SUBMISSION COVER SHEET

***IMPORTANT*: Check box if Confidential Treatment is requested** □

Registered Entity Identifier Code (optional): 23-233

Organization: Chicago Mercantile Exchange Inc. ("CME")

Filing as a: □ **DCM** □ **SEF** ☒ **DCO** □ **SDR**

Please note - only ONE choice allowed.

Filing Date (mm/dd/yy): 06/14/23 Filing Description: Notification to the Commission Regarding the Migration of Clearing and Settlement Systems to the Google Cloud Platform

SPECIFY FILING TYPE

Please note only ONE choice allowed per Submission.

Organization Rules and Rule Amendments

□	Certification	§ 40.6(a)
□	Approval	§ 40.5(a)
□	Notification	§ 40.6(d)
☒	Advance Notice of SIDCO Rule Change	§ 40.10(a)
□	SIDCO Emergency Rule Change	§ 40.10(h)

Rule Numbers:

New Product **Please note only ONE product per Submission.**

□	Certification	§ 40.2(a)
□	Certification Security Futures	§ 41.23(a)
□	Certification Swap Class	§ 40.2(d)
□	Approval	§ 40.3(a)
□	Approval Security Futures	§ 41.23(b)
□	Novel Derivative Product Notification	§ 40.12(a)
□	Swap Submission	§ 39.5

Product Terms and Conditions (product related Rules and Rule Amendments)

□	Certification	§ 40.6(a)
□	Certification Made Available to Trade Determination	§ 40.6(a)
□	Certification Security Futures	§ 41.24(a)
□	Delisting (No Open Interest)	§ 40.6(a)
□	Approval	§ 40.5(a)
□	Approval Made Available to Trade Determination	§ 40.5(a)
□	Approval Security Futures	§ 41.24(c)
□	Approval Amendments to enumerated agricultural products	§ 40.4(a), § 40.5(a)
□	“Non-Material Agricultural Rule Change”	§ 40.4(b)(5)
□	Notification	§ 40.6(d)

Official Name(s) of Product(s) Affected:

Rule Numbers:

CME Group

Christopher Bowen
Managing Director & Chief Regulatory Counsel
Legal Department

June 14, 2023

VIA ELECTRONIC PORTAL

Mr. Christopher J. Kirkpatrick
Office of the Secretariat
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

Re: CFTC Regulation 40.10(a) Advance Notice. Chicago Mercantile Exchange Inc.'s Notification to the Commission Regarding the Migration of Clearing and Settlement Systems to the Google Cloud Platform.
CME Submission No. 23-233

Dear Mr. Kirkpatrick:

Pursuant to Commodity Futures Trading Commission ("CFTC" or "Commission") Regulation 40.10(a), Chicago Mercantile Exchange Inc. ("CME" or "Clearing House"), a derivatives clearing organization ("DCO"), submits this advance notice that CME will migrate the systems supporting its clearing and settlement functions to a cloud-based infrastructure hosted on the Google Cloud Platform ("GCP").

The purpose of this notification is to alert the Commission of the material change in connection with the proposed migration, as more specifically described in Appendix A below, to its operation. There is no correlating rule change to this operation change.

CME reviewed the DCO core principles ("Core Principles") as set forth in the Commodity Exchange Act ("CEA" or "Act") and identified that the following Core Principle may potentially be impacted:

- **DCO Core Principle I – System Safeguards**: CME has expanded and adapted its program of risk analysis and oversight to incorporate and cover its GCP-hosted operations and automated systems. CME has designed the migration to meet its obligations under the CFTC's System Safeguards requirements and will conduct tests and reviews to gain assurances that CME has effectively executed these designs.[1]

Pursuant to Section 5(c) of the Act and CFTC Regulation 40.10(a), CME certifies that the proposed migration complies with the Act and regulations thereunder. There were no substantive opposing views to the proposal.

Notice of this submission has been concurrently posted on the CME Group website at http://www.cmegroup.com/market-regulation/rule-fillings.html.

[1] *See Infra* § III.

Should you have any questions concerning the above, please contact the undersigned at (212) 299-2200 or christopher.bowen@cmegroup.com.

Sincerely,

/s/ Christopher Bowen
Managing Director & Chief Regulatory Counsel

Attachment: Appendix A – Description of Proposed Migration

APPENDIX A

The Clearing House operated by Chicago Mercantile Exchange Inc. ("**CME,**" "**CME Clearing**," or the "**Clearing House**"), in its capacity as a registered derivatives clearing organization ("**DCO**") and a systemically important DCO ("**SIDCO**"),[1] hereby provides advance notice to the Commodity Futures Trading Commission ("**CFTC**" or the "**Commission**") that it intends to migrate the systems supporting its clearing and settlement functions to a cloud-based infrastructure hosted on the Google Cloud Platform ("**GCP**"). CME is a wholly owned subsidiary of CME Group Inc. ("**CME Group"** or the "**Company**"). This modernization effort will support CME evolving its system performance, operational resiliency, cybersecurity, and capacity, for itself, its clearing members, and the broader industry.

I. Background

a. Overview

CME has built and maintains its infrastructure with a focus on creating high-capacity, secure, redundant systems that meet CFTC regulatory requirements and industry best practices. These systems have successfully and reliably supported CME's clearing operations through ever-increasing volumes, spikes of capacity demands, and evolving cybersecurity threats. With an eye towards the future and recognizing the profound technology advances in cloud-computing, CME has entered into a ten-year agreement with Google LLC ("**Google**"), through which it will further modernize and migrate its technology infrastructure to GCP. Google has made a long-term commitment to CME, which is reflected in the terms of the 10-year agreement.[2] The migration to GCP is part of CME's natural technology progression and will further evolve its already robust technology infrastructure.

One of CME's aims with the GCP migration is to further enhance the security and reliability of clearing and settlement systems by taking advantage of GCP's expansive global and resilient infrastructure, data centers, and support. Additionally, CME seeks to take advantage of GCP's elastic capacity to meet increasing demands on CME's technology systems. This cloud-based infrastructure will allow CME to increase its use of automation tools and enable CME to use development and testing environments in a more efficient manner than in on-premise infrastructures. Collectively, these capabilities will enable CME to accelerate its pace of developing and deploying innovative, resilient, and secure systems.

Importantly, the migration to GCP will further enhance CME's ability to address the cybersecurity threat landscape facing CME as a systemically important financial institution. CME is confident in the strength and maturity of its information security programs, but also recognizes that security capabilities and standards must continue to advance as threats evolve. Through this migration, CME will collaborate with Google to develop cloud architecture standards and deploy cloud-native tools to support, enhance and continually scale CME's security capabilities. The migration will allow CME to automate more controls, increasing both coverage and effectiveness, and streamline efforts such as vulnerability and patch management across environments. The partnership between security experts at CME and Google, each with their respective domain knowledge of the financial sector and globally scaled systems, will position CME to implement security at the speed and scale necessary to address risks to CME's systems and enhance the overall security posture of CME.

This Advance Notice provides information about how CME has designed and is executing this migration to meet its goals of deploying safe, secure, and resilient infrastructure in GCP. The Advance Notice covers the following:

[1] On July 18, 2012, Chicago Mercantile Exchange Inc. was designated as a systemically important financial market utility under Title VIII of the Dodd-Frank Act.

[2] CME has separately submitted a request for confidential treatment to the CFTC regarding the agreements with Google, which CME has provided in confidential Exhibit A to File No. 23-233.

- **Governance:** The Advance Notice begins by describing the governance structures CME Group and CME Clearing have established to oversee this migration effort. This includes information related to the roles of the CME Group Board and its Committees, as well as the involvement and leadership of the Senior Management Team of the Clearing House.
- **Third Party Risk Management and Global Assurance:** Next, we describe the role of CME Group's Third Party Risk Management Program ("**TPRM**"), as a second line of defense, as well as Global Assurance, as a third line of defense.
- **GCP Migration Framework**: The Advance Notice then covers the framework by which CME will execute this migration, including the establishment of the foundational cloud-based platform, as well as the process by which applications will migrate to this platform.
- **System Safeguards Compliance**: The Advance Notice will further provide a detailed description of how CME will continue to meet its regulatory obligations and extend its program of risk analysis and oversight with respect to its operations and automated systems to cover its GCP-hosted infrastructure both during and following the migration.
- **Clearing Member and Third Party Engagement**: Finally, the Advance Notice will address planned engagement with Clearing Members and other third parties during this transition.

b. Governance

The CME Group and CME Boards of Directors (collectively, the **"Board"**)[3] have an active role, as a whole and at the committee level, in overseeing management of CME Clearing's risks, including operational risks that impact the safety and efficiency of CME Clearing. The overall risk management of CME Clearing is governed by the Board, which is supported by committees and individuals with powers delegated by the Board, including the Risk Committee, Clearing House Oversight Committee ("**CHOC**"), CME Clearing Risk Committees, and certain members of the Senior Management of CME Clearing.[4] Committees with powers delegated by the Board play an active role in the risk management of CME Clearing and keep the Board apprised of CME Clearing's activities.

GCP does not alter these oversight responsibilities. CME understands the significance of the migration to GCP and the importance of designing reporting processes to the Board and its Committees that provide information on the strategies, risks, challenges, and successes relating to the operations of CME Clearing. The Clearing House and key stakeholders (e.g., Global Information Security, TPRM, Enterprise Risk Management**,** and Operational Resilience) will continue to provide information to the Board, the Risk Committee, and CHOC regarding the safety and efficiency of the Clearing House and its risk profile, as impacted by the migration to GCP, and will seek approval of certain aspects of the migration as required by the Clearing House's established governance framework.

i. Board and Risk Committee Oversight through ERM Program

CME Group's Enterprise Risk Management ("**ERM**") program will support the aggregated reporting of relevant GCP migration information to management, the Board, and relevant committees, in coordination with the Office of the Secretary and program leaders. CME Group's ERM program is designed to identify events that may affect the enterprise, manage and report on the associated risks and opportunities, and provide reasonable assurance that risks are managed in accordance with the company's risk appetite and business objectives. The ERM function's mission is to apply a holistic and systematic approach to identifying, assessing, managing, and monitoring threats and opportunities at CME Group, including compliance, financial, clearing house, operational, reputational, and strategic and commercial. Key elements of the ERM Program are the Enterprise Risk Management Framework ("**ERMF**"), the Statement

[3] The CME Group and CME Boards of Directors are comprised of the same individuals.

[4] The "Senior Management of CME Clearing" is comprised of the Global Head of Clearing & Post-Trade Services and those individuals that report directly to the Global Head of Clearing & Post-Trade Services, with the exception of the Head of the Financial and Regulatory Surveillance department. The Senior Management of CME Clearing is described in greater detail below.

of Risk Appetite (**“SRA”**), the Company’s risk universe, the quarterly risk assessment process by designated risk owners and the quarterly reporting process in the Enterprise Risk Profile Report (“**ERPR**”).[5]

CME Group leverages its ERM program and framework and CME Group’s other second line functions to identify and monitor the risks related to the GCP migration across CME Group’s risk universe through the quarterly risk assessment process. Results are compiled and collated within Appendix C of the ERPR, which is a distillation of quarterly risk information provided by risk owners throughout the Company, including risks related to the GCP migration that could impact the risk profile of the Company. The quarterly risk assessments that support the ERPR includes details regarding, risks, responses, and opportunities related to GCP.

The ERM team provides the ERPR to the Management Team, the Risk Committee, and the Board on a quarterly basis. The ERM team also provides verbal updates on the ERPR to the Risk Committee, and the Risk Committee Chair provides a report to the Board. The Risk Committee also receives information about the GCP migration efforts from the Chief Enterprise Risk and Compliance Officer, the Managing Director of Operational Resilience and Global Security, and the Chief Information Security Officer (“**CISO**”), as appropriate, as well as other key leaders responsible for the initiative.

The Risk Committee, which is comprised entirely of Board Members, has had a long-standing role in overseeing CME Group’s program of risk analysis with respect to its operations and automated systems to identify and minimize sources of operational risk. Certain members of the Risk Committee have experience related to technology and operations, which has been further honed by their experience overseeing the Global Information Security (“**GIS**”), Operational Resilience, ERM, and TPRM programs. Risk Committee members also have access to outside advisors to supplement their experience and expertise.

ii. Clearing House Oversight Committee

The CHOC Charter[6] provides CHOC with the authority to approve this Advance Notice and refer the changes contemplated in it for approval by the Board, pursuant to the below:

- *The Committee shall review and approve any changes to core processes and core systems for the Clearing House that significantly impact the risk profile of the Clearing House and refer such changes to the Board for approval.*

CHOC is comprised entirely of Board members. The day-to-day activities of the Clearing House are led by the Senior Management of CME Clearing under the guidance and purview of CHOC and other committees of the Board.

CHOC is responsible for determining if a matter would have a significant impact on the risk profile of the Clearing House and thereby require the approval of the full Board, including in relation to the GCP migration. Where such a conclusion is reached by CHOC, the matter is deemed to constitute a major decision of the Clearing House. The Global Head of Clearing & Post-Trade Services, Chief Risk Officer of the Clearing House, and Chief Compliance Officer of the Clearing House, collectively, are responsible for making a recommendation to CHOC as to whether a matter would have a significant impact on the risk profile of the Clearing House in accordance with CME Group’s Statement of Risk Appetite, including providing appropriate support for their recommendation.

At the April 3, 2023, meeting of the CHOC, members of the Senior Management of CME Clearing presented to CHOC regarding GCP developments and planned migrations of CME Clearing applications and databases, including notification of the planned migration of the Banking & Asset Management System

[5] CME has separately submitted a request for confidential treatment to the CFTC regarding the Enterprise Risk Management Framework, the Statement of Risk Appetite, and the Risk Universe, which CME has provided in confidential Exhibit B to File No. 23-233.

[6] The CHOC Charter can be found on CME Group’s public website: http://investor.cmegroup.com/static-files/16d6afbf-c684-41eb-ad3f-2abf91234717.

(“**BAMS**”). Additionally, CHOC reviewed and approved this regulatory filing at their May 2, 2023, meeting and had the opportunity to discuss GCP migration further with members of the Senior Management of CME Clearing. The CHOC determined that the 40.10 filing should be submitted to the Board for approval. The Board received a draft of the Advance Notice ahead of its May meeting, and on May 3, 2023, approved the 40.10 filing.

iii. Other Board Committee Oversight Responsibilities

Information regarding the strategies, risks, challenges, and successes relating to the GCP migration will be regularly communicated to the Board and its Committees in accordance with their roles. For example, the Board will receive updates on the overall status of the GCP migration efforts. And the Audit Committee is informed of the results of audits, including any internal audits relating to the collaboration with Google.

iv. GCP Program

CME has organized the overall migration effort into a Google Cloud Transformation Program (the “**GCP Program**”).[7] The GCP Program owner is CME Group’s Chief Transformation Officer, who reports to the Chairman and Chief Executive Officer. Through the GCP Program, CME and its management, subject to the oversight of the CME Group Board and its Committees as appropriate, provide decision making and direction in relation to the GCP Program, and retain sole responsibility for all decisions related to the GCP Program that impact CME Group’s strategic priorities and regulatory compliance, including, but not limited to, those priorities related to systems, operations, and risk management. Such decisions are subject to governance of the organization, including the oversight and approval responsibilities of CHOC and compliance with the established Statement of Risk Appetite.

The GCP Program is governed by a Steering Committee (“**GCP Program Steering Committee**”). This committee oversees the overall GCP Program, sets strategic priorities for the execution of the GCP Program, and provides clarity and alignment on direction. The GCP Program Steering Committee consists of senior leaders from CME Group and Google, including CME’s Chief Operating Officer, and Global Head of Clearing & Post-Trade Services. The Steering Committee’s roles and responsibilities include (but are not limited to) driving resolution of risks through consultation with subject matter experts (consistent with the Statement of Risk Appetite set by the Board) and reviewing general performance, program progress and any changes.

v. Clearing House Management Oversight

Throughout the migration to GCP, the Senior Management of CME Clearing has been kept up-to-date and has assigned members of their own respective teams to support a smooth GCP transition for core processes or systems that are scheduled for migration. This team will continue to oversee the GCP-hosted systems once migration is complete.

The Senior Management of CME Clearing is comprised of individuals that possess the necessary skills and experiences in the derivatives industry and more granularly, in the area for which they maintain primary oversight. Further, all members of the Senior Management of CME Clearing are expected to demonstrate the highest level of integrity in performing their roles, including leading critical functions of CME Clearing. Collectively these functions are under the oversight of the Global Head of Clearing & Post-Trade Services, to whom all members of the Senior Management of CME Clearing have a direct reporting line.

The Senior Management of CME Clearing has been delegated the authority, per CME Group’s Commitment and Signing Authority Policy – Appendix D, to select Clearing Members, customers, and other appropriate stakeholders for consultation based on the nature and scope of impact of a major decision in a manner consistent with the Board’s governance objective to consider the legitimate interests of Clearing Members

[7] CME has separately submitted a request for confidential treatment to the CFTC regarding the Google Cloud Transformation Program Charter, which CME has provided in confidential Exhibit C to File No. 23-233.

and their customers.[8] Discussions with and feedback received from relevant stakeholders are fairly considered by CME Clearing, documented within the Clearing House's records relating to such major decision, and maintained in accordance with CME Group's Information Governance program.

The migration of CME's clearing systems to GCP will not impact CME's control and authority over its clearing and settlement functions. Nor will the migration change any of CME's underlying financial risk management best practices or principles. The authority of Senior Management of CME Clearing over the application of risk management best practices and the Board's and CHOC's oversight responsibilities for all clearing functions will remain unchanged.

c. Third Party Risk Management Program

To meet CME Group's third party risk management regulatory and business objectives, the Company follows its TPRM Program, which established and maintains the framework by which the Company identifies, manages, and monitors risks resulting from its reliance upon outside parties that the Company has engaged to provide products and services to the Company or on the Company's behalf (referred to as "**third parties**"). TPRM monitors third parties who present moderate to critical risk throughout their engagement lifecycle.

TPRM maintains a risk-based approach for the identification, mitigation, management, and closure of third party risks in alignment with the Company's Statement of Risk Appetite. Through this approach and framework, CME has determined that the services received from Google are of a critical nature, and Google has been designated a Tier 1 third party.

As a Tier 1 third party, Google is subject to an annual Third Party Risk Assessment ("**TPRA**") that incorporates risk assessments by the TPRM Risk Domains, which include Information Governance, GIS, and Operational Resilience. Findings will be recorded and addressed either through risk treatment plans or a risk exception. A memorandum prepared by TPRM summarizes the risk assessments and is reviewed and acknowledged by key business and risk stakeholders in accordance with the TPRM Segmentation and Risk Assessment Procedures document.[9]

TPRM, as a second line of defense function, will also participate in ongoing monitoring of Google on multiple fronts pursuant to its generally applicable procedures, as may be amended to address the new relationships with Google.[10] Other functions in the Company will inform TPRM of incidents, threats, and service disruptions, in coordination and collaboration with key stakeholders and business owners.

Given the importance and unique risks presented by CME's relationship with Google, monitoring and oversight above and beyond the generally applicable TPRM procedures is appropriate. As an example, in 2022, TPRM completed a review of Google Cloud's third party risk management program, as part of its initial TPRA. TPRM will work with Google to identify key fourth parties by service category. Critical fourth parties will be added to ongoing monitoring activities coordinated by TPRM. Also, in further collaboration with CME Group's Operational Resilience program, TPRM coordinated an on-site assessment of a primary Google data center in January 2023.[11] Going forward, TPRM will coordinate on-site assessments of a primary Google data center as needed. TPRM will also report on the risk and performance of Google, which will be provided on a quarterly basis and delivered to the TPRM Steering Committee.

d. Global Assurance

[8] CME has separately submitted a request for confidential treatment to CME Group's Commitment and Signing Authority Policy, which CME has provided in confidential Exhibit D to File No. 23-233.

[9] CME has separately submitted a request for confidential treatment to the TPRM Risk Memorandum for GCP and the TPRM Segmentation and Risk Assessment Procedures, which CME has provided in confidential Exhibit E and Exhibit F to File No. 23-233.

[10] CME has separately submitted a request for confidential treatment to the TPRM Procedures, which CME has provided in confidential Exhibit G to File No. 23-233.

[11] CME has separately submitted a request for confidential treatment to the Site Visit Operational Resilience Memo, which CME has provided in confidential Exhibit H to File No. 23-233.

CME Group's Global Assurance ("**GA**") department is an independent and objective assurance and advisory function that assists CME Group in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of the organization's governance, risk management, and internal control processes. GA will consider the scope of reviews and assessments conducted by independent accountants, regulators, and other compliance and control functions for the purpose of providing optimal assurance to the organization. Opportunities for improving management control, profitability, and the organization's image may be identified during audits. These opportunities are communicated to the appropriate level of management.

In 2022, GA completed two Special Projects related to the GCP migration.[12] In 2023, Global Assurance plans to complete four Special Projects.[13] GA will continue to engage with management on GCP migration activities and will identify future Google-related audits or Special Projects based on its annual risk assessment process, or as needed based on changes to the applicable risk profile.

II. Migration Execution Framework

a. CME GCP Platform

To support the successful migration of CME's clearing systems to GCP, CME first established the CME GCP Cloud Platform (the "**Platform**"), on which CME's applications will be deployed. This foundation forms the backbone of CME's GCP environment and is designed to meet CME's requirements, including those relating to its operation of the Clearing House.

Through this migration, CME is developing cloud architecture designed not only to support its current security standards and controls, but also to further strengthen them with cloud-native tools and solutions. A more in-depth description of CME's IT controls is below.[14] For the Platform in particular, CME employed a process designed to support the consistent deployment of its IT controls in this environment. While building the Platform, CME mapped each of its IT control(s) to a specific user story. In software development and product management, a user story is an informal, natural language description of software feature requirements. Each user story was in turn tracked through CME's development process to completion.[15]

The Platform is also designed to support automation, enabling CME to build more robust infrastructure that can dynamically scale and minimizes the risk of human error. One example of this automation advancement is evidenced through CME's use of the "policy-as-code" and "infrastructure-as-code" approach through Open Policy Agent ("**OPA**"). OPA policies provide a standard framework for defining controls for enforcing compliance and security requirements during continuous integration ("**CI**") and continuous deployment ("**CD**") to protect CME's deployed resources. Terraform and Kubernetes Configuration Connector are used as deployment tools for infrastructure-as-code.

CME will meet certain control requirements in the Platform by leveraging cloud services, including services offered by GCP. Before relying on such services, CME's GIS Architecture team conducts a Cloud Services Review to evaluate the service's use within the CME GCP environment.[16] The purpose of these reviews is to identify governance requirements for the proposed service scope and to provide details on potential applicable cloud service limitations that may require compensating controls to be put to use. Upon

[12] CME has separately submitted a request for confidential treatment to the CFTC regarding the Global Assurance Google Cloud Transition Special Project and the Google Cloud Platform Technology Special Project reports, which CME has provided in confidential Exhibit I and Exhibit J to File No. 23-233.

[13] CME has separately submitted a request for confidential treatment to the CFTC regarding the Global Assurance Project Overview, which CME has provided in confidential Exhibit K to File No. 23-233.

[14] *See Infra* § III.

[15] CME has separately submitted a requestion for confidential treatment to the CFTC regarding the User Stories, which CME has submitted as Exhibit L to File No. 23-233.

[16] CME has separately submitted a request for confidential treatment to the CFTC regarding the list of Cloud Service Reviews, which CME has provided in confidential Exhibit M to File No. 23-233**.**

completion, the Cloud Services Reviews will feed into the development of OPA policies, which will be designed to automatically apply appropriate configurations through deployment.

CME designed the Platform to allow deployed applications to leverage different reliability and resilience strategies. CME's clearing systems will base their resilience strategies on multi-region GCP resources and services at the infrastructure level. CME is deploying a multi-region strategy, primarily leveraging two geographically dispersed Google regions. Data will be captured and replicated across regions, allowing CME to run its systems in either region. These regions may expand or change as planning continues. For a regional failover, systems supporting CME's clearing and settlement processes will be designed and tested to recover within the established two-hour recovery time objective ("**RTO**") in a geographically dispersed region. Capacity and performance in both the primary and recovery region will be similarly architected to support capabilities in either region.

In addition to multi-region deployment, certain systems will have an additional layer of redundancy within region by leveraging redundant zones. Certain systems will be designed to withstand a zone-wide failure, by failover to another redundant zone within region. Systems with this design will be built to withstand a zone-wide failure at the component level, while ensuring data loss continues to meet CME's recovery point objectives, and will be tested and maintained on an ongoing basis.

Given the foundational nature of the Platform, CME has conducted various forms of validation testing to provide added assurance that the IT controls are designed effectively and work as intended.[17] For example, the GIS IT Compliance Team has conducted a test of the design of the controls deployed on the Platform, with findings tracked and remediated through CME's existing processes.[18] CME also conducted two rounds of penetration tests as it iteratively built out the Platform. The initial penetration test was conducted by a third party in October 2022. This third party penetration testing vendor performed a Cloud Configuration Review against the Platform. The objective was to identify vulnerabilities and/or misconfigurations an attacker could potentially exploit to gain unauthorized access to sensitive data or systems. In March 2023, as the Platform continued to mature and could support internet ingress and egress, CME engaged a different third party vendor to conduct an unauthenticated external network and web applications penetration test. Findings from these tests are tracked and remediated through CME's existing processes.

b. Application Migration

CME plans to deploy its clearing systems to the Platform by taking an iterative, methodical, and deliberate approach to the migration, which will allow for the application of lessons learned in earlier deployments to subsequent deployments and phases. During this transition, CME will continue to maintain its program of risk analysis and oversight with respect to its on-premise operations and automated systems to identify and minimize sources of operational risk, while also expanding this program to include the GCP deployments as described in more detail below.[19]

The first phase of applications migrated to the Platform in 2022. These applications did not support core clearing or settlement activities, but acted as focused, discrete test cases on non-regulated systems. For example, in 2022 CME launched the Referential Data Warehouse, which provides access to historical, publicly available product information at GCP. In 2023, CME has continued to prepare for the migration, by deploying systems to the Platform not for production purposes, but for quality assurance and testing. This early work has laid the foundation for CME to prepare for the migration of its core clearing and settlement applications to the Platform for production.

The applications supporting the CME Clearing House are grouped together in domains, with the target of completing the migration of all clearing systems by the end of 2024, pending regulatory review and subject

[17] CME has separately submitted a request for confidential treatment to the CFTC regarding the CME GCP Platform Milestone Testing Support, which CME has provided in confidential Exhibit N to File No. 23-233.

[18] CME has separately submitted a request for confidential treatment to the CFTC regarding the CME GCP IT Control Testing 2022-2023, which CME has provided in confidential Exhibit O to File No. 23-233.

[19] *Infra* § III.

to project-related dependencies. Domains are a set of pre-defined groupings of CME applications based on the function and process they support. Relevant Domains include Clearing House Managed, Clearing Risk, and Core Clearing.[20] Domains will be leveraged to consolidate stakeholder coverage, status reporting, and project management related to the GCP application migration. CME will primarily migrate applications to the Platform through three methods:

- Rehost: The machine currently deployed in an on-premise data center on which a migrating application runs (i.e. the host) will be moved to the Platform as a virtual machine, running the same, equivalent, or compatible operating system and same application. In short, the host with the application moves to GCP.
- Replatform: The application will move to the Platform, but not the machine. CME will accomplish this by decoupling the application from its underlying machine and packaging it in a "Container." Replatforming may require minimal code changes to an application because the application may have made assumptions about the host guarantees (e.g., persistent disk, host IP, hostname etc.). Replatforming also may require the adoption of certain cloud native services. In short, an application is decoupled from a host-based deployment and execution model, while also adopting some basic cloud native services so that it no longer relies on an on-premise data center for such services.
- Refactor: An application undergoes significant code changes to modernize and adopt more cloud native services. In short, an application is materially upgraded for GCP deployment.

Within each of the migration methodologies, applications will be tracked through stage gates, including:

- Production Ready: Development and quality assurance testing is complete, and the application is deployed in the highest available non-production environment.
- Production Live: The application is deployed in a production environment and all operational and customer requirements have been met. CME has received any necessary non-objection from regulators to deploy into production. The Production Live stage is when the application becomes the new system of record.
- Decommission: This is the final stage where processes and servers have been shut down in the legacy, on-premise data centers.

As with the Platform, applications will be designed and developed to meet CME's requirements, including information security requirements, as described in more detail below.[21] Each application will go through testing and validation, pursuant to CME's development lifecycle processes, which are also described below.[22] Additional detail on the applications within scope for this migration, the method of their migrations, and projected timelines for deployment are provided in Exhibits Q and R.[23]

III. CME's Cloud-Based Clearing Systems Will Meet System Safeguards Requirements

As noted above, CME is taking an iterative approach to the migration of its clearing systems to GCP, to allow for the application of lessons learned in earlier deployments to subsequent deployments and phases. During the period that CME will have systems running both on-premise and in GCP, CME will continue to

[20] CME has separately submitted a request for confidential treatment to the CFTC regarding the Clearing House Managed, Clearing Risk, and Core Clearing Domain Map, which CME has provided in confidential Exhibit P to File No. 23-233.

[21] *Infra* § III.a.

[22] *Infra* § III.e.

[23] CME has separately submitted a request for confidential treatment to the CFTC regarding the GCP Migration Report, which CME has provided in confidential Exhibit Q to File No. 23-233, and future state clearing architecture, which CME has provided in confidential Exhibit R to File No. 23-233.

maintain its program of risk analysis and oversight with respect to its on-premise operations and automated systems to identify and minimize sources of operational risk.[24]

CME has also expanded and adapted this program of risk analysis and oversight to incorporate and cover its GCP-hosted operations and automated systems. The GCP migration will enable CME to enhance and evolve its risk management, reliability, cybersecurity, and capacity for itself, market participants, and the broader industry.[25] CME has designed the migration to meet its obligations under the CFTC's System Safeguards requirements and will conduct tests and reviews to gain assurances that CME has effectively executed these designs.

a. Information Security

Information security is an important area of focus for CME both during the migration and as it builds towards a secure target state in GCP. Throughout the transition to GCP, CME has updated information security controls and standards in partnership with platform and application teams and tested GCP environments and deployed controls. CME applications and architectures are reviewed for security throughout development and deployment processes, and GCP components, including cloud-native offerings, undergo security review before use by CME. CME remains committed to its defense-in-depth approach, which uses overlapping detection and response capabilities to enhance its security posture.

i. IT Controls, Standards and Policies

Throughout the migration, CME has and will continue to apply consistent technical control requirements both to the Platform and the applications it deploys to that Platform. CME has historically and will continue to align its control framework to the National Institute of Standards and Technology ("**NIST"**) Security and Privacy Controls for Information Systems and Organization, Special Publication 800-53. CME also will continue to leverage its existing control library to ensure these controls are cataloged and deployed consistently throughout the migration process and once systems are running in GCP. In addition to CME's existing controls, CME mapped cloud specific controls to the existing control library, leveraging Cloud Security Alliance (CSA) Cloud Control Matrix, version 4 (CCM), adding controls to its library, where appropriate, to address unique risks posed by the GCP migration.[26]

CME's existing IT Policy framework will continue to define the capabilities necessary to effectively manage information technology and information risks throughout the Company and will be maintained to reflect the new GCP Environment. CME has updated, where appropriate, its Technical Standards to cover Cloud and GCP-specific expectations.[27]

Through the controls and policy framework described above, CME has designed the Platform, and the applications that will be deployed to it, to be secure and resilient. Below is a description of some of the key features this control and policy framework is designed to enforce:

- Access Control: As a demonstration of its commitment to information security and in support of the creation and maintenance of a comprehensive security infrastructure, CME has applied several industry standard principles to its access controls in GCP, including need to know, authentication, data protection, least privilege, and separation of duties. CME's identity and access management controls are designed to ensure the security principles are met through its identity governance and administration program, access governance, directory management, privileged access

[24] CME expects to operate in this hybrid state – with both on-premise and GCP based architecture – even after the Clearing House systems successfully migrate. For example, CME's Designated Contract Markets has systems and applications that will require a longer time frame for migration to GCP.

[25] The GCP migration will result to changes to CME's the infrastructure and technical systems. No additional changes to its risk management or public disclosures will accompany this technology change.

[26] CME has separately submitted a request for confidential treatment to the CFTC regarding the CME IT Control Library (April 28, 2023), which CME has provided in confidential Exhibit S to File No. 23-233.

[27] CME has separately submitted a request for confidential treatment to the CFTC regarding the CME Group Information Technology Policy, which CME has provided in confidential Exhibit T to File No. 23-233, and relevant technical standards, which CME has provided in confidential Exhibit U to File No. 23-233.

management and password storage, single sign-on and federation, multi-factor authentication and access onboarding and offboarding controls.

- Network Segmentation: The Platform has both environmental segmentation, designed to separate production and non-production workloads, as well as zone segmentation, designed to limit availability outside of CME's network to specifically configured services. If internet exposure is required for CME applications hosted on the Platform, the Platform is designed to intercept and inspect all internet ingress and egress traffic, pursuant to approved design.
- Logging, Monitoring, and Auditing: Application and cloud infrastructure-related logs are gathered through Google's cloud logging service and retained and archived in storage buckets and forwarded to CME's existing security tooling for monitoring and detection events.
- Encryption, Key Management and Data Security: As a native security control of GCP, all data stored on GCP is encrypted by default. Encryption of data in transit through Google APIs will be tied to certificates issued by Google's Certificate Authority. For virtual machine to virtual machine data transfers, as a native security feature of GCP's networking, GCP encrypts and authenticates data in transit at one or more network layers.[28] Google Cloud KMS is leveraged for key management so that all encryption keys are managed and controlled by CME within GCP. Data is secured in GCP through a VPC service control perimeter through interconnect that prevents access to data barring services without explicitly granted access. Service perimeter allows access through IP addresses through the data center and approved service accounts are access managed.
- Vulnerability Management: CME will maintain and extend its vulnerability management program to its GCP-deployed applications. This program includes ongoing cyclical management of vulnerabilities, including coordination of identification, classification, remediation, and mitigation, as well as metrics to track these activities. Additionally, CME subscribes to a commercial vulnerability feed for early notification of critical vulnerabilities; this feed includes vulnerabilities published in the National Vulnerability Database (NVD). GCP also monitors its network for suspicious activity and performs vulnerability scans. GCP maintains a Vulnerability Management Program, through which CME will collaborate with GCP to monitor and address security vulnerabilities.
- Record Retention: CME will continue to meet its record retention obligations in accordance with 17 CFR § 1.31, through the GCP migration process and thereafter. The Records and Information Management Policy and associated Record Retention Schedule remain applicable and are intended to support CME's compliance with its regulatory and legal obligations.[29]

ii. Cybersecurity Incident Management

CME maintains and regularly tests an enterprise-wide Cyber Incident Response Plan ("**CIRP"**), the cyber incident response framework used for both CME's on-premise and cloud environments.[30] The CIRP has been updated to include specific response and forensics playbooks for GCP-related incidents, as well as target initial response times governing coordination efforts with Google's Customer Support teams. The CIRP will continue to guide the cyber incident response process as the GCP migration occurs, including the migration of clearing-related systems and applications. The CIRP will continue to work as a portion of the overall CME Incident Response Framework when there are cyber considerations.

During a GCP-related incident, and per the updated CIRP, CME may leverage support from a Google Technical Account Manager ("**TAM**"). The TAM is a long-term technical advisor, assigned to CME. During an incident involving GCP, CME will also be assigned a Google Technical Solutions Engineer ("**TSE**"). The

[28] For more details, please refer to the Encryption in Transit in Google Cloud white paper, https://cloud.google.com/docs/security/encryption-in-transit.

[29] CME has separately submitted a request for confidential treatment to the CFTC regarding the Records and Information Management Policy and associated Record Retention Schedule, which CME has provided in confidential Exhibit V and Exhibit W to File No. 23-233,

[30] CME has separately submitted a request for confidential treatment to the CFTC regarding the CME Group Cyber Incident Response Plan, which CME has provided in confidential Exhibit X to File No. 23-233.

TSE answers and troubleshoots issues CME may face when using GCP, for cases filed by CME, the TAM and/or account teams.

iii. System Safeguards Information Security Testing and Assessments

CME also has expanded its System Safeguards required testing and assessment programs to cover the GCP-hosted systems. As noted above, the GIS IT Compliance Team already has conducted a test of design for the controls deployed on the Platform. As part of its annual control testing program, going forward the GIS IT Compliance Team will also incorporate testing of controls in the GCP environment (both for the Platform, as well as for the applications deployed there), based on its risk-based approach. Any findings from the testing will be tracked through remediation, pursuant to the IT Compliance Team's existing processes.

In addition, GCP regularly undergoes independent, third party audits and certifications to verify that its information security practices match its controls and commitments. GCP has made its key compliance reports, independent audits, and certifications available to CME as part of its due diligence review and will continue to do so to support CME's ongoing oversight requirements. By way of example, some of the key international standards GCP is audited against include System and Organization Controls, Type Two and Three ("SOC2" and "SOC3" respectively), International Organization for Standardization ("ISO") Standards 27001, 27017, ISO 27018, and NIST 800-53, among others.

CME's penetration testing efforts will also expand to cover the CME GCP environment. As noted above, CME has already conducted two penetration tests of the Platform.[31] The GCP environments also will be incorporated into CME's existing internal and external penetration testing programs on a going forward basis. In addition to CME's efforts, Google conducts its own penetration tests of its infrastructure, summarized results of which CME will have the opportunity to review annually, per the agreement with Google.[32]

CME's System Safeguards required security incident response plan testing efforts will expand to test and assess CME's readiness to detect and respond to security incidents in GCP environments. CME will continue to use exercises of appropriate breadth and complexity to test CME's readiness to discover and alert incident responders of suspicious activity and to test the effectiveness of its escalation and decision-making processes. Scenarios including systems and threat actor activity in GCP will be planned and scheduled according to CME's existing, risk-based planning process. Results from this testing will be tracked and remediated through CME's existing process.

CME's technology risk management program, including activities that support its Enterprise Technology Risk Assessment, will expand to the identification, analysis, and evaluation of risks arising from GCP infrastructure, systems, and related processes. CME will continue to use risk assessments for risks identified by stakeholders, through vulnerabilities and findings, and those identified within projects. CME will manage the treatment of identified risks through its existing risk management processes.

b. Operational Resilience

CME Group's Operational Resilience ("**OpRes**") Program serves to mitigate potential impacts to its markets, customers, assets, and employees, and to safeguard the availability of essential products and services. The OpRes Program – including Business and System Resilience – is designed to ensure that CME can respond appropriately to incidents while protecting the interests of its stakeholders, ensuring the safety of employees, and protecting its reputation and brand. OpRes provides quarterly reports to the Risk Committee and regular reports to ERM. The Management Team is involved in many aspects of the program and the program components are fully supported by leadership.

[31] *Supra* § II.a.

[32] *See* Exhibit A, Google Cloud Mast Agreement § 2.5.

The System Resilience ("**SR**") Component of the OpRes Department manages the intersection of Operational Resilience efforts and the technology that supports the delivery of CME's essential products and services. The team works to mitigate risk by helping ensure CME can recover its essential business processes via recovery of technology systems following an event that renders regular production systems unusable.

OpRes' focus is not limited to a catastrophic event. OpRes has a responsibility to prepare for and identify alternative ways that critical processes can be completed when systems are not available. System Resilience is achieved by defining and communicating requirements, reviewing and approving design and architecture, planning for contingencies, detecting any single point of failure, testing, and engaging independent verification and validation of recovery and resiliency strategies. The SR Component is also responsible for the coordination and facilitation of the technology resources required to validate, recover, and test CME Group systems within their applicable recovery time objectives as identified within the Business Impact Analysis and/or by regulatory mandate.

CME has built and maintains its current infrastructure with a focus on creating a high-capacity, redundant system, with tested, efficient, and effective system resilience capabilities that meet CFTC regulatory requirements and industry best practices. Moving to GCP will allow CME to continue to meet these obligations, while availing itself of expanded global and regionally resilient infrastructure and data centers. Cloud deployments can introduce additional resilience options, and CME will apply its architecture and system agnostic Business and SR programs to migrated services to continue to verify that CME Clearing meets its critical Business and System Resilience System Safeguard controls.

CME has developed Cloud Resilience Principles and will use them as a guide as applications are designed, migrated, and deployed. These principles summarize, at a high level, resilience and availability requirements, which CME will consult along with SR program requirements and non-functional requirements when designing and building solutions for individual services, applications, and systems.

As noted above, CME is deploying a multi-region resilience strategy.[33] Services, applications, and systems will be deployed to more than one region, either simultaneously or as necessary. Services, applications, and systems should be designed to run independently in a second region in the event of a total region failure. Services, applications, and systems that are not simultaneously running across multiple regions should have deployable infrastructure available to recover in a second region within stated, business-driven RTOs. In accordance with 17 CFR § 39.34(b), systems will be deployed or deployable in a second, geographically dispersed region, which relies on distinct underlying infrastructure. This recovery time objective is two hours for systems deemed necessary to support clearing and settlement.

Through CME's development lifecycle process, described in more depth below,[34] the OpRes Team is engaged to incorporate SR Principles and Requirements into the development and design of CME's clearance and settlement systems, as well as create necessary documentation for failover planning. Prior to entering Production Live status on GCP, deployments to GCP will be tested to demonstrate that they can be recovered in a second region within their recovery time objectives. Regional failover exercises will be scheduled on a regular cadence during the clearance and settlement system migration to capture additional applications and deployments throughout the migration. These regional failover exercises will include application and business unit testing tied to essential processes for clearance and settlement and will encompass both on-premise and GCP hosted systems. Once the migration is complete, SR testing will continue to be performed for clearing and settlement systems at least annually. As with the tests conducted during migration, these tests will include application and business unit testing tied to essential processes for clearance and settlement. For these tests, the SR Team communicates objectives and scope, facilitates exercises, and prepares after-action reports, which are distributed to senior leadership.

[33] *Supra* § II.a.
[34] *Infra* § III.e.

Business Recovery Plans, including Business Impact Analyses, which contain dependencies for process completion (systems, important vendors, locations, etc.), are reviewed and approved at least annually. Business unit testing, whereby employees test their processes from alternate locations on backup systems, is performed at least annually.

OpRes, through the Vendor Risk Management component of its program, has worked with key GCP Program stakeholders to identify and document an exit planning framework for the Google relationship ("Google Exit Plan"). This plan outlines areas such as business decisions, timelines, substitutability, and the potential impact to the Company if a need for an exit were to occur. This Google Exit Plan supports and works in conjunction with TPRM's third party offboarding procedure. For a planned exit, contractual provisions with Google will support CME's transition to an alternate cloud service provider or infrastructure provider.[35] As an initial matter, Google has made a long-term commitment to CME, which is reflected in the terms of the 10-year agreement. This agreement sets forth limitations on Google's ability to terminate the contract, as well as provides for adequate transition periods and transition assistance as a backstop if CME determines a change in provider is required.[36] From a governance and oversight perspective, the GCP Program Steering Committee will oversee the Parties' performance under the agreement. The Steering Committee will attempt to resolve disputes and escalate matters that arise out of the agreement in a timely manner. CME Group has established terms, roles and responsibilities, and escalation paths have been put in place between the companies, to manage and resolve any performance issues. In the unlikely event that an unplanned exit is required, considerations, alternate solutions, and business decisions have been documented within the Google Exit Plan.

c. Capacity and Performance Planning

CME will continue to monitor Clearing system capacity in the same manner as it currently does with its on-premise infrastructure. Daily capacity reports, metrics, and batch cycle Service Level Agreement ("**SLA**") reporting will continue to be used by Global Operations and the Clearing House to monitor system capabilities and any SLA violations. Where technically feasible and advantageous, CME may implement elastic capabilities for scaling.

Capacity testing of CME's clearing and settlement systems will follow CME's existing processes.[37] CME has no contractual capacity limits or restrictions in its agreement with Google. CME's documented capacity testing processes include message-based capacity management, message-based SLAs, message-based capacity monitoring, message-based capacity stress testing, batch cycle SLAs, and batch cycle capacity testing methods. Generally, CME does not expect the capacity testing methods to change, and there are no currently planned changes to the SLA targets as a result of the migration to GCP.

d. Systems Operations

The GCP migration will not change CME's ultimate control and authority over its systems. CME will continue to operate its existing IT Operations support model framework leveraging the current toolsets; with the Technology Operations Command Center ("**TOCC**") monitoring servers, databases, applications and storage devices for issues, and performing incident management and escalation as necessary for all customer-facing environments, including fully-migrated GCP-based applications, on a 24/7 basis using a follow-the-sun model.

i. System Maintenance

Google builds and maintains its infrastructure from chips to data centers and has logical, operational, and physical controls to fulfill its security, data protection, and compliance obligations. A Google data center consists of thousands of servers connected to a local network. Google designs the server boards,

[35] *Supra* § I.b.

[36] *See* Exhibit A, Google Cloud Master Agreement § 12.

[37] CME has separately submitted a request for confidential treatment to the CFTC regarding the Clearing Capacity Planning and Testing Plan, which CME has provided in confidential Exhibit Y to File No. 23-233.

networking equipment, and custom chips, including a hardware security chip, that is deployed on servers, devices, and peripherals. These chips enable Google to identify and authenticate legitimate GCP devices at the hardware level and serve as hardware roots of trust.

To support maintenance, Google has developed automated systems to ensure that servers run up-to-date versions of their software stacks (including security patches), detect and diagnose hardware and software problems, ensure the integrity of the machines and peripherals with verified boot and implicit attestation, ensure that only machines running the intended software and firmware can access credentials that allow them to communicate on the production network, and remove or re-allocate machines from service when they are no longer needed.

Google personnel have met with multiple teams from CME from the outset of the relationship and shared various resources with CME's IT, GIS, Risk, Compliance, and GA teams, among others, to provide training and transparency into GCP's security and data protection posture. The Google team meets and will continue to meet with CME personnel, upon CME's request, on a recurring or ad-hoc basis, as appropriate.

ii. Operational Incident Management

As noted above, the migration to GCP will not alter CME's commitment to support resilient systems, including 24/7 coverage of all its customer-facing environments. Throughout and following the migration, CME will leverage the existing event and problem management processes that it uses today. As applications migrate to GCP, coordination and communication with Google resources will continue and expand as necessary, as CME maintains its commitment to support the resiliency of its systems.

For example, CME and Google will collaborate through Google's incident response process, through which CME will be notified of potential incidents that may impact the confidentiality, integrity, or availability of its data. CME receives GCP incident notifications in the following ways:

- Mandatory Service Announcements that are essential to continued use of a product or service or a critical update on a specific action or event.
- Early Incident Notification, which Google's internal systems trigger when Google detects a potential issue which subsequently allows CME to get ahead of any potential issue that can impact its workloads.
- GCP's public status page provides status information on the services that are part of Google Cloud.

If triage is required on a GCP Product, Google's customer care and technical experts are committed to support CME. If necessary, CME can also request additional attention on a support case by escalating the support case.

iii. Configuration Management

Where possible, CME is embracing an infrastructure-as-code approach using a set of industry standard tooling and best practices. These centrally managed and monitored deployment pipelines allow for the enforcement and continual validation of critical operational and security policies and controls.

For core infrastructure assets, Terraform and the Google-managed Google Cloud Provider are used to manage and maintain infrastructure. For applications and systems being deployed into Kubernetes and many other cloud-native Platform as a Service ("**PaaS**") solutions, the Google provided Kubernetes Configuration Controller ("**KCC**") is being used. With both Terraform and KCC, all updates to the configuration and state of the environments are managed via updates to Infrastructure as Code ("**IaC**") repositories. These updates require peer review and corresponding approval, which can be audited to determine what was changed, when, and who made and approved the changes.

Policy-as-code has been implemented in both Terraform and KCC pipelines using OPA policies. This tooling has a variety of important use cases, including Security and Operational control policies. These policies are also managed in IaC repositories and reviewed by the appropriate parties before deployment.

These policies enforce critical controls and help prevent undesirable changes from occurring in the environments. All changes to the environments, regardless of the automation pipeline used, continue to follow CME Group's existing Change Management policy, tooling, and process.

For Virtual Machines, in which CME is accountable for configurations and patching of the operating system, Packer is used to create a golden image of each required Operating System Version. Application teams can consume these base images in their Packer pipelines and create application-specific Virtual Machine images for deployment and promotion through the environments. For some applications where fully automated deployments cannot be completed with each patch cycle, CME's standard patching process will be utilized for maintaining patch levels of systems. CME will use Tripwire to identify and remediate configuration drift and policy compliance violations.

Additionally, Google Security Command Center ("**SCC**") provides compliance monitoring based on industry standards, such as CIS Benchmarks, across all Google Cloud assets. CME will use SCC to identify security misconfigurations and compliance violations in Google Cloud assets and remediate them by following actionable recommendations and a risk-based approach.

e. Systems Development and Quality Assurance

CME has established a set of processes to obtain the necessary approvals for planning, designing, developing, testing, and deploying its Information Systems, referred to as the System Development Life Cycle ("**SDLC**"). This process pertains to all core clearing systems that support the acceptance and novation of trades, and the calculation of margin and settlement obligations. The SDLC requires that systems are designed to meet quality standards and undergo quality assurance testing prior to deployment.

As appropriate, testing includes functional, performance, integration, regression, and security testing. Quality assurance tests are performed through a combination of manual and automated activities. Additionally, testing may include customer certification. The implementation of CME's SDLC program is supported by the Corporate Obligations and Governance ("**COG**") framework. The COG Framework is designed to identify work that requires specific security and operational reviews performed by specialist teams outside of the developer and quality assurance ("**QA**") teams. These reviews include:

- Application Security
- Application Architecture
- Infrastructure Security
- Operational Resilience
- Information Governance
- Operational Readiness
- Vulnerability Management

CME's existing SDLC processes support waterfall and continuous (i.e., agile) software development methodologies and remain in effect for GCP deployments. As CME continues to transition to continuous development methodologies and cloud native deployment tools, including IaC technologies, CME will review and update processes to ensure appropriate oversight, quality, and controls.

f. Physical and Environmental Controls

Google designs and builds its own data centers, which incorporate multiple layers of physical security and environmental controls. Access to these data centers is tightly controlled. Google uses multiple physical security layers to protect the data center floors, as well as other controls including biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems.

As CME moves systems and applications into the Google Data Centers, it continues to evaluate and monitor the physical and environmental controls. Following an operational evaluation, CME Group's Global Security and Facilities Teams confirmed the Google Data Center controls to be generally at the current level as those of CME group's existing data center providers, which includes due diligence discussions, review of SOC testing, and onsite assessments of processes and protocols. Global Security follows the Department of Homeland Security model for physical assessments by identifying significant areas and assets and evaluating risk broadly by taking into consideration the criticality, vulnerability, threat, and existing mitigation efforts. Global Security and Facilities will continue to monitor the control environment associated with CME's business employed to GCP.

IV. Clearing Member and Third Party Engagement and Feedback

CME intends to engage with Clearing Members, market participants, and middleware providers as it approaches GCP migration for CME Clearing core systems and applications. Before switching any significant migration to production, CME plans to host a parallel production phase where participants can interact with the soon-to-be migrated applications and databases to ensure operational readiness.

The duration of each hosted parallel production phase will vary depending on the application and database, and also on the extent of development work performed to effect migration. For example, where a non-core clearing application or database is simply rehosted from on-premises to GCP, in a manner which does not impact any downstream usage by market participants, it is reasonable to expect a more limited amount of testing necessary by market participants to ensure continuity of service.

Conversely, for a GCP migration with a higher degree of impact, for example migration of the CME Clearing Banking and Asset Management System (**"BAMS"**), a more detailed engagement strategy will be employed. CME Clearing's legacy system for collateral management and settlement variation is an application named "C21". Collateral management and settlement variation are important parts of the daily operations at CME Clearing; collateral management offers CME's clearing members the ability to substitute their collateral posted to CME Clearing on a given day and is a non-core clearing activity, while settlement variation is a core part of the CME Clearing process of daily settlements. In an effort that predates the GCP migration efforts, CME initiated a project to replace C21 with BAMS. In light of the GCP Program, CME intends to continue its project to replace C21 with BAMS in its entirety, as well as migrate BAMS to GCP.

The first impact to Clearing Members from the BAMS project was in April 2022 with the deployment of the new BAMS Clearing Firm User Interface ("**UI**") for collateral management. This technology was deployed on-premise. Importantly, this included a migration of collateral management and did not impact the daily settlements functioning of the Clearing House. Given the impact of collateral management processing for Clearing Members (non-core but nevertheless important), outreach and engagement for testing was performed before launch. This outreach occurred in Q4 2021 and Q1 2022. Advisory Notices to clearing members were distributed in November 2021, January 2022, and March 2022. In addition to Advisory Notices, Clearing House Banking Staff presented the planned change and request to perform testing to Clearing Members in monthly working group calls hosted by CME including at the Clearing Advisory Group and the OTC Clearing Initiatives Forum. The Clearing House Banking Processing Team also contacted Clearing Members bilaterally to ensure all members had a dedicated CME point of contact to assist with testing and to receive any feedback. In addition to the multiple channels of outreach, a user guide for the external UI was shared with each Clearing Member to assist in the transition to the new UI. Clearing Members had discretion in determining their own testing process. The CME point of contact working with each Clearing Member collected feedback and then communicated the information to the development team. CME received requests for additional features and enhancements but did not receive any negative feedback. Each request was evaluated with input from the Clearing House Banking Team.

As these BAMS collateral management components are transitioned to GCP, CME intends to ensure a consistent outreach and testing experience for Clearing Members. After migration dates have been finalized, CME will engage in outreach and engagement to Clearing Members as migration dates become solidified in order to provide them with a testing experience consistent with what was provided for the collateral management changes from C21 to BAMS. Additionally, CME plans to use this outreach as a template for the migration of the settlement variation components of C21 to a GCP-based BAMS. This will include outreach to Clearing Members bilaterally, presentation at customer forums, and advisory notices providing clarity around testing windows and ultimate transition dates.

As an extra precaution, prior to the execution of the GCP migration for CME Clearing applications or databases with external user impacts, CME will evaluate the criticality of the application or database and provide advance notice to external uses as appropriate.[38] Where a core clearing application or database is scheduled for migration, CME will issue a public notice to the market either via a CME Clearing Advisory or some other substantially similar process well in advance of the migration. In addition, CME hosts a monthly CME Clearing Advisory Group (**"CAG"**) meeting where Clearing Members and market participants are invited to receive updates, ask questions, and provide feedback on any CME Clearing operational initiative.

As GCP migrations increase in frequency, CME intends to use the CAG forum to ensure broad awareness of its plans. An example of the usefulness of the CAG is illustrated in the planning for the April 2023 Eurodollar and OTC USD LIBOR Swaps conversions to SOFR. The CAG meeting was used as a forum for feedback and questions from Clearing Members on the operational details for-the migrations. CME will continue to follow that approach in its GCP migrations to utilize feedback from participants to ensure smooth transitions.

[38] In addition, CME will submit notices of planned changes to its automated systems that may impact the reliability, security, or capacity of its systems, as necessary and appropriate to the CFTC, pursuant to 17 CFR § 39.18.