Corporate Risk Management Policy

Effective Date:	12/22/2022
Approval:	Board of Directors

I. INTRODUCTION

The Options Clearing Corporation ("OCC") manages risks in accordance with regulations, industry standards, the OCC Rules and By-Laws, and OCC's Risk Management Framework. This Corporate Risk Management Policy details OCC's enterprise risk management approach, including activities to identify, measure, monitor, manage, report, and escalate risks to inform decision-making.

The Corporate Risk Management department ("Corporate Risk"), in conjunction with other departments in the first and second lines of defense, evaluates risks that may affect OCC's ability to promote stability and market integrity by providing effective and efficient clearance, settlement, and risk management services ("Services"). The risks listed in OCC's Risk Management Framework include financial, operational, information technology and security, legal and regulatory, and general business risks. Corporate Risk reports to the Chief Risk Officer ("CRO") who maintains independence by reporting to OCC's Board of Directors ("Board") Risk Committee.

II. RISK GOVERNANCE

The establishment and maintenance of OCC's risk universe, risk appetites, risk tolerances, and risk rating scales is facilitated by Corporate Risk and used across OCC to create a transparent means to manage risk. Corporate Risk establishes the risk universe which organizes OCC's risks into categories, sub-categories, and individual risk statements mapped to OCC's process universe. The risk categories and sub-categories are owned and approved by the CRO and provided to the Management Committee and Board. The Board oversees OCC's risk management by approving risk appetites which establish the type and amount of risk OCC is willing to accept and risk tolerances which establish thresholds to monitor risk within appetites. Risk rating scales provide an assessment of risk from an impact and likelihood perspective consistently across OCC. These risk rating scales are approved by the CRO and provided to the Management Committee and Board.

A. Risk Universe

Corporate Risk establishes OCC's risk universe to provide organized groupings of individual risks which become more detailed starting from risk categories down to individual risk statements. The risk universe is organized into three layers to classify and aggregate risks.

- Risk categories are the highest-level groups of risk aggregation.
- Risk sub-categories further classify risks within risk categories into detailed groups. Risk sub-categories are associated with a risk category.
- Risk statements are descriptions of the drivers, events, and consequences of risks. Risk statements are established and managed at the business process level by employees within OCC's business with the accountability and authority to manage the risk ("Risk Owner"). Risk statements are associated with a risk category and risk sub-category.

At least every twelve months, Corporate Risk determines whether updates to the risk universe are necessary to better align risk categories, sub-categories, and statements with OCC's Services. Risk category and sub-category updates are approved by the CRO while risk statements are approved by

Corporate Risk management. The Management Committee and Board are notified of updates to risk categories and sub-categories.

B. Risk Appetite

Risk appetite is the qualitative articulation of the amount of risk OCC is willing to accept and establishes expectations for OCC's risk management. At least every twelve months, risk appetites are established at a risk sub-category level and presented by the CRO to the Management Committee for recommendation to the Board for approval. Risk Owners manage the level of risk exposure posed by a process against risk appetites. Corporate Risk monitors risks to identify breaches of risk appetite. Risk appetite breaches are escalated by the CRO to the Management Committee, Risk Committee, and Board. Risk Owners, with input from relevant business areas, develop and execute risk treatment[1] plans to reduce risks that exceed OCC's risk appetites. At least every twelve months, Corporate Risk and Risk Owners review risk appetites and, where necessary, make adjustments to align with OCC's Services. The CRO reviews and presents changes to risk appetites to the Management Committee for recommendation to the Board for approval.

C. Risk Tolerances

Risk tolerances are qualitative or quantitative measures that help inform whether risks are within risk appetites. Risk tolerances are established at a risk sub-category level and presented by the CRO to the Management Committee for recommendation to the Board for approval. Risk Owners are responsible for managing applicable risks within established tolerances and developing risk treatment plans to resolve breaches of risk tolerance. Risk tolerance breaches are escalated by the CRO to the Management Committee, Risk Committee, and Board. At least every twelve months, Corporate Risk and Risk Owners review risk tolerances and, where necessary, make adjustments to align with OCC's Services. The CRO reviews and presents changes to risk tolerances to the Management Committee for recommendation to the Board for approval.

D. Risk Rating Scales

OCC's risk rating scales rate the magnitude of impact an event will have on a process and the likelihood an event will occur. The impact risk rating scale considers operational, internal financial, external financial, legal and regulatory, and reputational impacts. The likelihood risk rating scale considers a 10-year financial cycle and yearly corporate planning activities. These risk rating scales are used to measure inherent and residual risk at a risk statement level. Inherent risk is the level of risk exposure posed by a process absent any controls to reduce the likelihood or severity of an event. Residual risk is the level of risk exposure posed by a process or activity after the application of controls or other risk-mitigating factors. At least every twelve months, Corporate Risk and Risk Owners perform a review of the risk rating scales. The CRO reviews and approves changes to the risk scales. The Management Committee and Board are notified of changes to the risk rating scales.

III. RISK IDENTIFICATION AND MEASUREMENT

Corporate Risk identifies risks across OCC processes utilizing enterprise risk assessments and operational scenario analysis to measure current and emerging risks. The information gathered through the execution of enterprise risk assessments and operational scenario analysis is used to report against risk appetites.

[1] Risk treatment is the process to manage a risk through avoidance, mitigation, transference, or acceptance. See Section V, Risk Management.

A. Enterprise Risk Assessments

Enterprise risk assessments are a quarterly activity where the control environment is evaluated to determine its effectiveness in preventing or mitigating inherent risks identified to arrive at a residual risk rating for each risk statement. Corporate Risk maintains an inventory of all business processes, risks, and associated controls in a database used by OCC to manage Enterprise Governance, Risk and Compliance. Corporate Risk uses data from a variety of sources (e.g., risk events, Internal Audit findings, security risk assessments and observations, third-party observations, control design assessments, management control self-testing results, and business impact analyses) to rate the impact and likelihood of a risk associated to a process and assess the quality of the control environment. Enterprise risk assessments are conducted through workshops across the first and second lines of defense and are supplemented by including information from emerging risk surveys (top-down), process-based risk assessments (bottom-up), and enterprise technology assessments. Quarterly, the results of the enterprise risk assessment (the levels of residual risk) are aggregated and provided to the CRO for approval and presented to the Management Committee. The CRO then presents the enterprise risk assessment to the Board at its next regularly scheduled meeting.

B. Operational Scenario Analysis

Operational scenario analysis is the process of leveraging OCC subject matter expertise to identify potential operational risks and assessing the potential outcomes of stressed operations. Operational scenarios consider both internal and external scenarios that may impact OCC's ability to perform its Services. Corporate Risk, through workshops with the first and second lines of defense, designs operational scenarios utilizing available information (e.g. annual top-risk survey conducted by Corporate Risk, Management Committee recommendation, enterprise risk assessments). The workshops are designed to identify risks that may not have been previously uncovered or weaknesses in the current control environment. Operational scenarios are used to assess the potential that future extreme but plausible business disruptions may impact OCC's Services and are inputs in OCC's target capital requirements and recovery and wind-down planning. Corporate Risk includes potential risks identified through operational scenario analysis when analyzing and reporting across risk categories and sub-categories.

IV. RISK MONITORING

Corporate Risk and Risk Owners monitor internal and external risks to determine whether OCC's risk management practices operate effectively. The information gathered during this monitoring is used to inform enterprise risk assessments.

A. Key Risk Indicator Monitoring

Key risk indicators ("KRIs") are qualitative or quantitative metrics designed to identify changes to risks. Corporate Risk and Risk Owners utilizes KRIs to measure and monitor levels of risk against risk appetite and risk tolerances. KRIs are established at a risk sub-category level. KRIs include three thresholds: green, amber, and red. Green indicates a low risk of breaching tolerance, amber indicates a moderate risk of breaching tolerance, and red indicates a breach of tolerance. Amber and red thresholds are points of escalation to the CRO, Management Committee, and Board.

Risk Owners, in collaboration with Corporate Risk, develop KRIs by considering business (e.g. process and controls) and regulatory requirements. Corporate Risk facilitates identifying, modifying, and reviewing KRIs with a designated Management Committee member, including defining and reviewing the risk tolerance and risk thresholds for the KRI. KRIs that breach the red threshold result in the development

and execution of risk treatment plans by Risk Owners. Quarterly, Corporate Risk reports against red, amber, and green thresholds to the CRO and Management Committee. Corporate Risk also reports against red, amber, and green thresholds to the Board at each regularly scheduled meeting.

B. Operational Risk Event Monitoring

An operational risk event is an event which results in a financial loss, an adverse impact to OCC or its ability to deliver its Services. Such events arise from failed or inadequate internal processes, people, systems, or exposure to external events. Risk Owners are responsible for identifying, assessing, and escalating operational risk events. Quarterly, Corporate Risk is responsible for ensuring that material operational risk events are reported to the CRO and Management Committee, as well as identifying any trends. Corporate Risk also reports risk events and any identified trends to the Board at each regularly scheduled meeting. Risk Owners perform root cause analysis and enhance or develop processes and controls, that would reduce the impact or likelihood of similar events occurring in the future. Risk Owners are responsible for escalating operational risk events causing serious and extended disruptions in production operations. Risk events which have a major or extreme impact to OCC's ability to perform its Services are immediately reported to the Management Committee and Board..

V. RISK TREATMENT

Risk Owners manage risk exposures by utilizing risk treatment methods to remain within risk appetites and tolerances. Risk treatment methods are implemented by Risk Owners and include the decision to mitigate, avoid, transfer, or accept an identified risk.

Mitigation is a risk treatment method where controls including policies, procedures, processes, and systems are implemented to manage a risk within established risk appetites and tolerances (e.g. OCC creates a procedure to document a process, including implementing controls to mitigate a risk). The second line provides oversight to the activities implemented by executing programs and reviews to assess the design and operating effectiveness of these items.

Avoidance is a risk treatment method that may be used when controls are ineffective at preventing or mitigating a risk within approved risk appetites or tolerances (e.g. OCC does not onboard a clearing member due to poor financial health).

Transference is a risk treatment method where risks are moved to a third party usually through the purchase of insurance (e.g. fraud, general liability, and employment insurance). Insurance coverage is coordinated by the Corporate Finance team, with involvement from other first and second line stakeholders, and subject to review by the Management Committee and the Board.

Acceptance is a risk treatment method that may be used to acknowledge when the cost or complexity of avoiding, mitigating, or transferring the risk exceeds the potential impact (e.g. OCC accepts a risk temporarily and implements short-term mitigants, knowing that a long-term solution is planned). Corporate Risk evaluates risk acceptances submitted by Risk Owners. Any risks presented for acceptance that are outside of risk appetite or risk tolerance must be approved by the Management Committee annually. Corporate Risk reports on risks accepted above approved risk appetite or risk tolerance to the CRO, Management Committee, and Board.

VI. RISK REPORTING, ESCALATION, AND TRAINING

Corporate Risk reports and escalates risks to the CRO, Management Committee, and Board and trains employees about risk and control to support risk management and decision-making.

A. Reporting

Risk reporting provides a view of OCC's risks to facilitate risk management and inform decision-making. Corporate Risk reports risks based on its risk identification, measurement, and monitoring activities to assist in the understanding of the risks OCC faces and whether these risks are being managed within OCC's risk tolerances and appetites. Quarterly, the CRO reports risks (e.g. risk appetite or risk tolerance breaches, material operational risk events, summary of risk acceptances, and risk mitigation) to the Management Committee. The CRO also reports risks to the Board and relevant Board committees at each regularly scheduled meeting.

B. Escalation

OCC employees are responsible for escalating risks through timely identification and reporting. In accordance with OCC's Employee Handbook and Policy Governance Policy, OCC employees are expected to escalate risks through their reporting line, OCC's internal working groups, Corporate Risk, OCC's hotline or to the Management Committee. Quarterly, Corporate Risk, through the CRO, escalates breaches of risk appetites and risk tolerances to the Management Committee. The CRO escalates breaches of risk appetites and risk tolerances to the Board and relevant Board committees at each regularly scheduled meeting. Escalation occurs (i) consistent with obligations established in the Management Committee Charter, Board Charter, Board Committee Charters, policies, and procedures, or (ii) or anytime through the CRO directly to the Board.

C. Training

OCC employees are trained to promote a culture of risk and control awareness. Corporate Risk collaborates with other OCC departments to create and disseminate training to enable accountability, empower decision-making, promote risk awareness, and detail escalation. This training promotes awareness of OCC's regulatory requirements, policies, procedures, processes, controls, and standards of conduct.