 has, and will continue to, publish papers of significance on core subjects concerning the industry. Recent noteworthy publications include a white paper published in December 2018, "*CCP12 Primer on Initial Margin – A CCP White Paper*"[1], a report published in February 2019, "*Incentives for Central Clearing and the Evolution of OTC Derivatives – A CCP12 Report*"[2] and a position paper published in May 2019, "*CCP Best Practices – a CCP12 Position Paper*"[3]. Continuing these contributions to the industry is critical considering that even longtime industry participants may not be fully aware of key concepts within the CCP space. In order to remedy this, CCP12 is publishing this paper to clearly elaborate on several core principles within central clearing and best practices that have been developed across the industry during the past years. We firmly believe that these best practices that have been developed prove ever increasing levels of resiliency to not only the individual CCPs, but the global markets at large.

It should however be made clear that this paper is not intended to and does not attest to any particular CCP and its individual practice but represents a general consensus view on certain subject matters without prejudicing individual CCP variances. CCPs are not "one-size-fits all" and it's important to recognize differences due to market, regulatory environment and other legal concerns, ownership structures, operational preferences, and other factors. Therefore, this paper and its best practices serves the intended purpose of providing a high-level educational tool to the industry on certain positions CCPs currently can agree on noting that measured variations may exist for the aforementioned reasons.

[1] http://ccp12.org/wp-content/uploads/2018/12/CCP12_White_Paper_Primer_on_Initial_Margin.pdf

[2] http://ccp12.org/wp-content/uploads/2019/02/INCENTIVES-FOR-CENTRAL-CLEARING-AND-THE-EVOLUTION-OF-OTC-DERIVATIVES-A-CCP12-REPORT_FINAL.pdf

[3] https://ccp12.org/wp-content/uploads/2019/05/CCP-Best-Practices__CCP12_Position_Paper.pdf

EXECUTIVE SUMMARY

CCPs enter into relationships with a wide range of domestic and foreign third-parties to outsource entire functions, interact directly with customers, address deficiencies in operations/compliance, leverage emerging technologies etc. In the interest of leveraging emerging technologies, CCP delivery model is moving increasingly from traditional in-house delivery methods to more complex supply chain models that require specialized skills and resources (for instance, skills to support increasing use of artificial intelligence, blockchain etc.). This increases the need for better oversight of the third-parties utilized. CCP12 recognizes that if such third-parties do not have proper risk oversight and controls in place, a CCP could be exposed to increased fiscal, operational, regulatory or reputational risks.

In that light, CCP12 believes it is best practice that CCPs adopt oversight and risk management processes that are commensurate with the level of risk and complexity introduced by its third-party relationships and the overall CCP organizational structure. Adopting appropriate risk management best practices will allow the CCP to identify, manage and monitor risks associated with the use of third-parties.

CCP12 supports that an effective third-party risk management process provides a framework for ongoing operationalized risk management for critical third-party service providers, follows a continuous lifecycle, reduces risk exposure and improves overall transparency around third-party relationships.

The remainder of this document outlines principles that a CCP may consider when adopting processes to manage third-party risks. The reader should note that this paper refers to Third-Party Risk Management Programs as a catch-all term to describe how a CCP may implement some or all of the outlined principles. Therefore, this paper is designed to provide a high-level educational tool to the industry on certain risk management practices of CCPs, noting that variations may exist for the aforementioned reasons.

PURPOSE OF THIRD-PARTY RISK MANAGEMENT PROGRAMS

A properly constructed and well-run third-party risk management program will reduce risks associated with the operational and commercial benefits that the third-party relationships bring to the CCP. With the third-party risk appropriately mitigated, the CCP can focus on driving the most value from the third-party relationship. A well-designed third-party risk management program provides simple, repeatable, reliable metrics for evaluating the risk levels of a CCP's third-parties. The program is useful during initial third-party selection, but it can also be used during contract renewals. Understanding and keeping up-to-date with a third-party's risk level allows the CCP to engage with third-parties with a proven track record of strong internal controls and data protection mechanisms, thereby reducing the total cost a CCP might spend on third-party maintenance, monitoring, and mitigation over the lifetime of the third-party contract.

A Third-Party Risk Management ("TPRM") Program's, (which may also be known as Vendor Management Program, or Vendor-Managed Services Program) objective is to identify, manage, and monitor risks posed by any third-party relationship to a Central Counterparty ("CCP"). Using this paradigm, the CCP is the first-party, its customers are the second-party, and its vendors or the external entities providing services to the CPP are the third-party.

Effective TPRM programs should be proactive in their risk management approach to third-parties with an aim to identify risks before they happen, and not just act on a reactive basis, as and when incidents or issues occur. This can become particularly important when third-parties become integral to the success of the CCP and pose a high enough risk that a third-party failure or a service disruption could severely impact the CCP's core functions. To manage this risk, the TPRM program assesses third-party risk and works with the business owners to implement sufficient risk controls or risk mitigation strategies prior to onboarding and then throughout the engagement with the third-party.

Effective third-party risk management is a necessity for all CCPs.

SCOPE OF THIRD-PARTIES RISK MANAGEMENT PROGRAMS

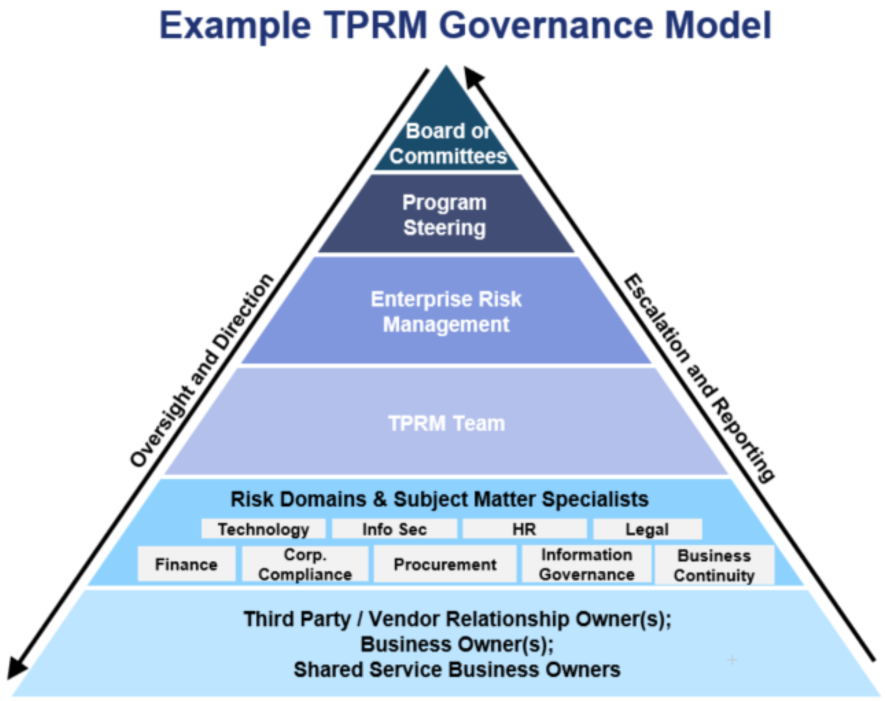
Most CCPs rely on products and services provided by a variety of third-party providers to outsource services, purchase products or engage consultants/contractors. Accordingly, each CCP should design and implement their own TPRM program in line with industry standards and regulatory expectations. This should include formalizing the program; including establishing a governance framework, reviewing procurement practices, formalizing policies and procedures to ensure that third-parties operate in a manner consistent with the CCP's business needs, obligations to its regulators, customers and shareholders and at a level commensurate with the CCP's approach to risk. Each CCP should consider the extent to which third-parties should be evaluated through TPRM or other functions within the CCP, including: affiliates, partner companies, charities, shared industry services, strategic investment companies, subsidiaries, and agents or agencies acting on the CCP's behalf.

As CCPs consider which third-parties need to go through due diligence, they may also need to identify a third-party's reliance on fourth parties. CCPs should consider the potential risks which may be found in their third-parties' reliance on fourth parties to conduct operations and perform services for the CCP.

TPRM PROGRAM FRAMEWORK AND GOVERNANCE

Each CCP should define how the TPRM program fits into its overall risk management strategy and risk appetite; specifically, how the TPRM program is governed, which key committees have the oversight of the CCP's TPRM activities, and who are the key risk owners and stakeholders.

Develop and Maintain a Formal TPRM Program Framework and Governance



(Figure 1)

The TPRM Governance Model example shown in Figure 1, illustrates one approach for how a TPRM program could be governed.

- The Board or Risk Committee would assist in defining and approving the company's risk appetite. Program Steering and/or Enterprise Risk Management ("ERM") programs would provide oversight of TPRM.
- The Program Steering and/or ERM programs would govern the ERM process relative to third-party relationships in a manner consistent with the CCP's goals and risk appetite. The Program Steering Committee could be made up of a cross-section of representatives from business units, risk management owners and subject-matter specialists. The governance framework should provide sufficient monitoring for significant performance and risk assessment deterioration in third-parties, with emphasis on the higher risk or essential/ critical third-parties. The TPRM team should collaborate with the ERM team and report upwards to the Board or its Committee(s) on a regular basis with respect to the ongoing third-party risks, with emphasis on third-party risks to essential/ critical business functions.

Develop and Maintain Formalized Governance Documents - The TPRM program should have formalized governance documents, which may include a policy, procedures, standards, and guidelines on how the TPRM program identifies, mitigates, monitors and reports on third-party performance and risk.

The governance framework and associated documents may consider the following areas:

- **Define the scope of the TPRM program** - This should include areas of applicability, and the high-level approach to third-party risk assessment management within the CCP
- **Define the roles and responsibilities of TPRM Stakeholders** - This should include groups and individuals responsible for, interacting with, or relying on the TPRM program
- **Define how Due Diligence would be conducted -** Once a CCP has determined which third-parties are in scope for due diligence, the framework should outline the level of due diligence that will be conducted for low risk third-parties vs. medium to high risk third-parties.
- **Define the scope of third-party risk assessments** - This should include the different types of risk assessments, and what standards the third-party is being measured against
- **Define risk finding (gap) management** - This should include defining what a finding is, how findings are managed, under what conditions the findings are escalated, and incorporate any compliance requirements
- **Define how ongoing risk monitoring would be conducted** - This should include details around how and in what frequency a third-party will need to be reassessed over time. This reassessment frequency should be more frequent, the higher the risk associated with the third-party
- **Define how performance management and oversight would be conducted** - This should include measurement of third-party performance against service delivery expectations (SLAs), establishing thresholds and monitoring the number of operational losses or incidents observed against the established thresholds. Third-parties that are high risk and more critical to the business should be regularly reviewed
- **Define TPRMs reporting obligations** - This should include regular reporting to the Program Steering, the Board or its committees.
- **Define Third-Party off-boarding activities** - This should include what actions need to take place when terminating a third-party

ASSESSING INHERENT RISK

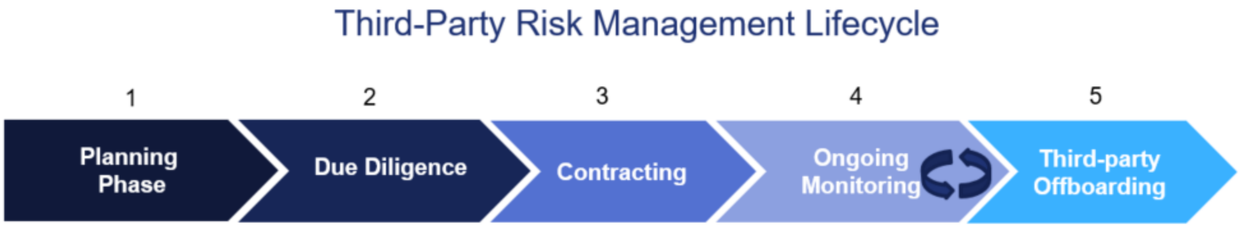
Since mature companies can have hundreds or thousands of third-parties, it can be more efficient for the CCP to define and assess the level of inherent risk posed by the third-party. Such risk assessments can be made for each individual third-party or for categories of third-parties. The level of risk will ultimately determine the amount of due diligence that needs to be performed, with high-risk third-parties subject to a more detailed due diligence process. An inherent risk categorization approach would add consistency to initial risk assessments, increase third-party onboarding efficiency, reduce subjectivity to specific third-party assessments, and more importantly, allows the TPRM team and its contributors to focus on third-parties that can pose more significant risks to the CCP (i.e. critical vendors).

The list below shows a selection of key risk indicators that a CCP may use to assess inherent risk:

- **Data Risk** - For the CCP to receive the service, does data need to be exchanged with the third-party? If so, what is the data? Could this data include personally identified information (PII), CCP financial data, or other confidential or proprietary data? Will the third-party store, transmit, process, generate or access confidential CCP data, networks or systems? Is the third-party capable of abiding by and assisting with data protection requirements?
- **Operational Risk** - What is the criticality of the good or service to the operations of the CCP? How long can the CCP operate without the third-party, without significant impacts?
- **Geographic Location Risk** - What is the geographic location where the third-party resides and / or operates? Is the country perceived to be a high risk country for corruption?
- **Physical / Logical Access Risk** - To provide the service, would the third-party require physical or logical access to the CCP? Where / what would the third-party have access to? Could this include any restricted areas or confidential data?
- **Regulatory Risk** - Would any third-party providing this service be required to adhere to any regulatory considerations or obligations?

THIRD-PARTY RISK ASSESMENT METHODOLOGY

The TPRM program's Third-Party Risk Management Lifecycle is frequently defined into five key phases as seen in Figure 2.



(Figure 2)

The lifecycle starts in the planning phase, where the business need is determined, and potential third-parties are identified. This lifecycle should continue through to the point-in-time where the service being provided by the third-party is no longer needed and the service and/or third-party needs to be off-boarded.

The third-party risk management lifecycle could include the following phases:

1. **Planning Phase** - During this phase, a business owner would qualify a business need and make a request to onboard a new third-party or to add services to an existing third-party. The inherent risk assessment will guide if additional information is required from the third-party, and if further, a third-party assessment is needed.

2. **Due Diligence Phase** - For third-parties where a determination is made that a due diligence is required, further information should be gathered from the business and the third-party. Some common due diligence and qualifying considerations include:
   - **Strategic Risk** - Is the third-party a strategic partner or is the third-party required for the CCP to meet any of their strategic objectives? Would a third-party failure jeopardize those objectives?
   - **Corporate and Legal Compliance Risk** - Does the third-party have the ability to meet local regulatory guidelines which the CCP is expected to be compliant? Does the third-party have a history of legal or compliance issues? Will some or all of the data be subject to General Data Protections Regulation (GDPR) compliance? Will the third-party be able to meet the CCP's internal compliance requirements? Additionally, during due diligence, some formal screenings

(World Check / Dow Jones) may be valuable or required, including screenings to identify potential risk of violating laws such as those promulgated by the Office of Foreign Assets Control (OFAC), Anti-money Laundering (AML), Foreign Corrupt Privacy Act (FCPA), or Modern Slavery Act (MSA).

- **Geo-political or Operating Location Risk** - Where does the third-party provide service or conduct business? Does this location(s) present additional risk to the CCP?
- **Financial Risk** - Is the third-party financially stable? Based on the type of third-party, is application of a credit assessment and credit monitoring methodology appropriate? Is ongoing monitoring of financial positions warranted? And if so, at what frequency? If financial or credit risk thresholds or limits are defined for the third-party, how are they monitored and escalated in case of a breach?
- **Transferability Risk** - How easy could the third-party be replaced if the third-party is no longer meeting business needs? Are there substitutes in the marketplace? Would the third-party migration activities introduce additional risk?
- **Information Security / Cybersecurity Risk** - What controls and capabilities are in place to protect the CCP's data, including back-ups? Additionally, how is the integrity of production data or back-up data protected during a service disruption or failover? Will the third-party connect to, or have access to the CCP applications or systems? If so, does the third-party have adequate controls with respect to non-public personal information, proprietary information, systems, data centers and infrastructure? What is the third-party's approach to cybersecurity? Does the third-party present unique cybersecurity risks or is there a negative history related to cybersecurity?
- **Information Governance and Data Privacy Risk** - What data is being exchanged with the third-party and is that data protected sufficiently to meet CCP, regulatory, or jurisdictional requirements?
- **Business Continuity Management Risk (BCM)** - Is the third-party providing services to support an essential business function? If so, does the third-party have a BCM strategy? Does that strategy meet the CCP's minimum standards? Are there considerations for pandemic planning? What is the frequency? Are the resources that performing testing independent?
- **Technology / Operational Risk** - Does the third-party have a proper process to manage change management, records retention and its sub-contractors etc.

During the due diligence phase, the TPRM team would usually collect due diligence evidence from the third-party, which may include: third-party risk questionnaires, policies and procedures, financial information, independent audit reports, security certifications etc. Each third-party's capabilities and controls should be measured against a set of minimum standards. These minimum standards should be based upon the CCP's own internal IT, security, and compliance standards.

At the completion of a third-party due diligence phase, the business owner, TPRM, and other vested risk owners should have a clear view of the risk posed by the third-party. The business owner may need to work with the third-party to remediate risks, work with legal to make modifications to the contract terms to further protect the CCP, or the business may choose to accept some, or all of the risk findings observed. Depending on the severity of any open risk findings identified, additional risk acceptance may also be valuable from other stakeholders. This may include: downstream business owners, compliance, data governance, business continuity, and information security leaders. In some circumstances, when the third-party does not meet minimum standards, it may be necessary to terminate further negotiations with the third-party prior to finalizing a contract.

3. **Contracting Phase** - The CCP and vested business owners may try and close or remediate risks during contracting phase. When possible, the CCP should leverage standardized contract templates to ensure there are appropriate contract protection clauses to help improve contract lifecycle efficiency and account for third-party's compliance with CCP's anti-corruption policies and practices and code of conduct. Additionally, the contract should consider adding service level expectations (SLA's), clauses protecting against any cybersecurity risk, data privacy needs, right to audit and inspect, right of termination in the case of breach of anti-corruption laws, an exit plan with respect to transfer and deletion of data and address any regulatory requirements. After the contract is finalized, any un-remediated or accepted risks should be logged in a central repository.

4. **Ongoing Risk and Performance Monitoring Phase** - Each CCP should maintain a third-party master list. The inventory of third-parties should identify those third-parties that are tied to critical business activities and introduce more risk. Ongoing risk assessments and third-party performance monitoring should be conducted in context with the risk and complexity of the services provided by the third-party. Ongoing risk monitoring could include for example risk questionnaires, on-site due diligence visits or other monitoring techniques.

   This phase includes:

- **Risk Monitoring** - Risk assessments should consider the criticality of the business functions supported by the third-party, impact to CCP's customers, access to sensitive information/ data/ system, financial condition, projected spend, regulatory jurisdiction and requirements and domicile of third-party corporate headquarters. Third-party risk segmentation should influence the ongoing monitoring needs for the specific third-party. As a guideline, high-risk third-parties should have a more thorough pre-engagement due-diligence, should be continuously monitored, and should be reassessed regularly. Lower risk third-parties would likely be reassessed less frequently and undergo a more limited risk reassessment. Ongoing oversight of third-party service providers would entail similar due diligence activities as listed in the due diligence phase above. The risk assessment results, findings, recommendations and all supporting documentation received from the third-party should be stored for future reference and a Governance, Risk and Compliance ("GRC") system could be useful in facilitating the same. On a regular basis, TPRM should advise appropriate governing bodies, including Program Steering and Board committees of third-party risks, especially those risks / issues tied to critical third-parties.

- **Performance Management and Oversight** - TPRM should monitor third-party performance and track performance management issues when they arise utilizing established performance metrics, if any. Third-party performance should be tracked in a risk-based manner and in context with the third-parties risk segmentation. A CCP may choose to use a scorecard, if it fits the CCP's risk framework and assign an overall grade/ rating to the third-party. A performance evaluation could include a review of performance against established SLA's, remediation noted during the performance assessment process, third-party's ability to meet contractual obligations, any service delivery issues, any issues or disputes noted and any communication related issues. Third-parties should be monitored for any negative media and regulatory actions. Additionally, oversight should include contingency and transition plan reviews.

5. **Third-Party Off-boarding Phase** - When the lifecycle with a specific service, or all of the services provided by the third-party concludes, the third-party should be assessed for any data retention obligations to meet business needs or regulatory obligations. Other off-boarding activities should be considered, including: data transfer deliverables, obtaining data destruction certifications (when applicable), and system access removals and contractual provisions for transitioning to an incoming third-party provider.

PROGRAM AND PROCESS EXCEPTIONS

There may be circumstances where the TPRM program processes are not appropriate or there are other compensating assessment processes in place to assess the risk. In those cases, the program or process exceptions should be documented appropriately.

- **Program Exceptions** - There may be program exceptions where an entire area of the business or specific services have been determined to be out-of-scope. For example, governmental agencies may be determined to be out-of-scope and no risk assessment will be performed. These exceptions should be documented in a formal governance document, such as a policy, or a program framework document.
- **Process Exceptions** - There may be instances where an alternative process to risk assess a third-party exists. For example: Joint Venture investments. These exceptions should be documented in a governance, guidelines document, or an exceptions log. There may be circumstances where the risk assessments procedures cannot be adhered to or are unattainable. In this case, process exceptions should be documented and approved.

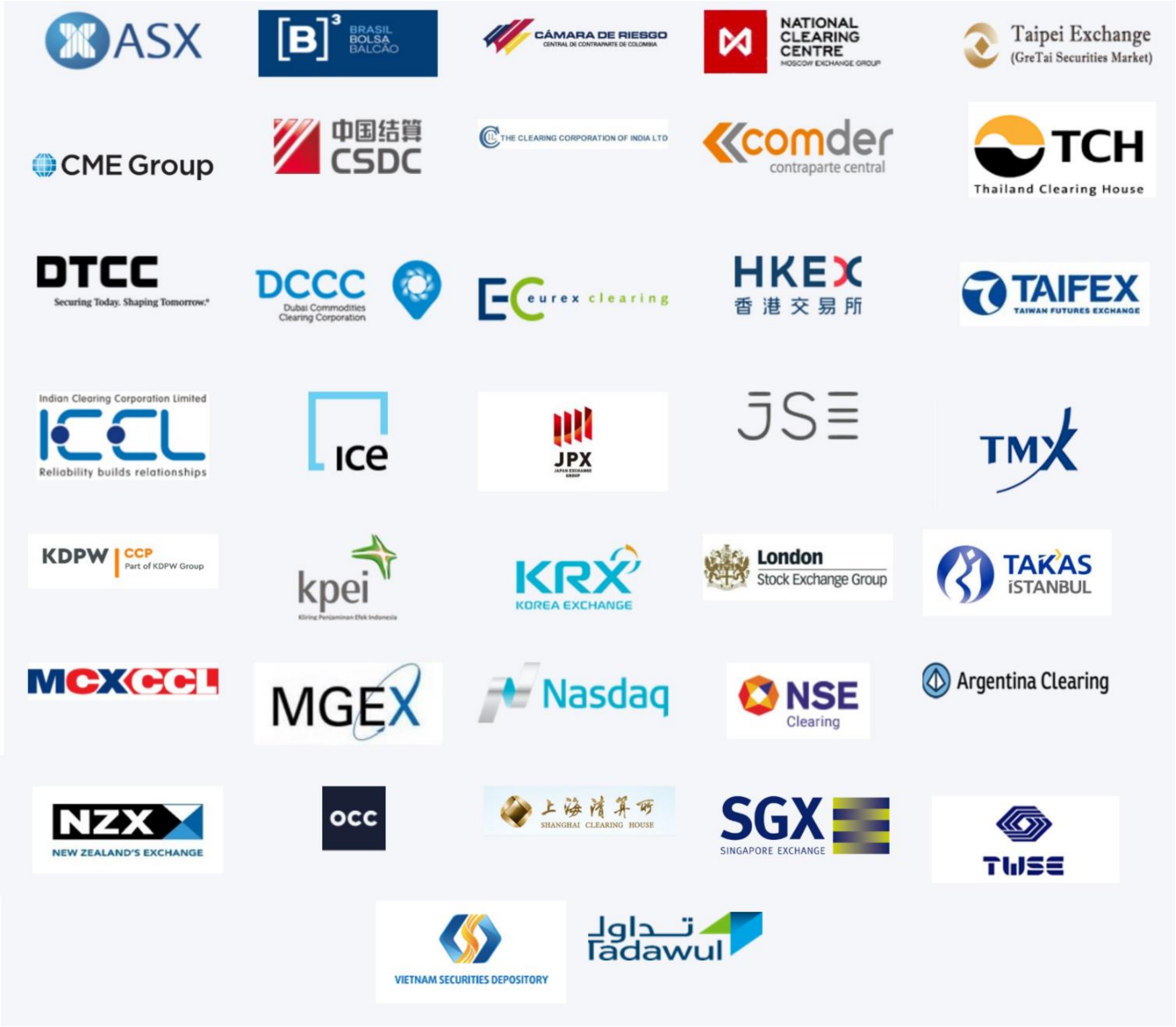
TRENDS AND FURTHER CONSIDERATIONS

- **Concentration Risk** - Concentration risk can be a concern if there is use of the same third-parties across the business. This should be monitored, and contingency plans put in place that could be executed should there be an issue with a highly concentrated third-party. Additionally, geographic concentrations can arise when a CCP's own operations and that of its third-parties and subcontractors are located in the same region or are dependent on the same critical power and telecommunications infrastructures.
- **Fourth-Parties** - Fourth-party risk management is a growing area in the TPRM discipline. Many third-parties use their own third-parties to fulfill services for their customers; these vendors are referred to as fourth-parties.
- **Software as a Service (SaaS) and Infrastructure as a Service (IaaS)** - Cloud and internet-based applications and services can be very effective from a business, financial, and operational efficiency perspective. However, these cloud third-parties can pose significant risk particularly if the third-party will be managing the CCP's data, processes, or infrastructure; particularly if the SaaS/IaaS third-party is instrumental to complete essential business functions. There should be

appropriate due diligence to ensure that expectations with regards to operational contract management, service levels and contract exit clauses are agreed upon upfront and that the third-party has the proper controls in place including ongoing third-party monitoring. This is particularly important as cloud providers tend to adopt a shared responsibility model with their customers for the operations and management of the security controls. This would ensure that the roles and responsibilities of the relevant IT and operations department are clearly understood, defined and contractually agreed before transferring any data into the cloud.

- **Shared risk/ reward models -** As internal organizational needs evolve and grow, to support continued growth and expansion, third-party relationships are becoming more symbiotic in nature and third-parties are transitioning from being traditional service providers to strategic/ business partners that leverage their wide breadth of skills and expertise, allowing organizations to focus on their core competencies.
- **Global and Regional Jurisdictional Considerations** - Some regions or countries present unique requirements or risks which TPRM may need to consider during the lifecycle of the third-party. These factors could add to the risk posed by a third-party, could encumber technology implementations, and should be considered during due diligence prior to procuring a third-party.
- **Third-Party Redundancy and Resiliency** - Resiliency and back-up plans should exist for critical / high-risk third-parties. This should include understanding the third-party's capabilities in this area. Additionally, back-up and failover plans may be necessary to prepare for any third-party service loss.
- **Financial Services Industry and CCP12 Collaboration on TPRM** - TPRM is a non-competitive advantage discipline. A controlled third-party risk environment helps protect the industry. The financial services industry including CCP12 may benefit from further discussions and collaboration in this space including harmonized third-party questionnaires and minimum control requirements for concentrated vendor exposures in the industry.

CCP12 MEMBERS


ASX
[B]3 BRASIL BOLSA BALCÃO
CÁMARA DE RIESGO CENTRAL DE CONTRAPARTE DE COLOMBIA
NATIONAL CLEARING CENTRE MOSCOW EXCHANGE GROUP
Taipei Exchange (GreTai Securities Market)
CME Group
中国结算 CSDC
THE CLEARING CORPORATION OF INDIA LTD
comder contraparte central
TCH Thailand Clearing House
DTCC Securing Today. Shaping Tomorrow.
DCCC Dubai Commodities Clearing Corporation
EC eurex clearing
HKEX 香港交易所
TAIFEX TAIWAN FUTURES EXCHANGE
Indian Clearing Corporation Limited ICCL Reliability builds relationships
ice
JPX JAPAN EXCHANGE GROUP
JSE
TMX
KDPW CCP Part of KDPW Group
kpei Kliring Penjaminan Efek Indonesia
KRX KOREA EXCHANGE
London Stock Exchange Group
TAKAS İSTANBUL
MCXCCL
MGEX
Nasdaq
NSE Clearing
Argentina Clearing
NZX NEW ZEALAND'S EXCHANGE
occ
上海清算所 SHANGHAI CLEARING HOUSE
SGX SINGAPORE EXCHANGE
TWSE
VIETNAM SECURITIES DEPOSITORY
تداول Tadawul

For further details please email office@ccp12global.com or visit www.ccp12.org.