Microsoft Corporation – Next Generation Privacy – Privacy Information Management System

Report on Controls at Service Organization Relevant to Security and Availability (SOC 2)

July 1, 2018 through June 30, 2019

Deloitte.

Table of contents

Executive summary

Microsoft Corporation—NGP-PIMS	
Scope	Next Generation Privacy – Privacy Information Management System (NGP – PIMS)
Period of Examination	July 1, 2018 through June 30, 2019
Applicable Trust Principles	Security and Availability
Locations	Redmond, WA
Subservice Providers	Yes: • Microsoft Azure ("Azure")
Opinion Result	Unqualified
Testing Exceptions	One control – two services affected – see Page 61
Complimentary User Entity Controls	Yes – **Page 20**

Section I: Independent service auditors' report

Deloitte & Touche LLP

925 Fourth Avenue, Suite 3300
Seattle, WA 98104-1126 USA

Tel: +1 206 716 7000
Fax: +1 206 965 7000
www.deloitte.com

Section I:
Independent service auditors' report

Microsoft Corporation
Redmond, Washington

Scope

We have examined the attached description of the system of Microsoft Corporation ("Microsoft", the "Service Organization") related to its Next Generation Privacy – Privacy Information Management System (NGP-PIMS) online service throughout the period July 1, 2018 to June 30, 2019 (the "Description"), based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period July 1, 2018 to June 30, 2019 to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

The information included in **Section V**, *Supplemental information provided by the Service Organization*, is presented by management of Microsoft to provide additional information and is not a part of the Description. Information about Microsoft's management responses to testing exceptions has not been subjected to the procedures applied in the examination of the Description and the suitability of the design and operating effectiveness of the controls, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria.

Microsoft uses Microsoft Azure "subservice organization" to provide Platform as a Service cloud services for hosting the NGP-PIMS applications. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria. The Description presents Microsoft's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Microsoft's controls. The Description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria. The Description presents Microsoft's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Microsoft's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Microsoft is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved. Microsoft has provided the accompanying assertion titled "Assertion of Microsoft Management" ("assertion") about the Description and the suitability of the design and operating effectiveness of controls stated therein. Microsoft is also responsible for preparing the Description and assertion, including the completeness, accuracy, and method of presentation of the Description and assertion; providing the services covered by the Description; selecting the applicable trust services criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the Service Organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of design and operating effectiveness of controls stated in the Description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board (IASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the Description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the Service Organization's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the Service Organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of those controls stated in the description to provide reasonable assurance that the Service Organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditors' Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA.

We applied the statements on quality control standards established by the AICPA and accordingly maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects:

a. The Description presents the Microsoft's system that was designed and implemented throughout the period July 1, 2018 to June 30, 2019 in accordance with the description criteria.

b. The controls stated in the Description were suitably designed throughout the period July 1, 2018 to June 30, 2019 to provide reasonable assurance that Microsoft's service commitments and systems requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls throughout that period.

c. The controls stated in the Description operated effectively throughout the period July 1, 2018 to June 30, 2019, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Microsoft's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the Service Organization, user entities of the Service Organization's system related to NGP-PIMS during some or all of the period July 1, 2018 to June 30, 2019, business partners of Service Organization subject to risks arising from interactions with the NGP-PIMS system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization
- How the Service Organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how they interact with related controls at the Service Organization to achieve the Service Organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the Service Organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the Service Organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Deloitte & Touche LLP

September 19, 2019

Section II:
Management’s assertion

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

Section II: Management's assertion

Assertion of Microsoft Management

We have prepared the description of the system in Section III of Microsoft Corporation ("Microsoft", the "Service Organization") related to its online service throughout the period from July 1, 2018 through June 30, 2019 (the "period") related to Next Generation Privacy – Privacy Information Management System ("NGP-PIMS") service, based on the criteria for a description of a service organization's system in DC section 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* ("description criteria") (description criteria). The description is intended to provide report users with information about the our system that may be useful when assessing the risks arising from interactions with Microsoft's system, particularly information about system controls that Microsoft has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("applicable trust services criteria").

Microsoft uses Microsoft Azure to provide infrastructure as a service cloud services for hosting the NGP-PIMS applications. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria. The description presents Microsoft's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Microsoft's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria. The description presents Microsoft's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Microsoft's controls.

We confirm, to the best of our knowledge and belief, that

a. the description presents Microsoft's system that was designed and implemented through the period, July 1, 2018, through June 30, 2019, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period from July 1, 2018 through June 30, 2019, to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period, July 1, 2018, through June 30, 2019, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of Microsoft's controls operated effectively throughout that period.

Section III:
Description of system

Section III:
Description of the system

Overview of operations

Business description

NGP-PIMS is the Organization effort to address new worldwide privacy regulations, such as the European Union's (EU's) General Data Protection Regulation (GDPR). The GDPR has established a set of privacy standards for companies that handle EU citizen data, including the requirement to enable EU citizens ("data subject") to access or delete their personal data processed within a company. NGP-PIMS aims to provide commercial customers fulfill the need for GDPR compliance for their data subjects. NGP-PIMS is a collection of the following services:

NGP is a group of core services which supports the orchestration of the data subjects' requests to access or delete the personal data within systems across the Organization. NGP's primary functions include:

- aggregation of personal data related information from data sources across the company
- enablement of the execution of data subjects' delete/account close requests across the company
- collection of filed exemptions ("variant"[1])

DataGrid Catalog ("DataGrid") is used as a platform for classifying the data assets including data subject and privacy tags. DataGrid is responsible for maintaining a data catalog which is an inventory of systems and data specific metadata, including client and service telemetry, data processing pipelines, data entities, pipeline configurations, and Microsoft applications.

Applicability of the report

This report has been prepared to provide information on NGP and DataGrid internal controls related to the security and availability trust service criteria.

This report covers the following NGP and DataGrid service components:

- **Personal Data Management Service (PDMS):** PDMS is a service that stores an inventory of personal data assets. Personal data assets include applications, services, and storage systems that process or store personal data. In addition, PDMS stores the variants. All variants are approved by Corporate External & Legal Affairs (CELA) and Regulatory Affairs.
- **Privacy Compliance Dashboard (PCD):** PCD is a user interface for PDMS and is used by data custodians to register the info about the personal data they store. Data custodians are owners of data stores that contain personal data.
- **Privacy eXperience Service (PXS):** PXS is a service that receives and delegates the requests to access or delete personal data stored in various data stores across the Organization. PXS supports access requests by aggregating the data from many systems across the company. In addition, PXS supports the deletion process by authenticating requests from privacy dashboards and transmitting such requests to the Privacy Command Feed, where necessary. PXS relies on Azure Active Directory Request Verifier Service (AAD RVS) for the cross-verification of the request. It then passes the request verifier's token to Privacy Command Feed.
- **Privacy Command Feed (PCF):** Upon receiving the requests from PXS, PCF references PDMS to determine relevant data agents and metadata and inserts the information in data agent queues for

[1] Variant: It is an alternate method of GDPR compliance that does not violate the law but does deviate from the standard NextGen Privacy processes and guidance. All variants are approved by Corporate External & Legal Affairs (CELA) and Regulatory Affairs.

execution. Data agents send responses back to PCF to indicate the successful or unsuccessful execution of the requests. PCF produces an audit log of all export, account-close requests.

- **DataGrid Catalog:** DataGrid Catalog receives metadata from a variety of sources, such as, Windows client, Xbox consoles, services, such as Xbox Live, Office, Bing, and Azure subscriptions, Microsoft Store (store.microsoft.com), and Microsoft applications. Metadata about the datasets[2] are pushed using ingestion pipelines and service Application Programming Interfaces (APIs) to DataGrid Catalog. DataGrid Catalog then parses the assets, adds more meaning by categorizing data into logical groups, displays groups in the DataGrid Catalog user interface, and enables APIs for consumption. Additional details such as data owner and location are added to an asset to make the asset easily discoverable. Stored assets are only accessible to authorized individuals. In addition, DataGrid runs a daily job to collect the result of the scans performed by the DataMap[3] services. If there are any changes to the data asset privacy tags, the updated privacy tags are published back to DataMap for reconciliation.

Infrastructure

NGP and DataGrid services leverage Azure's Platform as a Service (PaaS). Azure's PaaS service offering enforces operating system (OS) protections within the NGP and DataGrid services. The Cloud and Enterprise Security team carries out frequent internal and external scans to identify vulnerabilities and assess the effectiveness of the patch management process. In addition, applicable patches are automatically applied to NGP and DataGrid VM scale set[4] via the Azure PilotFish[5] service.

Network layer protections, such as Incident Management (IcM), Configuration Management, Access Management, and Change Management, related to network devices are managed by Azure in coordination with NGP and DataGrid services.

Azure is responsible for physical and environmental security for the infrastructure. Main access to the datacenter facilities are restricted to a single point of entry manned by security personnel. The main interior or reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. In addition, rooms that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are restricted through various security mechanisms, such as electronic card access control, keyed lock on each individual door, mantraps, and / or biometric devices.

Software

In addition to the services described in the Applicability section above, the following utility software is used by the team to execute controls relevant to the NGP and DataGrid systems:

- **IDWeb** – Microsoft's corporate instance of Microsoft Identity Manager. The tool is leveraged to enforce role-based access and least privilege permissions using the AAD security groups.
- **OneIdentity** – An Identity and Access Management (IAM) tool that provides self-serve domain account provisioning and management to all C+E managed domains.
- **MyAccess** – An Identity & Access Management solution that delivers a governance-based approach to access management, compliance and provisioning processes for on-premise and cloud environment. It allows you to submit access requests to Microsoft resources and gathers approvals from management to enable access in a timely manner.
- **PilotFish** – A service that provides an Autopilot cluster co-located with Azure in every Azure region within Azure's compliance boundary. Autopilot is the data center infrastructure stack and service management layer for Microsoft. By leveraging PilotFish, services can automate the setup and pre-configuration of new devices within their environment. PilotFish is also used to perform vulnerability scanning and patch management.

---

[2] Dataset: It is a collection of data points that can be used to describe an entity.

[3] DataMap: See section Software for additional information.

[4] VM scaleset: Azure virtual machine scale sets let the user create and manage a group of identical, load balanced, and autoscaling virtual machines.

[5] PilotFish: See section Software for additional information.

- **Azure DevOps** – Automated configurations are placed within NGP and DataGrid deployment and source code management tool, Azure DevOps, to enforce multiple levels of code review and approval prior to deploying a change to production.
- **Incident Management tool (IcM)** – It is an incident management tool offered by Azure and is used to generate, assign, and track the security incidents. Incident tickets are created with severity and remediation steps in the case of an event. Incident tickets are tracked within the tool until the issue is resolved.
- **xPert** – It is an agent that resides on NGP and DataGrid servers and monitors the availability and capacity of the services. Alerts are configured based on defined thresholds and events to create IcM tickets.
- **XTS** – XTS is an access management tool and is used to provision elevated access; i.e., just-in-time (JIT) access, to the PilotFish environments. The JIT access provisioned through XTS expires within defined timeframe and is limited to one server per request.
- **Code Flow** – It is a tool integrated with PilotFish that enforces review and approval of a code change prior to deployment of the change in production.
- **Akamai portal** – It is the system resiliency dashboard used by services to configure the failover process.
- **Yabby** – A Microsoft internal tool that facilitates the automatic deployment of code to Azure hosting services.
- **CredentialScanner.exe (CredScan)** – It is a tool used to harden code security by checking for authentication information built in or hard coded into the logic as part of the code check in process. If the tool identifies credentials or authentication information, it flags the volition during the code commit process and prevents the code check in.
- **Cosmos** – Cosmos is Microsoft's internal big data platform that supports distributed storage, queries, and data analytic procedures.
- **DataMap** – DataMap is an application that leverages the services and infrastructure provided by ScopeScan. ScopeScan in turn is a process that analyzes the Scope scripts that have been run within the Cosmos environment and builds what is called the Base Data Graph (BDG). The BDG is a representation of the collection, transformation and storage of information operations that have taken place in the Cosmos virtual clusters over time. Once the BDG has been updated, it is analyzed according to the rules that have been codified into the DataMap database tables, and the results of this analysis are stored in a different table in the same DataMap database.
- **Azure EventHub** – Azure Event Hubs is a hyper-scale telemetry ingestion service that collects, transforms, and stores millions of events. As a distributed streaming platform, it gives you low latency and configurable time retention, which enables you to ingress massive amounts of telemetry into the cloud and read the data from multiple applications using publish-subscribe semantics.
- **Azure Notification Hubs** – Azure Notification Hubs provide an easy-to-use and scaled-out push engine that allows you to send notifications to any platform (iOS, Android, Windows, Kindle, Baidu, etc.) from any backend (cloud or on-premises).
- **Azure Active Directory (AAD)** – Microsoft's cloud-based identity and access management service which manages user's access to internal and external resources.
- **MSGraph** – MSGraph provides privacy APIs used by commercial customers to interact with the NGP system to send the data subject requests for execution.

People

NGP and DataGrid personnel are organized into a) service teams that develop and maintain the application and b) centralized support teams that provide supporting services for system operations. Each team has defined responsibilities and accountabilities related to the security and availability of the services. The service teams include the following groups:

- Compliance Services: responsible for development and maintenance of the PXS, PCF, and PDMS systems, and the PCD dashboard
- DataGrid: responsible for development and maintenance of the DataGrid Catalog.

The centralized support teams provide specialized functions, including the following:

- Business Continuity Management – Provides a single resource to assist service teams to analyze continuity and disaster recovery requirements, document procedures, and test the of established procedures for the business continuity and disaster recovery of the services.
- COSINE, Devices, and Gaming (CDG) Security – Manages cross-platform security functions, such as security incident response, security monitoring, and vulnerability scanning.
- Commerce Services & Compliance (CSC) – Identifies, documents, and advises service teams to identify risks, design and implementation of mitigating controls, and maintain regulatory and compliance requirements and commitments to the internal stakeholders and external customers.
- Azure Identity Management (IDM) – Operates the IDM tool to provide access control automation for the services.
- Core Services Engineering (CSE) – Provides the access control and authentication mechanism for NGP and DataGrid systems via IDWEB system.
- Cloud & Enterprise – Provides authentication infrastructure, such as Azure Active Directory services, PilotFish, Microsoft Organization ID, AAD, AAD RVS, CosmosDB[6], DataMap, and IcM.
- CDG Data and Analytics Team: Provides tools for event monitoring, including xPert.

Procedures

NGP and DataGrid services adhere to Microsoft's security policy that is owned by the Information Risk Management Council (IRMC), comprising business and security leaders across the company, and approved by the IRMC chair, who is also the Chief Information Security Officer for Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses:

- Human resources (HR) security
- Access control
- Physical and environmental security
- Communications security
- Compliance
- Supplier relationships
- Business continuity management
- Asset management
- Cryptography
- Operations security
- Systems acquisition, development, and maintenance
- Information security incident management

[6] Azure Cosmos DB: Microsoft's proprietary globally-distributed multi-model database service for managing data at planet-scale.

Data

Data is maintained in Azure services and server databases. Each service team and support team is responsible for managing security and availability of the data on the database servers. Reference the table below for the defined data classifications for this report and the NGP-PIMS environment.

Data classification	Definition
Access control data	Data used to manage access to administrative roles or sensitive functions.
Customer content	Content directly created by users. Content is not viewed by Microsoft personnel, unless required to resolve a ticketed service problem.
End-user identifiable information (EUII)	Data unique to a user or generated from a user's use of the service. • Linkable to an individual user • Does not contain customer content
Organization identifiable information (OII)	Data that can be used to identify a particular tenant (generally configuration or usage data). • Not linkable to an individual user • Does not contain customer content
System metadata	Data generated in the course of running the service, which is not linkable to an individual user or tenant and does not contain customer content, EUII, OII, or account data.
Account data	Administrator data Payment data Support data

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, and Monitoring

Control environment

Integrity and Ethical Values

Corporate governance at Microsoft starts with an independent board of directors that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the company. Corporate governance at Microsoft serves several purposes:

- To establish and preserve management accountability to Microsoft's owners by distributing rights and responsibilities among Microsoft board members, managers, and shareholders.
- To provide a structure through which management and the Board set and attain objectives and monitor performance.
- To strengthen and safeguard a culture of business integrity and responsible business practices.
- To encourage the efficient use of resources and to require accountability for the stewardship of these resources.

Further information about Microsoft's general corporate governance is available on the Microsoft website.

Microsoft's Standards of Business Conduct

Microsoft's Standards of Business Conduct (SBC) reflect a commitment to ethical business practices and regulatory compliance. They summarize the principles and policies that guide Microsoft's business activities and they provide information about Microsoft's Business Conduct and Compliance Program. The SBC was developed in full consideration of the Sarbanes-Oxley Act of 2002 (SOX) and proposed NASDAQ listing requirements related to codes of conduct. The Office of Legal Compliance (OLC) updates the SBC as necessary and the code is made available to all employees on the intranet.

SBC training and awareness is provided to Microsoft employees, contractors, and third parties on an ongoing basis to educate them on applicable policies, standards, and information security practices. Full-time employees must also take a mandatory SBC training course within the first 60 days of their start date and then again on an annual basis thereafter.

Further information about Microsoft's SBC is available on the Microsoft website.

OLC – Business Conduct Hotline

There is a confidential and anonymous Business Conduct Hotline available for employees to report issues. The hotline is accessible 24 hours per day and seven days per week through email, phone, fax, and mail. The individual may also send a letter or fax reporting the concern to Microsoft's Director of Compliance. Employees are instructed that it is their duty to promptly report any concerns of suspected or known violations of the Code of Professional Conduct, the SBC, or other Microsoft policies or guidelines. The procedures to be followed for such a report are outlined in the SBC and the Whistle-Blowing Reporting Procedure and Guidelines in the *Employee Handbook*. Employees are also encouraged to communicate the issue to their manager, their manager's manager, their CELA contact, their HR contact, or the Compliance Office.

Hiring

Microsoft hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities involved in the job, background characteristics needed to perform the job, and personal characteristics required. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make appropriate hiring decisions.

Background Checks

Due to international regulations prohibiting background checks, international employees are exempt from the background check process. For US citizens, backgrounds checks are required before full-time employees and vendors are granted access to the corporate network. Background checks are valid for two years.

Vendors/Contractors: Vendor companies are responsible for providing Microsoft with evidence showing that a valid background check has been performed for each contracted vendor. Once completed, Microsoft receives an attestation letter from the vendor company confirming the validity of the vendor's background check. Once the background check validation is received, Microsoft HR enters relevant information into ECS.

Workload administrators configure requirements, including background check, for eligibilities within each work stream. If no background check is on file, or if a background check has expired, the user receives an error indicating that the employee does not have required background check, thus preventing the employee or vendor from obtaining those eligibilities.

Training

NGP and DataGrid services leverage the Microsoft Corporate SBC to provide employees with education and resources to make informed business decisions and act on their decisions with integrity. SBC training and awareness is provided to Microsoft employees, contractors, and third parties on an ongoing basis to educate them on applicable policies, standards, and information security practices. Full-time employees must also take a mandatory SBC training course within the first 60 days of their start date and then again on an annual basis thereafter.

NGP and DataGrid personnel are required to participate in Microsoft's mandatory security and privacy trainings including Security 101 and Privacy 101. In addition, NGP personnel are required to participate in Microsoft Security 201 and Privacy 201 trainings.

Accountability

All NGP and DataGrid staff and contingent staff are accountable for understanding and adhering to the guidance contained in the Microsoft Policies and applicable supporting standards. Individuals not employed by NGP, but allowed to access, manage, or process information assets of the NGP system are also accountable for understanding and adhering to the guidance contained in the Microsoft Policies and applicable supporting standards.

Performance Reviews

Microsoft employees create individual core priorities that align with those of their manager, organization, and Microsoft, and are supported with customer-centric actions and measures so that everyone is working toward the same overarching vision. These core priorities are established when an employee is hired, and then updated throughout the year according to business needs.

Periodically, performance reviews, called "Connects," are held between employees and their managers, during which progress is analyzed against accountabilities and accountabilities are adjusted, if needed. The manager evaluates the individual's contributions to the team and business or customer impact, taking into consideration contributions toward creating a high-performing team and the demonstration of competencies relevant to his/her role, which can include an individual's internal control responsibilities.

Microsoft organization guidance requires that "Connects" be performed a minimum of two times a year; however, each group may adjust the timing of these reviews throughout the year to coincide with its business processes.

OLC - Board of Directors and Senior Leadership

The OLC designs and provides reports to the board of directors on compliance matters. The OLC also organizes annual meetings with the Senior Leadership team for its compliance review.

Internal Audit (IA) Department

Microsoft has an IA department that reports directly to the Audit Committee (AC) of the board of directors, which is constituted solely of independent directors. IA has a formal charter that is reviewed by the AC and management. The responsibilities of IA include performing audits and reporting issues and recommendations to management and the AC.

AC

The AC charter and responsibilities are communicated on Microsoft's website, www.microsoft.com. The AC meets privately on a quarterly basis with Microsoft's external auditors and IA. The topics for the quarterly AC meetings are found in the AC Responsibilities Calendar sent out in the charter. In addition, the AC influences the company through the IA function. The AC reviews the scope of IA and advises on the process of identifying and resolving issues. Lastly, the AC monitors itself by completing an annual self-evaluation.

Information and Communication

Internal Communication

Responsibilities concerning internal control are communicated broadly, which includes monthly controller calls, all-hands meetings run by the CFO, and update conference calls held by the Financial Compliance Group (FCG) with the Sarbanes-Oxley extended project team. Responsibilities for compliance with policies are set out in the SBC for which mandatory training has been established for all employees. Additionally, compliance manager meets with the control owners to make sure they understand the controls for which they are accountable and update the controls based on changes in the business environments.

Office of the CFO – Communications External to the Company

CFO communications outside the company occur throughout the year and, where applicable, these external communications include discussions of the company's attitude toward sound internal controls. The office of the CFO is responsible for a number of communications outside of Microsoft, including quarterly earnings releases, financial analyst meetings, customer visits, outside conferences, and external publications.

Policies

All NGP, DataGrid, and contingent staff are accountable for understanding and adhering to the guidance provided in Microsoft policies and applicable supporting standards. These policies define accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification, asset management, risk assessment, access control, incident response, business continuity, cryptography, system development, training, and where to go for additional information. These policies are available on the Microsoft intranet.

In addition to the Microsoft-wide Security Policy, CSC team has established the change management policy, which is communicated to the NGP and DataGrid team members via CSC's SharePoint site.

Business Planning

The NGP and DataGrid planning process is driven by GDPR compliance regulation that went into effect on May 25, 2018, in addition to product requirements from our internal partners. Senior management defines the vision and strategy for the overall NGP and DataGrid product on an annual basis. During this process, senior management considers its high-level commitments and requirements to security, availability, confidentiality, and processing integrity in a series of planning meetings and communicates the output to NGP and DataGrid teams through email announcements and all-hands meetings. NGP's and DataGrid's Engineering and Program Management team leads also consider their teams' commitments to security, availability, processing integrity, and confidentiality on a more specific level and translate the outcome into engineering scenarios, deliverables, and tasks that are scheduled into release sprints. In addition, DataGrid security v-team has been established, which is responsible for managing security, availability, confidentiality, and processing integrity within the DataGrid system. Finally, a CSC risk team has been defined and provides guidance for managing compliance related to security, availability, processing integrity, and confidentiality controls within the NGP and DataGrid

environments. Each team works to implement and maintain the commitments for security, availability, processing integrity, and confidentiality.

Customer Commitments and Responsibilities

Externally, NGP and DataGrid communicate their commitments, including those related to regulations, security and availability to customers via email announcements and NGP Program Update meetings. Customers are required to provide and maintain their own front-end portal, which is used by tenant admins, to initiate the data subject requests.

Customers are responsible to manage and monitor tenant admins' access to the front-end portal.

Information regarding the design and operation of NGP and DataGrid systems, including a description of the system, the system's boundaries, roles and responsibilities of internal users, and resources is available on Microsoft intranet (SharePoint sites). In addition, system description details are available through third-party audit and attestation reports.

System Description

Data Asset Registration Process

Currently, DataGrid Catalog includes more than 40 different data assets types. The sources for different types of data asset MetaData include: (a) DataMap that scans for the asset types, including Cosmos, Kusto[7], Object Store[8], Substrate[9], and SQL and (b) Microsoft employees and contractors who have access to the DataGrid portal publishing metadata. PDMS makes a call to DataGrid catalog to validate the data asset being registered in PDMS.

Export Request Process

The data subject request for export is initiated by tenant admins[10]. Once the request is initiated, it is authenticated by MSGraph and eventually gets submitted to the NGP system, where it is further authenticated and signed by AAD RVS. AAD RVS is a service provided by Azure and is used by the PXS to sign the data subject request to maintain the integrity of the request throughout the execution of the request. Once authenticated, the request is sent to PCF. PCF publishes these requests to all the subscribing data agents[11] owned by data custodians[12]. Data agents handle the request from PCF and process the request through Cosmos and nonCosmos data stores.

For nonCosmos workflow, once export request is processed, the data is copied to partner-provided location based on the Shared Access Signature (SAS)[13] write token, which was received in the request.

For Cosmos workflow, once the export request is processed, the data is copied to NGP-owned Cosmos staging area. From this area, the export data is copied by PXS, to partner-provided location based on the SAS write token, which was received in the request.

The request status is logged by PCF in CosmosDB and Azure Blob storage. PXS may query PCF for request status as needed. Once the request completes, tenant admins via the partner portal can download export data.

---

[7] Kusto: Kusto is an internal Big Data log search and text analytics cloud service.

[8] Object Store: Object Store is an internal distributed storage, being used for real-time scenarios.

[9] Substrate: Substrate is a data and intelligence platform that enables internal partners to build; deploy; and maintain compliant, productivity apps and services.

[10] Tenant Admins: A data processor acting on behalf of a data subject, who is an organization employee or member. Tenant admin initiates data subject requests (export or account close).

[11] Data Agents: Code or Script owned by data custodians that run on various data stores (Cosmos, SQL Server, Files, etc.) containing the customer's personal data. Data agents subscribe to Export and/or Account-Close signals published by PCF.

[12] Data Custodians: A role defined for the data owners that own customer's personal data in their data stores and are responsible for registering their data assets in DataGrid and data agent information in PDMS.

[13] SAS: A shared access signature provides delegated access to resources in the storage account. It is a secure way to share the storage resources without compromising the account keys.

Account-close Process

The data subject request for account-close is initiated by tenant admins. Once the request is initiated, it is authenticated by the MSGraph and submitted to the NGP system, where it is further authenticated and signed by the AAD RVS. Once authenticated, the request is sent to PCF for nonCosmos workflow and to PDMS data agent for Cosmos workflow. PCF stores the status of the request in CosmosDB for nonCosmos workflow.

There are two types of the account-close process: Cosmos and nonCosmos.

For Cosmos workflow, PXS pulls data agent and asset server information from daily dump of PDMS config in Cosmos and writes the data into an account-close request stream. Cosmos delete processors read the stream metadata from DataGrid and the account-close request stream to produce an account-close script to remove data for that tenant's streams.

For nonCosmos workflow, periodically, registered data agents poll PCF API from PXS service to get latest account-close requests. Each agent is on its own cadence. Sometimes these are in a constant polling or long-poll mode. Others may only poll once every few hours (usually less than 24 hours). Each data agent deletes data from its known stores that match the account-close request. This is usually one system or subsystem.

Once the request (cosmos or non-cosmos) completes, these data agents write to the audit log in NGP-owned Cosmos virtual cluster for audit purposes.

Variant

A variant must be approved by CELA. An approved variant is entered in PDMS by NGP policy managers. PDMS writes the variant request to a Cosmos stream as part of PDMS configuration and is read by PCF, which enables delete agents to read and exclude variants when processing the account-close requests.

Dataflow Diagram

Dataflow diagrams that depicts in-scope NGP and DataGrid environments and the key supporting services are documented and maintained by the CSC teams with the assistance of members of the NGP and DataGrid product support teams.

Risk Assessment

Enterprise Risk Management (ERM) Risk Assessment

The Microsoft ERM team provides management and accountability of Microsoft short- and long-term risks. ERM collaborates with IA, the Financial Compliance group, Operations, and Legal and Compliance groups to perform a formal risk assessment. These risk assessments include risks in financial reporting, fraud, and compliance with laws.

IA Risk Assessment

IA and other groups within Microsoft perform periodic risk assessments. These assessments are reviewed by senior management. IA specialization area leaders determine high-priority risks across the company, including risks related to financial reporting, operational business processes, and systems controls. Control failures are also analyzed to determine whether they give rise to additional risks.

CSC Risk Assessment

In addition to the above Microsoft-wide risk assessments, CSC conducts a risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, and availability commitments specific to the organization. Risks that are identified are reviewed and approved by CSC management at least quarterly. In addition, risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. The results from this risk assessment are rolled into the company-wide risk assessment owned by ERM defined above.

OLC/IA/Risk Management – Risk Responsibility

The responsibility for risk is distributed throughout the organization based on the individual group's services. OLC, IA, and the ERM team work together to represent ERM across the company. Through quarter- and year-end reviews, the CFO and Corporate Controller (and respective groups) review the disclosures and issues that may have arisen.

Control Design and Implementation

Based on the risk assessment performed, control activities are put in place within the NGP and DataGrid control frameworks. The control frameworks are managed by the CSC group and evaluated at least on an

annual basis. This evaluation includes input from changes to the overall NGP or DataGrid environment, the regulatory landscape, and results of control assessments.

Software Development Life Cycle (SDLC Process)

NGP and DataGrid follow the standard Microsoft SDLC. The Microsoft SDLC includes the following requirements:

- Project Requirements/Design
- Implementation
- Testing Verification
- Final Approval

Based on established plans for product releases and specifications, features are developed and designed for release. There is an assigned feature crew for each service that includes developers and program managers. Feature crews propose changes, which are submitted for approval by the applicable stakeholders. Features are developed and tested according to the SDLC. Prior to releasing a new feature, the feature must be approved by a Team Lead and a Technical Lead, which can be the same individual in certain circumstances. If approved, signifying that the release has passed all appropriate testing and that it meets the specifications and requirements, the feature is scheduled to be automatically deployed into the production environment for the NGP system. Approved changes are manually deployed for DataGrid system.

Secure Development Life Cycle (SDL)

NGP and DataGrid follow the standard Microsoft SDL process, which includes, at a minimum, risk assessment, testing, approval, and documentation. The SDL process includes security, availability, confidentiality, and processing integrity development requirements, which are intended to reduce the number of security-related bugs that appear in the design, code, and documentation associated with a software release, as well as to detect and remove those bugs as early in the SDLC as possible.

For any major change in the system, a security review and risk assessment is performed by CSC, CDG Security and/or C+AI Security CDG, and the Microsoft Legal team. The SDLC is followed for the development, build, test, and deployment processes. The end-to-end process is tracked through Azure DevOps.

Access Management

Access to NGP and DataGrid services, related data stores, code base, and deployments must be authorized, conform to CSC's access management policies and procedures, and aligned with the Role-Based Access Control (RBAC) Model. RBAC model is implemented within NGP and DataGrid systems to enforce the concepts of least privileged access and the segregation of incompatible duties.

The NGP and DataGrid source code is stored within Microsoft's instance of Azure DevOps GIT. Access to check in the source code is limited to authorized personnel. In addition, write access to the source code repository is reviewed on a quarterly basis.

Asset Management

NGP and DataGrid maintain an inventory of Azure subscriptions, service descriptions, and owners through Microsoft's corporate asset management tool, Service Tree. An inventory of all resources residing within each NGP and DataGrid Azure subscription is maintained within the Azure Portal.

Authentication

NGP and DataGrid systems use the Microsoft's instance of AAD /corporate active directory infrastructure for centralized authentication and authorization to the systems.

Identity Access Management

NGP and DataGrid leverages the Microsoft corporate instance of Microsoft Identity Manager, referred as IDWEB, which is managed by the Microsoft CSE group. This tool is leveraged to enforce RBAC permissions and least privilege within the NGP environment using the AAD security groups.

New User/Modification of User Access

The process to request and approve new access to NGP and DataGrid is managed through a manual workflow process by adding users to security groups. Once a user requests access to a security group through IDWEB, IDWEB automatically notifies the appropriate security group approvers via email that a request is pending his or her approval. Once the approver approves the request, the tool automatically assigns the user the appropriate membership for that security group.

Termination User Access Removal

When individuals leave the company, Microsoft HR updates the terminated employee's details in the HR system. Through an automated batch process, the terminated employee's access is removed from the Microsoft corporate network and corresponding security groups within 24 hours.

Periodic User Access Review

Periodic reviews of individual accounts and security group memberships within the NGP and DataGrid environment are performed by the NGP and DataGrid leads on a quarterly basis, to evaluate whether access is still required. Removal of user access is taken in a timely manner, as necessary, based on the review.

JIT Access

JIT tools allow individuals to request temporary elevated access privileges on an as-needed basis to privileged areas within the NGP and DataGrid production environment. The JIT approvers will review the access request and approve if deemed appropriate. When approved, the requesting user is granted access for a temporary basis, typically for under 24 hours as defined in the request itself, and the tool automatically removes the requested access upon expiration. Further, JIT access is being logged each time a person elevate access and quarterly a review of all related JIT access to the service is being performed to confirm that appropriate justification is in place for using the JIT access and that appropriate and authorized users were elevating their access to the service.

Developer / Operations Model – Developer Access to Production

NGP and DataGrid developers can get temporary access to production through the use of the JIT tools described above. Developer access is limited to specific areas of the environment for operations purposes, such as troubleshooting.

Automated configurations are in place within NGP to perform automated deployment through the Yabby tool to implement changes to production. DataGrid, however, uses manual deployment process where source code management tool, Azure DevOps, is used to enforce multiple levels of code review and approval prior to deploying a change to production.

In addition, NGP and DataGrid also use the CodeFlow tool to enforce at least one reviewer, other than the developer to review and approve the code changes prior to implementation.

The objective of these controls is to prevent inappropriate changes from being applied to production.

Mobile Devices

For Microsoft employees and other internal users, access to the NGP and DataGrid system via mobile device is restricted and the corresponding controls are managed by Microsoft's CSE organization.

Logical Security

Encryption of Customer Data in Transfer

Tenant restricted data is encrypted when transmitted between the customer and Microsoft, as well as when transmitted between Microsoft datacenters, in accordance with Microsoft Security Program Policy (MSPP).

Microsoft uses Secure Sockets Layer (SSL) encryption for establishing an encrypted link between the client and the Microsoft datacenters. Encryption protocol is applied in accordance with MSPP.

Microsoft leverages SSL and Azure for establishing an encrypted link between datacenters. Encryption protocol is applied in accordance with MSPP. Azure manages the configurations for encryption, while NGP and DataGrid manage the specific encryption keys. Access to the encryption keys are included in the periodic access reviews.

Key Management

NGP and DataGrid adhere to Online Services Security Standards (OSSS) for encryption key management. If the content of this policy conflicts with any other Microsoft security policy, the stricter of the policies apply. Upon creation, the services encryption keys are securely encrypted using PilotFish secret store. The encrypted keys are stored in the GIT repository and all copies of the key are immediately deleted. Access to decrypt the keys are restricted to authorized personnel.

To ensure compliance with key management, credential monitoring is used during NGP's SDL, which is intended to identify a breach in key confidentiality. NGP's Production environment uses different encryption keys than those found within Development and Test environments. Encryption keys are rotated on a periodic

basis in accordance with OSSS. Where these standards conflict with the Microsoft Security Policy, the stricter of the policies are applied to ensure proper and effective use of cryptographic confidentiality.

Data Segregation

Based on the system architecture, tenant's export data is copied directly from the Data Custodians' systems to the tenant's instance of Azure through the tenant-supplied SAS write token. The SAS write token is provided as part of the initial data subject request.

Azure Virtual Machine (VM) Scale Sets

NGP and DataGrid use EAP V2[14] deployment to deploy VMs to the PilotFish and no pre-provisioning of VMs is required.

Antivirus/Antimalware

NGP and DataGrid leverages Azure's PilotFish service to automatically provision all servers with an OS image that includes the System Center Endpoint Protection (SCEP) antivirus/antimalware service. This OS image is applied to the entire NGP Azure VM scale set automatically. The antivirus/antimalware agent is configured to obtain the latest available definition from Azure.

Patch Management

NGP and DataGrid leverages Azure's PilotFish service to enforce patch management for the VM scale set. Autopilot-managed servers run a Windows Server Enterprise SKU as the base OS image. The OS images for all Autopilot-managed machines are created, managed, and supported by Autopilot. The Autopilot team is responsible for these OS-related processes, including the base OS image creation and the upgrade of machines into the newly available OS image. This includes upgrading to major OS versions, as well as to incremental releases, such as service packs and patches.

Vulnerability Scanning and Security Monitoring

Microsoft's CDG Security Operations team uses Qualys to monitor assets and assess vulnerabilities across the CDG organization, including the NGP and DataGrid system. To ensure that NGP and DataGrid systems are appropriately monitored for security vulnerabilities, the CDG Threat Vulnerability Monitoring Qualys agent is installed on all NGP and DataGrid VMs. In addition to Qualys, Microsoft's CDG Security Operations team leverages additional telemetry collection in the Azure Cloud to identify and monitor OS-related security events. The NGP and DataGrid teams periodically reviews the vulnerability scan report from the CDG Security Operations team, assesses the criticality of the vulnerabilities, and resolves vulnerabilities when appropriate. Additional vulnerability scanning is performed through Azure via the PilotFish service, in which well-known OS and application vulnerabilities are scanned on a monthly basis.

Penetration Testing

NGP and DataGrid coordinate with the CDG Security Operations team to conduct an internal or external penetration tests annually or after any significant infrastructure changes. Corrective action, if required, is performed in a timely manner.

Network Management

NGP and DataGrid leverages Azure to ensure appropriate controls are in place to protect the network-layer, including, but not limited to IcM, Configuration Management, Access Management, and Change Management for network resources.

Data Flow Diagrams

The system data flow diagrams are reviewed and updated by NGP and DataGrid Engineering teams with input from the CSC team at least annually or upon significant changes in the system design. This review is performed to provide up-to-date NGP and DataGrid system design information to personnel to support their understanding of their role in addressing security, availability, processing integrity, and confidentiality within the systems.

[14] EAP V2: Elastic Autopilot (EAP) is a turnkey solution to run services built for the Autopilot service model on public Azure cloud. The Azure VMs provisioned for EAP will be co-managed by Azure and Autopilot stacks.

Capacity and Availability Monitoring

Processing capacity and availability are monitored by Service teams through a centralized dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.

In addition to the above monitoring, monthly the NGP teams prepare an overview of the service team's capacity, availability, and resiliency from the prior month for the NGP senior management team. This overview presents the root cause of anomalies or deviations to senior management and based on the meeting issues or changes to capacity and availability are tracked to resolution. Annually, NGP senior management reviews and approves the capacity for NGP and systems.

DataGrid team performs the review on a quarterly basis.

Monitoring of Controls

Security and Compliance Monitoring

NGP maintains reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect commercial data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

The effectiveness of security, availability, processing integrity, and confidentiality controls are analyzed by independent auditors at least annually. These assessments include external (e.g., International Organization for Standardization (ISO) and SOC2 audits) and internal evaluations (e.g., risk assessments and vulnerability scans). The results and findings from these assessments are addressed with corrective actions, which are tracked by the CSC team to substantiate that they are addressed in a timely manner.

IA

Microsoft's IA department provides support to management across the company by independently and objectively analyzing whether the objectives of management are adequately performed, as well as facilitating process improvements and the adoption of business practices, policies, and controls governing worldwide operations.

Monitoring of Subservice Organizations

Microsoft NGP uses the following subservice organization:

- Microsoft Azure provides the PaaS services for the NGP and DataGrid systems, including authentication (AAD, AAD RVS and MS Graph), virtual server hosting, data storage, as well as the physical servers, patch management, and network infrastructure that support those services.

The NGP and DataGrid teams are responsible for identifying dependencies of each service and monitoring the subservices' implementation of agreed-upon security, availability, processing integrity, and confidentiality controls. Monitoring includes, but is not limited to, the review of third-party service auditor reports, analyze the impact of identified deficiencies, evaluate CUECs and discussions with subservice organization management, where necessary.

Business Continuity and Disaster Recovery

Microsoft has established an organization-wide Enterprise Business Continuity Management framework. The program includes Business Continuity Policy, Implementation Guidelines, Business Impact Analysis, Risk Assessment, Dependency Analysis, Business Continuity Plan (BCP), IcM Plan, and procedures for monitoring and improving the program. The Business Continuity Management (BCM) Program Manager also manages the program for the Azure. Azure datacenter Service Resiliency (SR) program is coordinated through the datacenter SR Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics.

All datacenters are required to at least annually, exercise, test, and maintain the Datacenter BCP for the continued operations of critical processes and required resources in the event of a disruption.

NGP Service is Active/Active between Microsoft datacenters within North America, Europe, and Asia. NGP is a collection of four services: PDMS, PXS, PCF, and PCD.

DataGrid Catalog has a geo-redundant design and it runs in an active/passive configuration. If the primary datacenter, or DataGrid components within that primary datacenter, fails or is inaccessible, then the DataGrid team will manually failover using Akamai to the secondary datacenter. Additionally, weekly backups of the Elasticsearch cluster are stored in Azure and may be restored if needed. The DataSync service maintains 10 days of updates to the Elasticsearch cluster, so the cluster data maybe reapplied to bring the data to current.

Access to the NGP and DataGrid properties through Akamai portal is limited to appropriate individuals based on the job responsibilities. User access is reviewed on a quarterly basis. Failover requirements are configured in Akamai portal and the access is limited to authorized administrators. The Akamai activity log is reviewed on a quarterly basis to determine changes to the DataGrid and NGP properties were appropriate and authorized.

Annually, NGP and DataGrid review and test their BCPs for their relevant services.

Data Replication

Data for the NGP-PIMS system is replicated for redundancy and disaster recovery purposes by Azure. Data redundancy is achieved through fragmentation of data into extents, which are copied onto multiple nodes within each Azure region.

Elastic Search (DataGrid's metadata), is manually backed up in Azure storage on a weekly basis. DataGrid Engineering team initiate the weekly backup and the backup is retained for two months.

Changes during the period

There have been no changes in the control activities during the period.

Trust Criteria and related control activities

Trust criteria mapped to the related control activities is documented below. These control activities include preventive, detective, and corrective policies and procedures that help NGP-PIMS identify, decrease, manage, and respond to risk in a timely manner.

Complementary User Entity Controls considerations

Microsoft's NGP-PIMS system and the controls over that system were designed with the assumption that certain controls are in operation within the user entity organizations. This section describes those controls that should be in operation at user entity organizations to complement the controls of NGP-PIMS. The following list contains controls that NGP-PIMS assumes their user entities have implemented. User organization auditors should determine whether the user entities have established sufficient controls in these areas:

Complementary User Entity Controls	Relevant SOC 2 Control Criteria
CUEC-01: User entities properly administer users' access to the resources and monitor continued appropriateness of access.	**CC6.1, CC6.2, and CC6.3**
CUEC-02: User entities establish proper controls over the use of system IDs and passwords.	**CC6.1, CC6.2, and CC6.3**
CUEC-03: User entities manage the security and access to the tenant's Azure Blob storage.	**CC6.1, CC6.2, and CC6.3**

Complementary Subservice Organization Controls

Microsoft's NGP-PIMS controls related to the system detailed in this report cover only a portion of overall internal control for each user entity of NGP-PIMS. It is not feasible for the related control criteria to NGP-PIMS to be achieved solely by Microsoft. Therefore, in conjunction with NGP-PIMS's controls, a user entity must take into account the related Complementary Subservice Organization Controls (CSOC) expected to be implemented at the subservice organizations as follows.

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant SOC 2 Control Criteria
PaaS logical security	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting NGP-PIMS and DataGrid.	**CC5.1, CC6.1, CC6.2, and CC6.6**
PaaS physical security	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over physical access to the facilities, including data centers, supporting NGP-PIMS and DataGrid.	**CC6.4, CC6.5**
PaaS network security	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices.	**CC6.7**

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant SOC 2 Control Criteria
PaaS physical security	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over environmental protection of systems, including natural disasters and man-made threats, for infrastructure supporting NGP-PIMS.	**CC6.6, CC6.7**
PaaS logical security	Microsoft Azure	Microsoft Azure is responsible for monitoring and addressing security events and incidents related to the NGP-PIMS systems hosted on Azure platform services.	**CC7.3**
PaaS physical security	Microsoft Azure	Microsoft Azure is responsible for controlling that all Datacenters are required to at least annually, exercise, test, and maintain the Datacenter BCP for the continued operations of critical processes and required resources in the event of a disruption.	**CC7.5 and A1.3**
PaaS data replication	Microsoft Azure	Microsoft Azure is responsible for geographic replication and backups for NGP-PIMS systems hosted on Azure platform services.	**CC7.2 and A1.2**
PaaS change management	Microsoft Azure	Microsoft Azure is responsible for the maintenance and change management of the infrastructure and supporting systems that support their PaaS where NGP-PIMS and DataGrid are hosted.	**CC8.1**
PaaS logical security	Microsoft Azure	Microsoft Azure is responsible for the account close and delete requests authentication to validate the request is submitted by an authorized tenant admin.	**CC6.1 and CC6.2**
PaaS network security	Microsoft Azure	Microsoft Azure is responsible for network filtering implementation to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components.	**CC6.6 and CC6.7**
PaaS logical security	Microsoft Azure	Microsoft Azure is responsible for the password configuration and authentication processes for NGP and DataGrid in accordance with Microsoft security policy.	**CC6.1**
PaaS network security	Microsoft Azure	Microsoft Azure is responsible for processing capacity and use of system components for NGP-PIMS systems hosted on Azure platform services.	**A1.1**
PaaS data security	Microsoft Azure	Microsoft Azure is responsible for the encryption configurations for customer data being transmitted and while at rest.	**CC6.1, CC6.6, and CC6.7**

Principal Commitments and Requirements

Microsoft makes commitments and has established requirements for its products and services. The principal commitment for NGP-PIMS is to conform to internal organizational commitments for products and services to create a consistent level of compliance across all Microsoft environments. These commitments include the areas of logical and physical access security, system operations, change management, risk mitigation, and availability that are met through this report. These internal commitments when met, allow the NGP-PIMS environment to interact with other environments across Microsoft in a compliant manner.

Section IV:
Information Provided by Independent Service Auditor, Except for Trust Services Criteria and Control Activities

Section IV: Information Provided by Independent Service Auditor, Except for Trust Services Criteria and Control Activities

Introduction

This report, including the description of tests of controls and results thereof in this section are intended solely for the information and use of Microsoft Corporation ("Microsoft"), user entities of the NGP-PIMS system during some or all of the period July 1, 2018 through June 30, 2019, and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following: the nature of the service provided by the service organization; how each service organization's system interacts with user entities, subservice organizations, and other parties; internal control and its limitations; complementary user-entity controls and how they interact with related controls at the Service Organization to meet the applicable trust services criteria; the applicable trust services criteria; the description criteria; and the risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This section presents the following information provided by Microsoft:

- The controls established and specified by Microsoft to achieve the specified trust services criteria.

Also included in this section is the following information provided by Deloitte & Touche LLP:

- A description of the tests performed by Deloitte & Touche LLP to determine whether Microsoft's controls were operating with sufficient effectiveness to achieve specified trust services criteria. Deloitte & Touche LLP determined the nature, timing, and extent of the testing performed.
- The results of Deloitte & Touche LLP's tests of controls.

The examination was conducted in accordance with the security and availability principles as set forth in TSP section 100, 2017 *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("applicable trust services criteria"), DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* ("description criteria"), of the American Institute of Certified Public Accountants (AICPA), the International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board, and the AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE 18). SSAE 18 is inclusive of the following: (1) AT-C 105, *Concepts Common to all Attestation Engagements*; and (2) AT-C 205, *Examination Engagements*. Our testing of Microsoft's controls was restricted to the controls identified by Microsoft to meet the criteria for the security and availability principles listed in **Section IV** of this report and was not extended to controls described in **Section III** but not included in **Section IV**, or to controls that may be in effect at user organizations or subservice organizations.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities and subservice organizations to obtain an understanding and to assess control risk at the user entities. The controls at user entities, subservice organizations, and Microsoft's controls should be evaluated together. If effective user entity or subservice organizations controls are not in place, Microsoft's controls may not compensate for such weaknesses.

Control environment elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Microsoft, our procedures included tests of the following relevant elements of Microsoft's control environment:

a. Integrity and Ethical Values
b. Microsoft SBC
c. Training and Accountability
d. Commitment to Competence
e. OLC, IA Department, AC
f. Risk Assessment
g. Information and Communication
h. Monitoring

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Microsoft's activities and operations, inspection of Microsoft's documents and records, and re-performance of the application of Microsoft's controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

Tests of operating effectiveness

Our tests of the controls were designed to cover a representative number of transactions throughout the period from July 1, 2018 through June 30, 2019. In determining the nature, timing and extent of tests we considered, (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the nature of the trust services criteria to be achieved, (d) the assessed level of control risk, (e) the expected effectiveness of the test, and (f) the results of our tests of the control environment.

Description of testing procedures performed

Deloitte & Touche LLP performed a variety of tests relating to the controls listed in this section throughout the period from July 1, 2018 through June 30, 2019. Our tests of controls were performed on controls as they existed during the period of July 1, 2018 through June 30, 2019, and were applied to those controls relating to the trust services criteria.

In addition to the tests listed below, ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period. Tests performed are described below:

Test	Description
Corroborative Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control during the reporting period to evidence application of the specific control activity.
Examination of documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperformed the procedures. Compared any exception items identified with those identified by the responsible control owner.

Reliability of information produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes (a) information provided by the service organization to the service auditor in response to ad hoc requests from the service auditor (e.g., population lists); (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations); and (c) information prepared for user entities (e.g., user access lists), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes. Information we utilized as evidence may have included, but was not limited to:

- Standard "out of the box" reports as configured within the system
- Parameter-driven reports generated by Microsoft's systems
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
- Spreadsheets that include relevant information utilized for the performance or testing of a control

- Prepared analyses, schedules, or other evidence manually prepared and utilized by Microsoft

Our procedures to evaluate whether this information was sufficiently reliable included obtaining evidence regarding the accuracy and completeness included procedures to address (a) the accuracy and completeness of source data and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by Microsoft.

Reporting on results of testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because Deloitte & Touche LLP does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all deviations.

Description of control activities

The information regarding the tests of operating effectiveness is explained below in two parts:

- **Part A:** Contains the Trust Services Criteria, and the related Microsoft control activities that cover those criteria.
- **Part B:** Contains the details of the test procedures performed to test the operating effectiveness of the Microsoft control activities and the results of the testing.

The Security and Availability Trust Services Criteria and Microsoft Control Activities in **Part A** and **Part B** are provided by Microsoft.

Part A: Trust Services Criteria and Control Activities provided by Microsoft

Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles

CC1.0 – CONTROL ENVIRONMENT

Criteria	NGP-PIMS Control Activity
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**CCL-01** – Commerce has implemented Microsoft governance policies reflecting requirements of the current business, regulatory and compliance environments. The policies are reviewed and approved at least annually or more frequently, as necessary. **CCL-02** – Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. OLC provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately. **CCL-03** – Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**CCL-05** – The Audit Committee (AC) reviews its Charter and Responsibilities as listed in its calendar on an annual basis. The AC responsibilities include meeting privately with the external and internal auditors on a quarterly basis; reviewing and discussing the Company's quarterly financials; and completing an annual self-evaluation. **CCL-28** – Internal Audit Charter directs them to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**CCL-07** – The MS Policy tool enables users to access documents like policies and guidelines quickly via a central repository. Unifying the location of the policies is designed to provide users with greater access to consistent information and powerful search capabilities. Policies are defined by function, region, and product, as needed. In addition, there are overarching corporate policies that apply for the extended enterprise (anti-corruption, confidential information, insider trading, whistleblowing, global trade, etc.). Policies are located at the Company's MS Policy SharePoint site and are readily available. Policies are reviewed and approved on an annual basis. **CCL-08** – Commerce adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet.

Criteria	NGP-PIMS Control Activity
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**CCL-09** - Outsourced providers are expected to meet certain levels of skills and experience, depending on role. **CCL-10** - The Candidate's job descriptions are created and documented for open positions at Microsoft. Job descriptions include desired candidate competencies and expected job roles and responsibilities. **CCL-11** - Microsoft Human Resources works with organizations and vendor companies to perform a background check on new or transferred US personnel before they are granted access to the Microsoft corporate network. **CCL-13** - HR maintains an Employee Handbook and HR Web that orient employees on topics like equal employment opportunity, avenues to raise employee compensation and benefits, employee security, and safety and health. http://hrweb/lifeatmicrosoft/Handbook/Employee **CCL-14** - Employees hold periodic "connects" with their managers to validate they are on the expected career path and facilitate greater collaboration. Employees also review their performance against their documented deliverables (priorities) and discuss the results with their managers. **CCL-15** - Commerce has a defined security organization structure for the Information Security Program for security governance, accountability, and oversight. This structure includes clearly defined roles and responsibilities. **CCL-118** - Training is provided as needed (i.e., LOB apps, Microsoft Office, etc.). In addition, all outsourced providers are trained to understand and comply with Microsoft's code of conduct. **CCL-119** - Management holds all outsourced service providers accountable to achieving specific deliverables, as outlined in a Statement of Work.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**CCL-08** - Commerce adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet. **CCL-14** - Employees hold periodic "connects" with their managers to validate they are on the expected career path and facilitate greater collaboration. Employees also review their performance against their documented deliverables (priorities) and discuss the results with their managers. **CCL-15** - Commerce has a defined security organization structure for the Information Security Program for security governance, accountability, and oversight. This structure includes clearly defined roles and responsibilities. **CCL-16** - A security education and awareness training program has been formally defined and all employees and contractors are required to attend this training on an annual basis. Employees and contractors are made aware of their roles and responsibilities with regard to information security.

CC2.0 - COMMUNICATION AND INFORMATION

Criteria	NGP-PIMS Control Activity
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**CCL-08** - Commerce adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet. **CCL-12** - FCG reviews the Section 302 survey responses, the CFO Questionnaire, and the Policies and Controls Matrix responses as they come into the survey tools and assesses their ICFR significance. Survey responses help inform future risk assessments. Also, if deficiencies are identified, remediation may drive change to control activities and progress is monitored and reported to senior management. **CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-23** - The identified risks that would impair system security, confidentiality, availability and process integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners.

Criteria	NGP-PIMS Control Activity
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**CCL-01** - Commerce has implemented Microsoft governance policies reflecting requirements of the current business, regulatory and compliance environments. The policies are reviewed and approved at least annually or more frequently, as necessary. **CCL-08** - Commerce adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet. **CCL-20** - Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct. **CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-23** - The identified risks that would impair system security, confidentiality, availability and process integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**CCL-20** - Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct. **CCL-27** - Effectiveness of the internal controls is evaluated through multiple certification and assessment processes on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner. **CCL-169** - Services maintain and communicate the confidentiality and related security obligations for customer data via the Microsoft Trust Center.

CC3.0 - RISK ASSESSMENT

Criteria	NGP-PIMS Control Activity
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-23** - The identified risks that would impair system security, confidentiality, availability and process integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**CCL-11** - Microsoft Human Resources works with organizations and vendor companies to perform a background check on new or transferred US personnel before they are granted access to the Microsoft corporate network. **CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-23** - The identified risks that would impair system security, confidentiality, availability and process integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners.

Criteria	NGP-PIMS Control Activity
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-25** - Corporate, External, and Legal Affairs (CELA) reports confirmed or potential fraud matters to external auditors, Deloitte, in the Quarterly Fraud Certification meetings. In addition to the representatives of Deloitte, these meetings are attended by the Corporate VP of Finance, Assistant Corporate Controller, VP Deputy General Counsel for Corporate Finance, CVP of Internal Audit, Senior Director of the Financial Integrity Unit (FIU), and representatives of CELA, including the CVP Deputy General Counsel for CELA Litigation, Competition and Compliance Group and the Director of OLC Investigation. At the meetings, the Microsoft attendees disclose and discuss any matter that may a fall under the 302 definition and confirm that any such matters have been or will be further disclosed by CELA to the Audit Committees of the Board of Directors. **CCL-26** - Anti-Corruption Program Management Office (ACPMO) considers the potential incentives, pressures, attitudes, and the potential opportunities related to different types of anticorruption fraud when evaluating and prioritizing risk. ACPMO's mission is to design, implement and manage an effective global anticorruption program for Microsoft which includes driving business and functional accountability, oversight, monitoring, guidance, training, reporting and the development & coordination of a worldwide community across LCA, Finance, Controls & Compliance, AI/FUI, GPG, RE&F, SMSG and other pertinent organizational partners relative to the company's anticorruption effort. The risk assessment covers the extended enterprise and considers the inherent risks related to outsource service providers. Anticorruption polices can be found: http://lcaweb/policies/anticorruption/Pages/Anticorruption-landing-page.aspx **CCL-147** - Only variants that are approved by CELA are registered in PDMS.
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**CCL-12** - FCG reviews the Section 302 survey responses, the CFO Questionnaire, and the Policies and Controls Matrix responses as they come into the survey tools and assesses their ICFR significance. Survey responses help inform future risk assessments. Also, if deficiencies are identified, remediation may drive change to control activities and progress is monitored and reported to senior management. **CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-23** - The identified risks that would impair system security, confidentiality, availability and process integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners.

CC4.0 - MONITORING ACTIVITIES

Criteria	NGP-PIMS Control Activity
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-27** - Effectiveness of the internal controls is evaluated through multiple certification and assessment processes on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner. **CCL-28** - Internal Audit Charter directs them to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment. **CCL-33** - Penetration testing (internal or external) is performed at least annually, or after any significant changes in system design and/or infrastructure. Corrective action, if required, is performed in a timely manner.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	**CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-27** - Effectiveness of the internal controls is evaluated through multiple certification and assessment processes on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner. **CCL-28** - Internal Audit Charter directs them to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment. **CCL-30** - Internal Audit has open access to the Audit Committee members and attends regular meetings with the Audit Committee to maintain a close working relationship and adheres to professional standards of conduct.

CC5.0 - CONTROL ACTIVITIES

Criteria	NGP-PIMS Control Activity
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-27** - Effectiveness of the internal controls is evaluated through multiple certification and assessment processes on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner. **CSOC** - Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting NGP-PIMS and DataGrid.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-23** - The identified risks that would impair system security, confidentiality, availability and process integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners. **CCL-27** - Effectiveness of the internal controls is evaluated through multiple certification and assessment processes on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**CCL-01** - Commerce has implemented Microsoft governance policies reflecting requirements of the current business, regulatory and compliance environments. The policies are reviewed and approved at least annually or more frequently, as necessary. **CCL-08** - Commerce adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet. **CCL-16** - A security education and awareness training program has been formally defined and all employees and contractors are required to attend this training on an annual basis. Employees and contractors are made aware of their roles and responsibilities with regard to information security.

CC6.0 - LOGICAL AND PHYSICAL ACCESS CONTROLS

Criteria	NGP-PIMS Control Activity
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	**CCL-35** - Access to Services must be authorized, conform to Microsoft access management policies and procedures, and aligned with the Role-Based Access Control (RBAC) Model. Role Based Access Control (RBAC) is implemented within the Service's systems to enforce the concepts of the least privilege access and segregation of the incompatible duties. **CCL-36** - On a quarterly basis, the list of users with access to the Service's systems, including the Service tree admins, Azure subscriptions and resources, security groups, GTM portal or Azure Traffic Manager (ATM), source code repository, and encryption keys repository is reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner. **CCL-40** - User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change. **CCL-45** - Keys are rotated on a periodic basis in accordance with Online Services Security Standards (OSSS). Where these standards conflict with the Microsoft Security Policy, the stricter of the policies are applied to ensure proper and effective use of cryptographic confidentiality. **CCL-47** - Credential monitoring is performed in each build to prevent credentials from existing in the Service's source code. **CCL-148** - JIT activity is documented within a DevOps or ICM ticket describing the reason for and changes made during the login session. **CCL-149** - Services maintain an inventory of all Azure subscriptions in the Service Tree. An inventory of all resources residing within each Service's Azure subscription is maintained within the Azure Portal. Access to service tree and Azure portal is restricted to authorized individuals. **CCL-178** - Component Governance scanner is Integrated with the build definition to detect Open Source code and to alert whether there are vulnerabilities or legal impacts associated with the identified Open Source code/software. **CSOC** - Microsoft Azure is responsible for the account close and delete requests, and authentication to validate that the request is submitted by an authorized tenant admin. **CSOC** - Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting NGP-PIMS and DataGrid. **CSOC** - Microsoft Azure is responsible for the password configuration and authentication processes for NGP and DataGrid in accordance with Microsoft security policy. **CSOC** - Microsoft Azure is responsible for the encryption configurations for customer data being transmitted and while at rest.

Criteria	NGP-PIMS Control Activity
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**CCL-35** - Access to Services must be authorized, conform to Microsoft access management policies and procedures, and aligned with the Role-Based Access Control (RBAC) Model. Role Based Access Control (RBAC) is implemented within the Service's systems to enforce the concepts of the least privilege access and segregation of the incompatible duties. **CCL-36** - On a quarterly basis, the list of users with access to the Service's systems, including the Service tree admins, Azure subscriptions and resources, security groups, GTM portal or Azure Traffic Manager (ATM), source code repository, and encryption keys repository is reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner. **CCL-40** - User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change. **CCL-132** - The baseline configuration for Security Groups (SGs) enforce a requirement for SG Owner's approval for adding new users to the SG. **CCL-149** - Services maintain an inventory of all Azure subscriptions in the Service Tree. An inventory of all resources residing within each Service's Azure subscription is maintained within the Azure Portal. Access to service tree and Azure portal is restricted to authorized individuals. **CCL-152** - Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the Commerce Services change management policy. **CCL-185** - On a Semi-annual basis the list of the users with access to the Pilotfish environment is reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner. Changes in the access in Pilotfish environment must go through the change management process. **CSOC** - Microsoft Azure is responsible for account close and delete requests, and authentication to validate the request is submitted by an authorized Tenant Admin. **CSOC** - Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting NGP-PIMS and DataGrid.

Criteria	NGP-PIMS Control Activity
CC6.3- The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	**CCL-35** - Access to Services must be authorized, conform to Microsoft access management policies and procedures, and aligned with the Role-Based Access Control (RBAC) Model. Role Based Access Control (RBAC) is implemented within the Service's systems to enforce the concepts of the least privilege access and segregation of the incompatible duties. **CCL-36** - On a quarterly basis, the list of users with access to the Service's systems, including the Service tree admins, Azure subscriptions and resources, security groups, GTM portal or Azure Traffic Manager (ATM), source code repository, and encryption keys repository is reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner. **CCL-40** - User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change. **CCL-132** - The baseline configuration for Security Groups (SGs) enforce a requirement for SG Owner's approval for adding new users to the SG. **CCL-152** - Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the Commerce Services change management policy. **CCL-185** - On a Semi-annual basis the list of the users with access to the Pilotfish environment is reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner. Changes in the access in Pilotfish environment must go through the change management process.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**CSOC** - Microsoft Azure is responsible for controlling physical access to facilities and protected information assets in data center facilities, back-up media storage, and other sensitive locations, and is restricted to authorized personnel to meet the entity's objectives.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	**CCL-35** - Access to Services must be authorized, conform to Microsoft access management policies and procedures, and aligned with the Role-Based Access Control (RBAC) Model. Role Based Access Control (RBAC) is implemented within the Service's systems to enforce the concepts of the least privilege access and segregation of the incompatible duties. **CCL-36** - On a quarterly basis, the list of users with access to the Service's systems, including the Service tree admins, Azure subscriptions and resources, security groups, GTM portal or Azure Traffic Manager (ATM), source code repository, and encryption keys repository is reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner. **CCL-40** - User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change. **CSOC** - Microsoft Azure is responsible for controlling physical access to facilities and protected information assets in data center facilities, back-up media storage, and other sensitive locations, and is restricted to authorized personnel to meet the entity's objectives.

Criteria	NGP-PIMS Control Activity
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**CCL-29** - Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-33** - Penetration testing (internal or external) is performed at least annually, or after any significant changes in system design and/or infrastructure. Corrective action, if required, is performed in a timely manner. **CCL-47** - Credential monitoring is performed in each build to prevent credentials from existing in the Service's source code. **CCL-70** - Services conduct an annual review of the system's data flow to validate its accuracy, and update it if necessary. **CCL-178** - Component Governance scanner is Integrated with the build definition to detect Open Source code and to alert whether there are vulnerabilities or legal impacts associated with the identified Open Source code/software. **CSOC** - Microsoft Azure is responsible for network filtering implementation to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **CSOC** - Microsoft Azure is responsible for maintaining controls over environmental protection of systems, including natural disasters and man-made threats, for infrastructure supporting NGP-PIMS. **CSOC** - Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting NGP-PIMS and DataGrid. **CSOC** - Microsoft Azure is responsible for the encryption configurations for customer data being transmitted and while at rest.
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	**CSOC** - Microsoft Azure is responsible for network filtering implementation to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **CSOC** - Microsoft Azure is responsible for maintaining controls over environmental protection of systems, including natural disasters and man-made threats, for infrastructure supporting NGP-PIMS. **CSOC** - Microsoft Azure is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices. **CSOC** - Microsoft Azure is responsible for the encryption configurations for customer data being transmitted and while at rest.

Criteria	NGP-PIMS Control Activity
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	**CCL-29** - Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-33** - Penetration testing (internal or external) is performed at least annually, or after any significant changes in system design and/or infrastructure. Corrective action, if required, is performed in a timely manner. **CCL-54** - OS patching is automatically deployed to all Service's system resources through Pilotfish. CDG runs the scan to determine that all VMs have updated security patches. CDG will notify services regarding any outdated security patches. **CCL-59** - The JIT access to production environment is logged, and on a quarterly basis, log is reviewed to determine only appropriate users logged into production environment. Users have read-only access to the JIT log. **CCL-60** - An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CCL-61** - CDG Security handles/monitors security and incident alerts on an ongoing basis and communicates required actions and response efforts. Corrective actions, if required, are performed in a timely manner. **CCL-92** - For teams utilizing the Developer / Operations model, system configurations are in place to prevent implementation of unapproved changes to production. **CCL-148** - JIT activity is documented within a DevOps or ICM ticket describing the reason for and changes made during the login session. **CCL-178** - Component Governance scanner is Integrated with the build definition to detect Open Source code and to alert whether there are vulnerabilities or legal impacts associated with the identified Open Source code/software.

CC7.0 - SYSTEM OPERATIONS

Criteria	NGP-PIMS Control Activity
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	**CCL-29** - Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-33** - Penetration testing (internal or external) is performed at least annually, or after any significant changes in system design and/or infrastructure. Corrective action, if required, is performed in a timely manner. **CCL-59** - The JIT access to production environment is logged, and on a quarterly basis, log is reviewed to determine only appropriate users logged into production environment. Users have read-only access to the JIT log. **CCL-60** - An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CCL-61** - CDG Security handles/monitors security and incident alerts on an ongoing basis and communicates required actions and response efforts. Corrective actions, if required, are performed in a timely manner. **CCL-94** - Quarterly, services validate that the Qualys agent is running on in-scope VMs. **CCL-148** - JIT activity is documented within a DevOps or ICM ticket describing the reason for and changes made during the login session. **CCL-152** - Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the Commerce Services change management policy. **CCL-178** - Component Governance scanner is Integrated with the build definition to detect Open Source code and to alert whether there are vulnerabilities or legal impacts associated with the identified Open Source code/software.

Criteria	NGP-PIMS Control Activity
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	**CCL-29** - Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-33** - Penetration testing (internal or external) is performed at least annually, or after any significant changes in system design and/or infrastructure. Corrective action, if required, is performed in a timely manner. **CCL-59** - The JIT access to production environment is logged, and on a quarterly basis, log is reviewed to determine only appropriate users logged into production environment. Users have read-only access to the JIT log. **CCL-60** - An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CCL-61** - CDG Security handles/monitors security and incident alerts on an ongoing basis and communicates required actions and response efforts. Corrective actions, if required, are performed in a timely manner. **CCL-148** - JIT activity is documented within a DevOps or ICM ticket describing the reason for and changes made during the login session. **CCL-178** - Component Governance scanner is Integrated with the build definition to detect Open Source code and to alert whether there are vulnerabilities or legal impacts associated with the identified Open Source code/software. **CSOC** - Microsoft Azure is responsible for geographic replication and backups for NGP-PIMS systems hosted on Azure platform services.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**CCL-29** - Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-33** - Penetration testing (internal or external) is performed at least annually, or after any significant changes in system design and/or infrastructure. Corrective action, if required, is performed in a timely manner. **CCL-60** - An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CCL-61** - CDG Security handles/monitors security and incident alerts on an ongoing basis and communicates required actions and response efforts. Corrective actions, if required, are performed in a timely manner. **CCL-111** - A root cause analysis of the incidents will be performed to reduce the likelihood or impact of future incidents; if applicable. **CSOC** - Microsoft Azure is responsible for monitoring and addressing security events and incidents related to the NGP-PIMS systems hosted on Azure platform services.

Criteria	NGP-PIMS Control Activity
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	**CCL-33** - Penetration testing (internal or external) is performed at least annually, or after any significant changes in system design and/or infrastructure. Corrective action, if required, is performed in a timely manner. **CCL-60** - An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CCL-61** - CDG Security handles/monitors security and incident alerts on an ongoing basis and communicates required actions and response efforts. Corrective actions, if required, are performed in a timely manner. **CCL-111** - A root cause analysis of the incidents will be performed to reduce the likelihood or impact of future incidents; if applicable.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	**CCL-17** - The Service has a geo-redundant design and it runs in an active/passive (or active/active) configuration. Services' fail over requirements are configured in a fail-over tool and access is limited to authorized administrators to modify the configurations. **CCL-60** - An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CCL-61** - CDG Security handles/monitors security and incident alerts on an ongoing basis and communicates required actions and response efforts. Corrective actions, if required, are performed in a timely manner. **CCL-111** - A root cause analysis of the incidents will be performed to reduce the likelihood or impact of future incidents; if applicable. **CSOC** - Microsoft Azure is responsible for controlling that all datacenters are required to at least annually exercise, test, and maintain the datacenter BCP for the continued operations of critical processes and required resources in the event of a disruption.

CC8.0 - CHANGE MANAGEMENT

Criteria	NGP-PIMS Control Activity
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	**CCL-47** - Credential monitoring is performed in each build to prevent credentials from existing in the Service's source code. **CCL-55** - Development of new features and major changes to Services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology. **CCL-56** - Changes are tested and technical specifications and/or configurations are validated for appropriateness. Testing results and Technical signoff are retained within the appropriate TFS record depending on the type of change as outlined in the Commerce Change Management Policy. **CCL-57** - Changes are appropriately approved prior to release to production, as defined in the Commerce Change Management Policy, indicating their approval of the production readiness of the tested code. **CCL-59** - The JIT access to production environment is logged, and on a quarterly basis, log is reviewed to determine only appropriate users logged into production environment. Users have read-only access to the JIT log. **CCL-76** - The third party Global Traffic Management (GTM) provider activity log is reviewed on quarterly basis to determine changes to the Service's properties were appropriate and authorized. **CCL-92** - For teams utilizing the Developer / Operations model, system configurations are in place to prevent implementation of unapproved changes to production. **CCL-98** - The Production and Pre-Production environment (PPE) are separated. New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments. **CCL-148** - JIT activity is documented within a DevOps or ICM ticket describing the reason for and changes made during the login session. **CCL-152** - Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the Commerce Services change management policy. **CSOC** - Microsoft Azure is responsible for the maintenance and change management of the infrastructure and supporting systems that support their PaaS where NGP-PIMS and DataGrid are hosted.

CC9.0 - RISK MITIGATION

Criteria	NGP-PIMS Control Activity
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-23** - The identified risks that would impair system security, confidentiality, availability and process integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners. **CCL-27** - Effectiveness of the internal controls is evaluated through multiple certification and assessment processes on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner. **CCL-78** - Commerce adheres to the Enterprise Business Continuity Management and Standard. The Service's business continuity plans (BCPs) are reviewed and approved at least annually. **CCL-101** - Failover procedures are defined and at least annually, integrity checks are performed through standard restoration activities.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	**CCL-21** - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. **CCL-22** - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management. **CCL-23** - The identified risks that would impair system security, confidentiality, availability and process integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners. **CCL-65** - Services monitor their dependencies on third parties through obtaining and evaluating attestation reports when available.

Additional Criteria for Availability

Criteria	NGP-PIMS Control Activity
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	**CCL-66** - Processing capacity and availability are monitored by Service teams. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed. **CCL-67** - Quarterly, Service management reviews and discuss system availability and reliability and addresses any issues. **CCL-68** - Annually, Services senior management reviews and approves the capacity for Service's systems. **CSOC** - Microsoft Azure is responsible for processing capacity and use of system components for NGP-PIMS systems hosted on Azure platform services.
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	**CCL-17** - The Service has a geo-redundant design and it runs in an active/passive (or active/active) configuration. Services' fail over requirements are configured in a fail-over tool and access is limited to authorized administrators to modify the configurations. **CCL-69** - Services have an architecture in place that supports the recovery of services through tools and services supporting the overall Service. **CCL-76** - The third party Global Traffic Management (GTM) provider activity log is reviewed on quarterly basis to determine changes to the Service's properties were appropriate and authorized. **CCL-101** - Failover procedures are defined and at least annually, integrity checks are performed through standard restoration activities. **CSOC** - Microsoft Azure is responsible for geographic replication and backups for NGP-PIMS systems hosted on Azure platform services.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**CCL-78** - Commerce adheres to the Enterprise Business Continuity Management and Standard. The Service's business continuity plans (BCPs) are reviewed and approved at least annually. **CSOC** - Microsoft Azure is responsible for controlling that all datacenters are required to at least annually exercise, test, and maintain the datacenter BCP for the continued operations of critical processes and required resources in the event of a disruption.

Part B: Control Activities Provided by Microsoft and Test Results Provided by Deloitte & Touche LLP

Control Activity	Tests Performed	Test Result
CCL-01 - Commerce has implemented Microsoft governance policies reflecting requirements of the current business, regulatory and compliance environments. The policies are reviewed and approved at least annually or more frequently, as necessary.	• Inquired of Commerce Managers to gain an understanding of the processes for information security awareness and training for employees, contractors, and third-party users. • Inspected training material to ascertain that it incorporated security policy requirements and was updated as needed. • Obtained and inspected the policies to ascertain that they are reviewed and approved annually.	No Exceptions Noted
CCL-02 - Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct (SBC) as necessary and the Code is made available internally and externally. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. OLC provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.	• Inquired of HR Managers to ascertain that a defined SBC policy was established and communicated to NGP and DataGrid personnel through intranet sites and trainings. • Obtained and inspected the SBC to ascertain that the standards include Microsoft's continued commitment to security and availability, and ethical business practices and regulatory compliance. • Obtained and inspected evidence that for a selection of employees, the SBC training course has been completed.	No Exceptions Noted
CCL-03 - Microsoft's values are accessible to employees via the Values SharePoint site and are updated as necessary by management.	• Inquired with Talent Managers that values are posted on a SharePoint site and accessible to all employees and updated if needed by management. • Inspected the SharePoint site to ascertain it was accessible using our Microsoft credentials.	No Exceptions Noted
CCL-05 - The Audit Committee (AC) reviews its Charter and Responsibilities as listed in its calendar on an annual basis. The AC responsibilities include meeting privately with the external and internal auditors on a quarterly basis; reviewing and discussing the Company's quarterly financials; and completing an annual self-evaluation.	• Inquired of Compliance Managers to gain an understanding of the Internal Audit Charter and the scope and frequency of assurance activities performed by Internal Audit. • Obtained and inspected the Internal Audit Charter and ascertained that the Charter directs the services of Internal Audit. • Obtained and inspected the Internal Audit plan and ascertained that the assurance activities are based on an annual risk assessment.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-07 - The MS Policy tool enables users to access documents like policies and guidelines quickly via a central repository. Unifying the location of the policies is designed to provide users with greater access to consistent information and powerful search capabilities. Policies are defined by function, region, and product, as needed. In addition, there are overarching corporate policies that apply for the extended enterprise (anti-corruption, confidential information, insider trading, whistleblowing, global trade, etc.). Policies are located at the Company's MS Policy SharePoint site and are readily available. Policies are reviewed and approved on an annual basis.	• Inquired with Finance Managers that the MS Policy tool was in a centralized repository for employees to access policies. • Inspected the SharePoint site to ascertain it was accessible by all employees. • Obtained and inspected a selection of a policy version to ascertain that it had been reviewed in the last year. • Obtained and inspected a selection of a policy to ascertain that a change to the policy was appropriately approved and documented.	No Exceptions Noted
CCL-08 - Commerce adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet.	• Inquired with Program Managers that the Microsoft policies are available to all employees through an intranet site, and that Commerce adheres to the policies. • Inspected the intranet site to ascertain the policies are available to all employees. • Obtained and inspected a selection of a policy version to ascertain that it had been reviewed in the last year. • Inspected that policies had links to applicable associated policies to the Commerce group.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-09 - Outsourced providers are expected to meet certain levels of skills and experience, depending on role.	• Inquired with Compliance Managers the process for citing expectations from outsourced providers to achieve specific deliverables and training outsourced providers on Microsoft's supplier code of conduct. • Obtained and inspected Microsoft's Statement of Work template to ascertain that it cited outsourced providers' role and accountability in achieving specific deliverables. • Inspected the supplier procurement website to ascertain that Microsoft's supplier code of conduct was available and accessible to all outsourced providers. • Observed during the supplier access provisioning process that completion of the supplier code of conduct training was required.	No Exceptions Noted
CCL-10 - The Candidate's job descriptions are created and documented for open positions at Microsoft. Job descriptions include desired candidate competencies and expected job roles and responsibilities.	• Inquired with HR Managers to ascertain that candidate's job descriptions are created and documented for open positions within Microsoft website. • Obtained and inspected a sample job posting to ascertain that the job listing includes desired candidate competencies and expected job roles and responsibilities.	No Exceptions Noted
CCL-11 - Microsoft Human Resources works with organizations and vendor companies to perform a background check on new or transferred US personnel before they are granted access to the Microsoft corporate network.	• Inquired with HR Managers that new and transferred U.S. employees and contractors are required to undergo a background check prior to being granted access to the environment. • Obtained and inspected procedures document to ascertain that background screening performed included verification of personal and professional history.	No Exceptions Noted
CCL-12 - FCG reviews the Section 302 survey responses, the CFO Questionnaire, and the Policies and Controls Matrix responses as they come into the survey tools and assesses their ICFR significance. Survey responses help inform future risk assessments. Also, if deficiencies are identified, remediation may drive change to control activities and progress is monitored and reported to senior management.	• Inquired with Finance Managers that the FCG reviews Section 302 responses on a quarterly basis to identify future risks and remediate any deficiencies. • Obtained and inspected the CFO and Controller trackers to ascertain the SOX 302 completion dates were documented. • Inspected that all identified exceptions were flagged; exceptions were tracked, monitored and followed-up on until resolution. • Obtained and inspected a selected quarterly review meeting to inspect the meeting presentation of the SOX 302 results.	No Exceptions Noted
CCL-13 - HR maintains an Employee Handbook and HR Web that orient employees on topics like equal employment opportunity, avenues to raise employee compensation and benefits, employee security, and safety and health. http://hrweb/lifeatmicrosoft/Handbook/Employee	• Inquired with HR Managers that the Employee Handbook was available to all employees and thoroughly covered HR topics. • Inspected the SharePoint site to ascertain the Employee Handbook was available to all employees. • Obtained and inspected the Employee Handbook to ascertain that it had been reviewed in the last year.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-14 - Employees hold periodic "connects" with their managers to validate they are on the expected career path and facilitate greater collaboration. Employees also review their performance against their documented deliverables (priorities) and discuss the results with their managers.	• Inquired of HR Managers to ascertain that performance reviews take place where employee commitments are evaluated by his/her manager on a semi-annual basis. • Obtained and inspected evidence for a selection of employees to ascertain that they completed a performance evaluation annually. • Obtained and inspected evidence to ascertain that a sample performance review includes an evaluation of employee performance against their assigned priorities.	No Exceptions Noted
CCL-15 - Commerce has a defined security organization structure for the Information Security Program for security governance, accountability, and oversight. This structure includes clearly defined roles and responsibilities.	• Inquired with Compliance Managers that the Commerce security organization structure was defined and included roles and responsibilities. • Inspected the wiki page containing the Commerce organization structure. • Obtained and inspected a selection of a user and corroborated the user's details in the organizational chart with the Dr. Who intranet page.	No Exceptions Noted
CCL-16 - A security education and awareness training program has been formally defined and all employees and contractors are required to attend this training on an annual basis. Employees and contractors are made aware of their roles and responsibilities with regard to information security.	• Inquired of the management to gain an understanding of the processes for awareness and training on information security for employees, contractors, and third-party users. • Inspected training material to ascertain that it incorporated security policy requirements and was updated as needed. • Obtained and inspected the policies to ascertain that they are reviewed and approved annually	No Exceptions Noted
CCL-17 - The Service has a geo-redundant design and it runs in an active/passive (or active/active) configuration. Services' fail over requirements are configured in a fail-over tool and access is limited to authorized administrators to modify the configurations.	• Inquired of Service Engineers that processes have been established for data backups and restorations. • Inspected the configuration of Services' geo-redundant design within the Akamai tool. • Obtained and inspected evidence to ascertain that the service was configured that separate data instances were available for restoration or failover. • Obtained and inspected evidence for how access to the Akamai tool was restricted to authorized individuals.	No Exceptions Noted
CCL-20 - Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.	• Inquired of Microsoft Office of Legal Compliance (OLC) team regarding the mechanisms (email, phone, fax, website) that permit reporting of issues related to Business Conduct. • Obtain and inspected evidence of each communication mechanism to ascertain that the mechanisms were available and functioning.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-21 - Relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.	• Inquired of the management regarding the procedures in place for identifying relevant statutory, regulatory, and contractual requirements, and making relevant updates to documentation or procedures accordingly. • Obtained and inspected policy, procedure, and agreement documents to ascertain that they included relevant and current statutory, regulatory, and contractual requirements.	No Exceptions Noted
CCL-22 - The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.	• Inquired of the Enterprise Risk Management (ERM) team on the ERM risk assessment process and how risks are identified and managed. • Obtained and inspected the agenda or meeting minutes to ascertain that the ERM risk assessment results are reviewed bi-annually and presented to the Board of Directors for review and consideration of the changes.	No Exceptions Noted
CCL-23 - The identified risks that would impair system security, confidentiality, availability and process integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners.	• Inquired of Program Managers to ascertain that a process has been established to track and mitigate risks identified as part of the ISO assessments. • Obtained and inspected that an ISO assessment has been performed for each NGP service. • Obtained and inspected that for a selection of the risks identified by the ISO assessment a risk mitigation strategy has been developed and has been put in place.	No Exceptions Noted
CCL-25 - Corporate, External, and Legal Affairs (CELA) reports confirmed or potential fraud matters to external auditors, Deloitte, in the Quarterly Fraud Certification meetings. In addition to the representatives of Deloitte, these meetings are attended by the Corporate VP of Finance, Assistant Corporate Controller, VP Deputy General Counsel for Corporate Finance, CVP of Internal Audit, Senior Director of the Financial Integrity Unit (FIU), and representatives of CELA, including the CVP Deputy General Counsel for CELA Litigation, Competition and Compliance Group and the Director of OLC Investigation. At the meetings, the Microsoft attendees disclose and discuss any matter that may a fall under the 302 definition and confirm that any such matters have been or will be further disclosed by CELA to the Audit Committees of the Board of Directors.	• Inquired with Compliance Managers that fraud matters are reported to external auditors during periodic meetings. • Obtained and inspected meeting notes from a selected fraud meeting to ascertain that appropriate individuals were included in the fraud discussion. • Inspected the details of the meeting minutes to ascertain that all fraud incidents that were discussed were also included in the SOX 302 report. • Inspected the details of a selected fraud incident discussed during the meeting to understand how it was being handled.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-26 - Anti-Corruption Program Management Office (ACPMO) considers the potential incentives, pressures, attitudes, and the potential opportunities related to different types of anticorruption fraud when evaluating and prioritizing risk. ACPMO's mission is to design, implement and manage an effective global anticorruption program for Microsoft which includes driving business and functional accountability, oversight, monitoring, guidance, training, reporting and the development & coordination of a worldwide community across LCA, Finance, Controls & Compliance, AI/FUI, GPG, RE&F, SMSG and other pertinent organizational partners relative to the company's anticorruption effort. The risk assessment covers the extended enterprise and considers the inherent risks related to outsource service providers. Anticorruption polices can be found: http://lcaweb/policies/anticorruption/Pages/Anticorruption-landing-page.aspx	• Inquired with Compliance Managers that the Anti-Corruption Program Management Office (ACPMO) considers potential corruption factors through a risk assessment. • Obtained and inspected that the risk assessment had been completed for the year, identifying potential issues. • Obtained and inspected the Anti-Corruption policy that was accessible to all employees and updated on an annual basis. • Inspected the One Vet tool that Microsoft uses for their anti-corruption vetting program.	No Exceptions Noted
CCL-27 - Effectiveness of the internal controls is evaluated through multiple certification and assessment processes on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner.	• Inquired of Program Managers to ascertain that the effectiveness of existing controls are assessed on an annual basis. Further ascertained per inquiry that any findings from these control assessments are addressed with corrective action plans and tracked through to timely resolution. • Obtained and inspected evidence to ascertain that internal control effectiveness reviews are performed by external parties and selected a sample of findings from those reviews to test that corrective action plans were developed and tracked to a timely resolution.	No Exceptions Noted
CCL-28 - Internal Audit Charter directs them to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.	• Inquired of the management to gain an understanding of the Internal Audit Charter and the scope and frequency of assurance activities performed by Internal Audit. • Obtained and inspected the Internal Audit Charter and ascertained that the Charter directs the services of the Internal Audit. • Obtained and inspected the Internal Audit plan and ascertained that the assurance activities are based on an annual risk assessment.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-29 - Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner.	• Inquired with Software Engineers that security threat modeling was performed and results are reviewed and followed-up on if needed. • Obtained and inspected selected threat models performed for services during the year. • Inspected any identified issues from the threat modeling to ascertain that they were addressed appropriately.	No Exceptions Noted
CCL-30 - Internal Audit has open access to the Audit Committee members and attends regular meetings with the Audit Committee to maintain a close working relationship and adheres to professional standards of conduct.	• Inquired with Compliance Managers to gain an understanding of Internal Audit's role within the organization and its access to the Audit Committee. • Obtained and inspected the Internal Audit Charter and ascertained that the Charter directs the services of the Internal Audit, including the requirements to work with the Audit Committee. • Obtained and inspected evidence to ascertain that Internal Audit was represented in the Audit Committee meetings.	No Exceptions Noted
CCL-33 - Penetration testing (internal or external) is performed at least annually, or after any significant changes in system design and/or infrastructure. Corrective action, if required, is performed in a timely manner.	• Inquired with Service Engineers that penetration testing was performed at least annually and identified issues are remediated immediately. • Obtained and inspected penetration tests performed for services covering the current year. • Inspected the results of the test and sampled an issue to ascertain that it was remediated in a timely manner.	No Exceptions Noted
CCL-35 - Access to Services must be authorized, conform to Microsoft access management policies and procedures, and aligned with the Role-Based Access Control (RBAC) Model. Role Based Access Control (RBAC) is implemented within the Service's systems to enforce the concepts of the least privilege access and segregation of the incompatible duties.	• Inquired with Service Engineers how access to the Services systems was managed and follows the Role-Based Access Control model. • Obtained and inspected the access management policies and when they were last reviewed and approved. • Inspected the Compliance Dashboard to ascertain that all users in the environment had completed required trainings. • Obtained and inspected a selected user that their access did not violate the segregation of duties outlined in the access policies. • Inspected the baseline configuration to security groups that requires approval prior to a new user being provisioned access.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-36 - On a quarterly basis, the list of users with access to the Service's systems, including the Service tree admins, Azure subscriptions and resources, security groups, GTM portal or Azure Traffic Manager (ATM), source code repository, and encryption keys repository is reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner.	• Inquired with Service Engineers that the periodic access reviews encompassed all users within the production environment as well as the specific access that each group provides. • Inspected the Access Management policies to understand how groups and roles are mapped to system access. • Obtained and inspected that users from selected access reviews were marked as appropriate. • Obtained and corroborated sampled users had appropriate access. • Obtained and inspected that users marked for a change in access were appropriately followed-up on, and the reason for their access changes was investigated.	No Exceptions Noted
CCL-40 - User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change.	• Inquired of Service Engineers to gain an understanding of the process for disabling or removing access in a timely manner. • Compared a listing of all terminated/transferred users to NGP and DataGrid security groups to ascertain that there were no terminated/transferred users with access. • Obtained and inspected the group activity logs for each security groups to ascertain that terminated/transferred users had been removed within 10 days of their termination/transfer date.	DataGrid Access for one DataGrid user was not removed within 10 business days of changing roles. NGP Access for one NGP user was not removed from within 10 business days of changing roles.
CCL-40.a - User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change.	• Inquired of Service Engineers to gain an understanding of the process for disabling or removing access in a timely manner. • Compared a listing of all terminated/transferred users within the examination period with active user accounts in the NGP-PIMS environments to ascertain if network access for terminated/ transferred employees was revoked. • Obtained and inspected termination reports for all terminated users to ascertain that their network access had been removed within 2 days of their termination date.	No Exceptions Noted
CCL-45 - Keys are rotated on a periodic basis in accordance with Online Services Security Standards (OSSS). Where these standards conflict with the Microsoft Security Policy, the stricter of the policies are applied to ensure proper and effective use of cryptographic confidentiality.	• Inquired with Service Engineers that processes for storing and rotating keys have been established. • Inspected the Microsoft Security Policy for how keys are restricted, and rotation periods are defined. • Obtained and inspected selected certificate to ascertain configuration of key was properly restricted and configured to rotate on a cadence in compliance with the policies.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-47 - Credential monitoring is performed in each build to prevent credentials from existing in the Service's source code.	• Inquired of Service Engineers that processes for Cred Scan have been established and outline requirements for addressing identified issues. • Obtained and inspected evidence that the Cred Scan was configured within all production build definitions. • Obtained and inspected evidence that the Cred Scan occurs prior to releasing changes to production.	No Exceptions Noted
CCL-54 - OS patching is automatically deployed to all Service's system resources through Pilotfish. CDG runs the scan to determine that all VMs have updated security patches. CDG will notify services regarding any outdated security patches.	• Inquired of Software Engineers that processes for security vulnerability scanning have been established and outline requirements for addressing identified issues. • Obtained and inspected evidence that the Qualys agent was configured to run on production machines to scan for outdated security patches. • Obtained and inspected any instance of CDG notifying Services of outdated patches.	No Exceptions Noted
CCL-55 - Development of new features and major changes to Services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology.	• Inquired of Software Engineers that procedures have been established and are followed prior to deploying changes to the production environment. • Obtained and inspected that the Change Management policies define the Security Development Lifecycle methodology. • Inspected that the Change policies were updated and approved within the last year.	No Exceptions Noted
CCL-56 - Changes are tested and technical specifications and/or configurations are validated for appropriateness. Testing results and Technical signoff are retained within the appropriate TFS record depending on the type of change as outlined in the Commerce Change Management Policy.	• Inquired of Software Engineers that Change Management procedures have been established and are followed prior to deploying changes to the production environment. • Inquired of Software Engineers that testing of changes was documented and required for deployment into production. • Obtained and inspected the change deployment tool configuration to ascertain that testing is enforced for every change. • Obtained and inspected evidence for a selected change to ascertain that changes are tested prior to release according to established procedures.	No Exceptions Noted
CCL-57 - Changes are appropriately approved prior to release to production, as defined in the Commerce Change Management Policy, indicating their approval of the production readiness of the tested code.	• Inquired of Software Engineers that procedures have been established and are followed prior to deploying changes to the production environment. • Obtained and inspected evidence for a selection of changes to ascertain that deployed changes were approved by appropriate stakeholders prior to release. • Obtained and inspected evidence for a selected change to ascertain that testing was reviewed and approved prior to release according to established procedures. • Inspected that the configuration of build definitions does not allow unapproved changes to be deployed.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-59 - The JIT access to production environment is logged, and on a quarterly basis, log is reviewed to determine only appropriate users logged into production environment. Users have read-only access to the JIT log.	• Inquired with Service Engineers that procedures are established to review JIT access on a quarterly basis. • Obtained and inspected the JIT elevations from selected access reviews were marked as appropriate. • Obtained and corroborated sampled users were appropriate to have the ability to use JIT access. • Inspected that JIT instances had an accompanying work item associated with each elevation.	No Exceptions Noted
CCL-60 - An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner.	• Inquired of Service Engineers that processes for identifying, reporting, and responding to security incidents have been established. • Inspected that the Xpert tool was configured to auto-generate incident alerts based on defined thresholds. • Obtained and inspected evidence for a selection of incidents to ascertain that identified incidents were documented within an incident tracking system and resolved in a timely manner. • Inquired of Service Engineers that processes for addressing incidents have been established and include processes for escalation and review. • Obtained and inspected evidence for a selection of incidents to ascertain that incidents were escalated and addressed by the appropriate team and required action was taken.	No Exceptions Noted
CCL-61 - CDG Security handles/monitors security and incident alerts on an ongoing basis and communicates required actions and response efforts. Corrective actions, if required, are performed in a timely manner.	• Inquired of Service Engineers that processes for identifying, reporting, and responding to security incidents have been established. • Obtained and inspected evidence for a selection of incidents to ascertain that identified security incidents were documented within an incident tracking system and resolved. • Inquired of Service Engineers that processes for addressing security incidents have been established and include processes for escalation and review. • Obtained and inspected evidence for a selection of incidents to ascertain that security incidents were escalated and reviewed by the appropriate team and required action was taken.	This control activity could not be tested, as there was no related activity during the examination period.
CCL-65 - Services monitor their dependencies on third parties through obtaining and evaluating attestation reports when available.	• Inquired of Service Engineers to ascertain that Services monitors its dependencies on third parties, and their compliance with SLAs / contract obligations. • Obtained and inspected evidence to ascertain that Audit Reports for each of the dependent third parties were obtained and inspected for issues. Any issues identified were followed-up on with the required party. • Obtained and inspected evidence that mapping was performed from Audit Reports for each of the dependent third parties to Services' controls.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-66 - Processing capacity and availability are monitored by Service teams. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.	• Inquired of Service Engineers to ascertain that each service has established a dashboard for monitoring capacity and availability. • Observed and inspected the capacity and availability dashboards for each workload for evidence that capacity and availability metrics are being tracked and displayed to identify service related issues. • Obtained and inspected an example automated availability alert to ascertain that alerting was in place and incidents are resolved as needed. • Obtained and inspected evidence for a selection of incidents to ascertain that capacity and availability incidents were escalated and reviewed by the appropriate team and required action was taken.	No Exceptions Noted
CCL-67 - Quarterly, Service management reviews and discuss system availability and reliability and addresses any issues.	• Inquired with Service Engineers that processes are in place to review system availability on a quarterly basis. • Obtained and inspected that selected availability reviews were performed and marked as appropriate. • Inspected that any identified issues in the review were documented, tracked, followed-up on and resolved.	No Exceptions Noted
CCL-68 - Annually, Services senior management reviews and approves the capacity for Service's systems.	• Inquired with Service Engineers that procedures have been established to review Services' capacity annually. • Obtained and inspected that the annual capacity review was attended by appropriate personnel and approved for current year.	No Exceptions Noted
CCL-69 - Services have an architecture in place that supports the recovery of services through tools and services supporting the overall Service.	• Inquired with Service Engineers that the Services have processes in place to support the recovery of services. • Inspected the configuration of Services' geo-redundant design within the Akamai tool to ascertain that the tool is configured to support service recovery.	No Exceptions Noted
CCL-70 - Services conduct an annual review of the system's data flow to validate its accuracy, and update it if necessary.	• Inquired of Service Engineers to ascertain that data flow diagrams are reviewed and updated on an annual basis. • Obtained and inspected each data flow diagram to ascertain that the defined processes were accurate and updated if necessary.	No Exceptions Noted
CCL-76 - The third party Global Traffic Management (GTM) provider activity log is reviewed on quarterly basis to determine changes to the Service's properties were appropriate and authorized.	• Inquired with Software Engineers that procedures have been established to review the Akamai activity log for unauthorized changes. • Obtained and inspected that selected activity log reviews were marked as appropriate. • Inspected that selected changes from the reviews had an associate work item documenting the reason for the change. • Inspected that only authorized individuals committed changes during the period.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-78 - Commerce adheres to the Enterprise Business Continuity Management and Standard. The Service's business continuity plans (BCPs) are reviewed and approved at least annually.	• Inquired of Service Engineers to ascertain that Business Continuity Management and Standards are defined. • Obtained and inspected the Business Continuity Management and Standards to ascertain that the Business Continuity Program was updated annually. • Inquired of Service Engineers to ascertain that failover tests occur on a regular basis. • Obtained and inspected that for a selection failover test, that the test was completed as designed, and that any issues identified were assigned to an appropriate owner and being tracked to resolution.	No Exceptions Noted
CCL-92 - For teams utilizing the Developer / Operations model, system configurations are in place to prevent implementation of unapproved changes to production.	• Inquired of Software Engineers that for the teams using the Developer / Operations model, restrictions are in place to monitor or limit access to implement unapproved changes. • Obtained and inspected evidence that system configurations are in place to deny deployment of unapproved changes.	No Exceptions Noted
CCL-94 - Quarterly, services validate that the Qualys agent is running on in-scope VMs.	• Inquired of Software Engineers that procedures are established to review that the Qualys agent is installed on VMs. • Obtained and inspected that selected reviews marked the Qualys agent as running without errors on all machines. • Inspected the XTS dashboard that all production machines had Qualys running without errors.	No Exceptions Noted
CCL-98 - The Production and Pre-Production environment (PPE) are separated. New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments.	• Inquired with Software Engineers that production and Pre-Production (PPE) environments were separated so that changes were tested prior to deployment to production. • Inspected that the XTS tool defines each environment and production or PPE. • Inspected and corroborated that Azure subscriptions were defined in ServiceTree as supporting production or PPE.	No Exceptions Noted
CCL-101 - Failover procedures are defined and at least annually, integrity checks are performed through standard restoration activities.	• Inquired with Service Engineers that fail-over procedures are defined in the Business Continuity Plans, and annual integrity checks are performed. • Obtained and inspected that the annual fail-over test occurred and was documented in a ticket. • Obtained and inspected evidence that any issues identified is resolved.	No Exceptions Noted
CCL-111 - A root cause analysis of the incidents will be performed to reduce the likelihood or impact of future incidents; if applicable.	• Inquired of Service Engineers that procedures for performing a root cause analysis have been established. • Obtained and inspected evidence for a selection of Sev 1 and Sev 2 incidents to ascertain that identified security incidents were responded to in a timely manner. • Inspected that selected incidents had a root cause analysis performed if necessary.	DataGrid For DataGrid this control activity could not be tested, as there was no related activity during the examination period. NGP No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-118 - Training is provided as needed (i.e., LOB apps, Microsoft Office, etc.). In addition, all outsourced providers are trained to understand and comply with Microsoft's code of conduct.	• Inquired with Compliance Managers the process for citing expectations from outsourced providers to achieve specific deliverables and training outsourced providers on Microsoft's supplier code of conduct. • Inspected the supplier procurement website to ascertain that Microsoft's supplier code of conduct was available and accessible to all outsourced providers. • Observed during the supplier access provisioning process that completion of the supplier code of conduct training was required.	No Exceptions Noted
CCL-119 - Management holds all outsourced service providers accountable to achieving specific deliverables, as outlined in a Statement of Work.	• Inquired with Compliance Managers the process for citing expectations from outsourced providers to achieve specific deliverables and training outsourced providers on Microsoft's supplier code of conduct. • Obtained and inspected Microsoft's SOW template to ascertain that it cited outsourced providers' role and accountability in achieving specific deliverables.	No Exceptions Noted
CCL-132 - The baseline configuration for Security Groups (SGs) enforce a requirement for SG Owner's approval for adding new users to the SG.	• Inquired with Service Engineers that the baseline configurations for Security Groups (SGs) enforce approval before provisioning new users. • Inspected that the SGs configurations in IDWEB required owner approval for new users. • Obtained and inspected the group activity logs for each SG that the owner approval configuration had been enabled throughout the whole period.	No Exceptions Noted
CCL-147 - Only variants that are approved by CELA are registered in PDMS.	• Inquired with Compliance Managers that procedures are established to approve variants before being registered in PDMS. • Obtained and inspected that selected variant was approved by CELA before being registered in PDMS. • Inspected that the variant had been uploaded to SharePoint and marked as approved.	No Exceptions Noted
CCL-148 - JIT activity is documented within a DevOps or ICM ticket describing the reason for and changes made during the login session.	• Inquired with Software Engineers that procedures established how JIT access was documented and logged. • Obtained and inspected that log of JIT activity was appropriately thorough. • Obtained and inspected that selected JIT instances had accompanying work item associated with the change and only authorized users elevated to JIT.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CCL-149 - Services maintain an inventory of all Azure subscriptions in the Service Tree. An inventory of all resources residing within each Service's Azure subscription is maintained within the Azure Portal. Access to service tree and Azure portal is restricted to authorized individuals.	• Inquired with Software Engineers that procedures are established for storing Azure subscriptions and restricting access. • Inspected Service Tree that production subscriptions were inventoried. • Inspected Service Tree that users with access to production subscriptions appear appropriate. • Obtained and inspected that quarterly access reviews check that users with access to Azure subscriptions are authorized.	No Exceptions Noted
CCL-169 - Services maintain and communicate the confidentiality and related security obligations for customer data via the Microsoft Trust Center.	• Inquired of the management on the process for maintaining and communicating confidentiality and related security obligations for customer data to customers. • Inspected Microsoft Trust Center to ascertain that confidentiality and related security obligations were maintained and communicated to customers. • Obtained and inspected changes documented in Microsoft Trust Center to ascertain that changes related to the confidentiality and related security obligations were communicated to customers.	No Exceptions Noted
CCL-178 - Component Governance scanner is Integrated with the build definition to detect Open Source code and to alert whether there are vulnerabilities or legal impacts associated with the identified Open Source code/software.	• Inquired of Service Engineers that processes for Component Governance scanning have been established and outline requirements for addressing identified issues. • Obtained and inspected evidence that Component Governance scans were configured within production build definitions. • Obtained and inspected evidence that the Component Governance scan occurs prior to releasing changes to production.	No Exceptions Noted
CCL-185 - On an annual basis the list of the users with access to the Pilotfish environment is reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner. Changes in the access in Pilotfish environment must go through the change management process.	• Inquired with Service Engineers that PilotFish access was reviewed on an annual cadence. • Obtained and inspected that the PilotFish access review was marked as appropriate. • Obtained and inspected that selected users with PilotFish access were appropriate. • Inspected that users marked for change were removed accordingly, if applicable.	No Exceptions Noted

Section V: Supplemental information provided by the Service Organization

Section V: Supplemental information provided by Service Organization

The information included in Section V of this report is presented by Microsoft Corporation ("Microsoft") to provide additional information to user entities and is not part of Microsoft's description of the system. The information included here in Section V has not been subjected to the procedures applied in the examination of the description of the system related to NGP-PIMS, and accordingly, Deloitte & Touche LLP expresses no opinion on it.

Business continuity planning

The NGP and DataGrid services incorporate resilient and redundant features in each service and utilize Microsoft's enterprise-level datacenters. These data centers use the same world-class operational practices as Microsoft's corporate line of business applications and provide a comprehensive solution for the company's online services with the ability to meet the high standards of its customers.

The company's online services designs include provisions to quickly recover from unexpected events, such as hardware or application failure, data corruption, or other incidents that may affect a subset of the user population. The company's service continuity solutions and framework are based on industry best practice and are updated on a regular basis to support Microsoft's ability to recover from a major outage in a timely manner.

ISO/IEC standards 27001:2015 and 27018:2014

NGP-PIMS is compliant with ISO standard 27001:2015 and 27018:2014, published jointly by the ISO and the International Electrotechnical Commission (IEC).

ISO27000 series of standards were developed in the context of the following core principles:

> "The preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)."

NGP-PIMS has undergone the ISO 27001 and ISO 27018 certification, and services have been certified by the British Standards Institute as follows.

NGP: ISO 27001 and 27018 (Issue Date – September 23, 2019)

DataGrid: ISO 27001 (Issue Date – September 23, 2019)

Cloud service continuous improvements

NGP-PIMS is a dynamic service, which Microsoft continually updates with the latest features and functionality. While new features and functionality are regularly being added to these services, the risk-based controls applied to the new components are expected to remain consistent with the risk-based controls applied to the existing NGP-PIMS services.

Management's response to control exceptions

The table below contains Management's responses to the exceptions identified in **Section IV – Information Provided by Independent Service Auditor Except for Trust Services Criteria and Control Activities**

Control Activity & Exception	Management's Response
CCL-40 – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change. Exception Access for one DataGrid user was not removed within 10 business days of changing roles. Access for one NGP user was not removed from within 10 business days of changing roles.	The risk related to this identified exception is deemed low. Procedures, including a review of activity logs for high risk credential actions, were performed to confirm that there was no inappropriate activity related to the account. Access was removed upon identification, during the periodic user access review. Follow-up training was provided to the team to reinforce the standard operating procedures for terminations.

Controls not subject to this examination

The following controls have been put in place by Microsoft, but have not occurred, and were not tested as part of this examination.

Control Activity	Management's Note
CCL-61 – CDG Security handles/monitors security and incident alerts on an ongoing basis and communicates required actions and response efforts. Corrective actions, if required, are performed in a timely manner.	No occurrence of security incidents relating to the NGP or DataGrid systems. Monitoring procedures are in place to alert and process security incidents as part of CCL-60.
CCL-111 (DataGrid) - A root cause analysis of the incidents will be performed to reduce the likelihood or impact of future incidents; if applicable.	No occurrence of security incidents relating to the DataGrid system. Monitoring procedures are in place to alert and process security incidents as part of CCL-60.