Microsoft Corporation – Next Generation Privacy – Privacy Information Management System

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

May 31, 2018

Deloitte.

Table of contents

Executive summary

Microsoft Corporation—NGP-PIMS	
Scope	Next Generation Privacy – Privacy Information Management System (NGP – PIMS)
Period of Examination	As of May 31, 2018
Applicable Trust Principles	Security and Availability
Locations	Redmond, WA
Subservice Providers	Yes: • Microsoft Azure ("Azure")
Opinion Result	Unqualified
Testing Exceptions	0
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 (the "Service Organization") related to Next Generation Privacy – Privacy Information Management System (NGP-PIMS) related to its online service as of May 31, 2018 (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* (American Institute of Certified Public Accountants (AICPA), *Description Criteria*), ("description criteria") and the suitability of the design of controls stated in the Description as of May 31, 2018, to provide reasonable assurance that NGP-PIMS' 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* (AICPA, *Trust Services Criteria*).

The information included in **Section IV**, *Supplemental information provided by the Service Organization*, is presented by management to provide additional information and is not a part of the Description. Information about controls not subject to this examination has not been subjected to the procedures applied in the examination of the Description and the suitability of the design of the controls to achieve NGP-PIMS's service commitments and system requirements based on the applicable trust services criteria.

NGP-PIMS uses subservice organization Microsoft Azure to provide Platform-as-a-Service (PaaS) cloud services for hosting the NGP-PIMS applications. The Description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at NGP-PIMS, to achieve NGP-PIMS's service commitments and system requirements based on the applicable trust services criteria. The Description presents NGP-PIMS's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of NGP-PIMS'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 of such complementary subservice organization controls.

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

Service Organization's Responsibilities

The Organization 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 NGP-PIMS's service commitments and system requirements were achieved. NGP-PIMS has provided the accompanying assertion titled "Assertion of Service Organization Management" ("assertion") about the Description and the suitability of the design of controls stated therein. NGP-PIMS 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 of controls stated in the Description based on our examination. Our examination was conducted in accordance with attestation standards established by the 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 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 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
- 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
- Evaluating the overall presentation of the description

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

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 of 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.

Opinion

In our opinion, in all material respects:

a. The Description presents the NGP-PIMS system that was designed and implemented as of May 31, 2018, in accordance with the description criteria.

b. The controls stated in the Description were suitably designed as of May 31, 2018, to provide reasonable assurance that NGP-PIMS's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of the Service Organization's controls as of that date.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the Description and, accordingly, do not express an opinion thereon.

Restricted Use

This report is intended solely for the information and use of the Service Organization, user entities of the Service Organization's system related to NGP-PIMS as of May 31, 2018, 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 5, 2018

Section II:
Management’s assertion

Section II:
Management's assertion

As of May 31, 2018

Assertion of Service Organization Management

We have prepared the accompanying description of Microsoft Corporation's ("Microsoft") Next Generation Privacy – Privacy Information Management System (the "Service Organization" or NGP-PIMS) related to its online service as of May 31, 2018 (the "Description") 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* (AICPA, *Description Criteria*) (description criteria). The Description is intended to provide report users with information about the NGP-PIMS system that may be useful when assessing the risks arising from interactions with the Service Organization's system, particularly information about system controls that the Service Organization 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 (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, (*AICPA*, Trust Services Criteria)*.

NGP-PIMS uses Microsoft Azure to provide PaaS cloud services for hosting the NGP-PIMS applications. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at NGP-PIMS, to achieve NGP-PIMS's service commitments and system requirements based on the applicable trust services criteria. The Description presents NGP-PIMS's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of NGP-PIMS'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 are necessary, along with controls at NGP-PIMS to achieve NGP-PIMS's service commitments and system requirements based on the applicable trust services criteria. The Description presents NGP-PIMS's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of NGP-PIMS's controls.

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

a. the Description presents NGP-PIMS's system that was designed and implemented as of May 31, 2018, in accordance with the description criteria.

b. the controls stated in the Description were suitably designed as of May 31, 2018, to provide reasonable assurance that NGP-PIMS'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 NGP-PIMS's controls as of that date.

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 (PCF), 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.
- **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.
- **Visual Studio Team Services (VSTS)** – Automated configurations are placed within NGP and DataGrid deployment and source code management tool, VSTS, 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.

---

[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.

- **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).
- **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:

- PDMS: responsible for development and maintenance of the PDMS system.
- PXS: responsible for development and maintenance the PXS system.
- PCF: responsible for development and maintenance of the PCF system.
- PCD: responsible for development and maintenance of 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.
- Windows and Devices Group (WDG) Security – Manages cross-platform security functions, such as security incident response, security monitoring, and vulnerability scanning.

- Universal Store (UST) Governance, Risk, and Compliance (GRC) – 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, AAD RVS, CosmosDB[6], DataMap, and IcM.
- WDG 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

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

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

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 Corporate External & Legal Affairs (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, UST GRC team has established the change management policy, which is communicated to the NGP and DataGrid team members via UST GRC'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 UST GRC 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, availability, processing integrity, and confidentiality 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

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

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.

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.

---

[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.

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 UST GRC 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.

UST Risk Assessment

In addition to the above Microsoft-wide risk assessments, UST 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 UST 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 UST GRC 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 UST GRC, WDG Security, 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 VSTS.

Access Management

Access to NGP and DataGrid services, related data stores, code base, and deployments must be authorized, conform to UST'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 VSTS 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, VSTS, 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.

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 segregated and resides within NGP's Azure storage in a staging container before it is copied over to tenant's instance of Azure through SAS write token. The SAS write token is provided as part of 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

[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.

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 WDG Security Operations team uses Qualys to monitor assets and assess vulnerabilities across the WDG organization, including the NGP and DataGrid system. To ensure that NGP and DataGrid systems are appropriately monitored for security vulnerabilities, the WDG Threat Vulnerability Monitoring Qualys agent is installed on all NGP and DataGrid VMs. In addition to Qualys, Microsoft's WDG 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 WDG 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 WDG 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 UST GRC 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.

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 UST GRC 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 fail over 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, 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.	**CC6.5**
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**
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.	**CC6.7**
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 are hosted.	**CC8.1**

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 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**

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.

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** – The Universal Store has implemented Microsoft governance policies and procedures reflecting requirements of the current business, regulatory and compliance environments. The policy/procedure are reviewed, approved, published, and formally communicated to all service teams at least annually or more frequently, as necessary. **CCL-02** – On an annual basis, OLC reviews the SBC and updates the standards as necessary. The code is made available to all employees internally on CELAWeb and externally at www.microsoft.com/compliance. **CCL-117** – OLC provides an annual SBC 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** – Values are accessible to employees via the Values SharePoint site. The values govern employees' interactions in their workgroup, across teams, with partners, and with customers.
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 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** – The 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 are 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 (anticorruption, confidential information, insider trading, whistle-blowing, global trade, etc.). Policies are located at the Company's MS Policy SharePoint site and are readily available. **CCL-08** – UST adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDLC 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, and Cryptography standard and OSSS, 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-15** – UST 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.

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-118** – Training is provided as needed (Line of Business apps, Microsoft Office, etc.). In addition, all outsourced providers are trained to understand and comply with Microsoft's vendor code of conduct. **CCL-119** – Microsoft holds all outsource service providers accountable to achieving specific deliverables, as outlined in a contract. NGP and DataGrid monitor their dependencies on third parties based on service requirements. **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 HR 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** – Annual and Midyear Reviews **–** Employees hold midyear check in discussions with their managers to validate they are on the expected career path. They also review their performance against their commitments at that time. Additionally, employees and managers discuss overall performance and results against commitments relative to peers in the organization during the annual performance review.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**CCL-15** – UST 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-08** – UST adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDLC 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, and Cryptography standard and OSSS, 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 are required to attend this training on an annual basis. Employees are made aware of their roles and responsibilities with regard to information security. **CCL-14** – Annual and Midyear Reviews - Employees hold midyear check in discussions with their managers to validate they are on the expected career path. They also review their performance against their commitments at that time. Additionally, employees and managers discuss overall performance and results against commitments relative to peers in the organization during the annual performance review.

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** – UST adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDLC 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, and Cryptography standard and OSSS, 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 internal control over financial reporting 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-23** – UST adheres to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability, and processing integrity commitments. **CCL-21** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management.
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** – The Universal Store has implemented Microsoft governance policies and procedures reflecting requirements of the current business, regulatory and compliance environments. The policy/procedure are reviewed, approved, published, and formally communicated to all service teams at least annually or more frequently, as necessary. **CCL-08** – UST adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDLC 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, and Cryptography standard and OSSS, 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-21** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management.

Criteria	NGP-PIMS Control Activity
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**CCL-20** – The company maintains several mechanisms that permit employees and nonemployees to communicate confidential and/or anonymous reports concerning Business Conduct. Compliance concerns may be communicated several ways: sending an email to msft.buscond@alertline.com, accessing an external website, www.microsoftintegrity.com and using the Web allegation tool to communicate concerns to OLC, calling the Business Conduct Line 24-hour number at +1 877 320 MSFT (6738) or International Toll-Free number at +1 704 540 0139, and emailing the Business Conduct and Compliance alias at buscond@microsoft.com. The individual may also send a letter or confidential fax +1 425 705 2985 reporting the concern to Microsoft's Director of Compliance. **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-83** – Services maintain and communicate the 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** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management. **CCL-23** – UST adheres to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability, and processing integrity commitments. **CCL-22** – The identified risks that would impair system security, confidentiality, availability, and processing integrity are reviewed and approved by NGP and DataGrid management. The status of the risk mitigation strategies and control gaps is 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-23** – UST adheres to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability, and processing integrity commitments. **CCL-22** – The identified risks that would impair system security, confidentiality, availability, and processing integrity are reviewed and approved by NGP and DataGrid management. The status of the risk mitigation strategies and control gaps is 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** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management. **CCL-25** – CELA reports confirmed or potential fraud matters to the external auditor, 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, 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 fall under the Section 302 definition and confirm that any such matters have been or will be further disclosed by CELA to the ACs 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 and coordination of a worldwide community across CELA, 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 on an internal Microsoft website.
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-23** – UST adheres to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability, and processing integrity commitments. **CCL-22** – The identified risks that would impair system security, confidentiality, availability, and processing integrity are reviewed and approved by NGP and DataGrid management. The status of the risk mitigation strategies and control gaps is 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-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** – The 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 are based on an annual risk assessment. **CCL-33** – Penetration testing (internal or external) or threat modeling is performed in the NGP and DataGrid system at least annually, or after any significant infrastructure changes. Corrective action, if required, is performed in a timely manner. **CCL-22** – The identified risks that would impair system security, confidentiality, availability, and processing integrity are reviewed and approved by NGP and DataGrid management. The status of the risk mitigation strategies and control gaps is monitored by the assigned owners.
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-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** – The 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 are based on an annual risk assessment. **CCL-22** – The identified risks that would impair system security, confidentiality, availability, and processing integrity are reviewed and approved by NGP and DataGrid management. The status of the risk mitigation strategies and control gaps is monitored by the assigned owners. **CCL-30** – IA has open access to the AC members and attends regular meetings with the AC 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** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management. **CCL-22** – The identified risks that would impair system security, confidentiality, availability, and processing integrity are reviewed and approved by NGP and DataGrid management. The status of the risk mitigation strategies and control gaps is 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. **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.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**CCL-23** – UST adheres to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability, and processing integrity commitments. **CCL-22** – The identified risks that would impair system security, confidentiality, availability, and processing integrity are reviewed and approved by NGP and DataGrid management. The status of the risk mitigation strategies and control gaps is 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** – The Universal Store has implemented Microsoft governance policies and procedures reflecting requirements of the current business, regulatory and compliance environments. The policy/procedure are reviewed, approved, published, and formally communicated to all service teams at least annually or more frequently, as necessary. **CCL-08** – UST adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDLC 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, and Cryptography standard and OSSS, 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 are required to attend this training on an annual basis. Employees 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-34** – NGP and DataGrid maintain an inventory of all Azure subscriptions in the Service Tree. An inventory of all resources residing within each NGP Azure subscription is maintained within the Azure portal. Access to service tree and Azure portal is restricted to authorized individuals. **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. Quarterly or upon addition of any new role/security groups the RBAC document is reviewed. **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 Frontdoor, 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-37** – On a quarterly basis, the UST GRC team conducts a review of users who have administrator access rights to production servers to ensure that access is restricted to those who are authorized and appropriate based on their job responsibilities. Inappropriate access identified as part of the user access review is removed. **CCL-40 (except DataGrid)** – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within two business days or as per policy, whichever is earlier. Access at the application level will be removed within 10 business days of the termination date. **CCL-41** – RBAC is implemented within the NGP and DataGrid systems to enforce the concepts of the least privilege access and segregation of the incompatible duties. **CCL-43** – Tenant restricted data is encrypted when transmitted between the customer and Microsoft, as well as when transmitted between Microsoft data centers, in accordance with Microsoft Security Policy. **CCL-47** – Credential monitoring is performed in each build to prevent credentials from existing in NGP and DataGrid source code. **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 the password configuration and authentication processes for NGP and DataGrid in accordance with Microsoft security policy.

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. Quarterly or upon addition of any new role/security groups the RBAC document is reviewed. **CCL-40 (except DataGrid)** – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within two business days or as per policy, whichever is earlier. Access at the application level will be removed within 10 business days of the termination date. **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 Frontdoor, 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-37** – On a quarterly basis, the UST GRC team conducts a review of users who have administrator access rights to production servers to ensure that access is restricted to those who are authorized and appropriate based on their job responsibilities. Inappropriate access identified as part of the user access review is removed. **CCL-152** – Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the UST 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.
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. Quarterly or upon addition of any new role/security groups the RBAC document is reviewed. **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 Frontdoor, 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-152** – Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the UST change management process. **CCL-40 (except DataGrid)** – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within two business days or as per policy, whichever is earlier. Access at the application level will be removed within 10 business days of the termination date.
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.

Criteria	NGP-PIMS Control Activity
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-40 (except DataGrid)** – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within two business days or as per policy, whichever is earlier. Access at the application level will be removed within 10 business days of the termination date. **CCL-52** – Assets (data or physical assets) are retired in a manner commensurate with security and privacy requirements, classification, and in accordance with any applicable rules, laws, and regulations. **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.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**CCL-33** – Penetration testing (internal or external) or threat modeling is performed in the NGP and DataGrid system at least annually, or after any significant infrastructure changes. Corrective action, if required, is performed in a timely manner. **CCL-43** – Tenant restricted data is encrypted when transmitted between the customer and Microsoft, as well as when transmitted between Microsoft data centers, in accordance with Microsoft Security Policy. **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.
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.	**CCL-43** – Tenant restricted data is encrypted when transmitted between the customer and Microsoft, as well as when transmitted between Microsoft data centers, in accordance with Microsoft Security Policy. **CCL-47** – Credential monitoring is performed in each build to prevent credentials from existing in NGP and DataGrid source code. **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 controlling network devices and configurations, and access to the networking system is restricted to authorized personnel to meet the entity's objectives.

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-54** – OS patching is automatically deployed to all NGP and DataGrid system resources through PilotFish. WDG runs the scan to determine that all VMs have updated security patches. WDG will notify services regarding any outdated security patches. **CCL-33** – Penetration testing (internal or external) or threat modeling is performed in the NGP and DataGrid system at least annually, or after any significant infrastructure changes. 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, the log is reviewed to determine only appropriate users logged into the production environment. **CCL-148** – JIT activity is documented within an VSTS or ICM ticket describing the reason for and changes made during the login session. **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. Quarterly or upon addition of any new role/security groups the RBAC document is reviewed. **CCL-60** – An IcM ticket is opened for incidents, and issues are addressed within reasonable timeframe. **CCL-84** – The WDG Security team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **CCL-92** – For teams utilizing the Developer/Operations model, system configurations are in place to prevent implementation of unapproved changes to production.

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-33** – Penetration testing (internal or external) or threat modeling is performed in the NGP and DataGrid system at least annually, or after any significant infrastructure changes. Corrective action, if required, is performed in a timely manner. **CCL-84** – The WDG Security team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **CCL-59** – The JIT access to production environment is logged, and on a quarterly basis, the log is reviewed to determine only appropriate users logged into the production environment. **CCL-148** – JIT activity is documented within an VSTS or ICM ticket describing the reason for and changes made during the login session.
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-33** – Penetration testing (internal or external) or threat modeling is performed in the NGP and DataGrid system at least annually, or after any significant infrastructure changes. 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, the log is reviewed to determine only appropriate users logged into the production environment. **CCL-148** – JIT activity is documented within an VSTS or ICM ticket describing the reason for and changes made during the login session. **CCL-84** – The WDG Security team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **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-33** – Penetration testing (internal or external) or threat modeling is performed in the NGP and DataGrid system at least annually, or after any significant infrastructure changes. Corrective action, if required, is performed in a timely manner. **CCL-84** – The WDG Security team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **CSOC** – Microsoft Azure is responsible for monitoring and addressing security events and incidents related to the NGP-PIMS systems hosted on Azure platform services.
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-29** – Annually, the NGP and DataGrid Security Champ and WDG Security team review the security confidentially and process integrity of the NGP and DataGrid systems. **CCL-84** – The WDG Security team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.

Criteria	NGP-PIMS Control Activity
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	**CCL-34** – NGP and DataGrid maintain an inventory of all Azure subscriptions in the Service Tree. An inventory of all resources residing within each NGP azure subscription is maintained within the Azure portal. Access to service tree and Azure portal is restricted to authorized individuals. **CCL-84** – The WDG Security team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures. **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-55** – Development of new features and major changes to NGP or DataGrid follow a defined approach based on the Microsoft SDL methodology. **CCL-56** – Changes are tested and technical specifications and/or configurations are validated for appropriateness. Testing results and Technical signoff are retained as defined in the UST Change Management Policy. **CCL-57** – Changes are appropriately approved prior to release to production in accordance with UST's change management policy. **CCL-58** – NGP uses autodeployment configurations to ensure all new features and major changes are appropriately approved prior to deployment to production. **CCL-59** – The JIT access to production environment is logged, and on a quarterly basis, the log is reviewed to determine only appropriate users logged into the production environment. **CCL-47** – Credential monitoring is performed in each build to prevent credentials from existing in NGP and DataGrid source code. **CCL-64** – Production commercial data is not stored or processed in NGP nonproduction environments. **CCL-85** – For teams utilizing the Developer/Operations model, system configurations are in place to prevent implementation of unapproved changes to production. **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-23** – UST adheres to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability, and processing integrity commitments. **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-22** – The identified risks that would impair system security, confidentiality, availability, and processing integrity are reviewed and approved by NGP and DataGrid management. The status of the risk mitigation strategies and control gaps is monitored by the assigned owners.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	**CCL-119** – Microsoft holds all outsource service providers accountable to achieving specific deliverables, as outlined in a contract. NGP and DataGrid monitor their dependencies on third parties based on service requirements. **CCL-23** – UST adheres to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability, and processing integrity commitments. **CCL-22** – The identified risks that would impair system security, confidentiality, availability, and processing integrity are reviewed and approved by NGP and DataGrid management. The status of the risk mitigation strategies and control gaps is monitored by the assigned owners.

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 through a centralized dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed. **CCL-67** – Monthly, NGP management reviews and discusses system availability and addresses any issues. Quarterly, DataGrid management reviews and discusses system availability and addresses any issues. **CCL-68** – Annually, NGP and DataGrid senior management reviews and approves the capacity for NGP and DataGrid 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-69** – NGP and DataGrid have an architecture in place that supports the recovery of services through tools and services supporting the overall NGP-PIMS service. These include controls in place over appropriate access to and changes to tool and service settings. **CCL-17** – The services have geo-redundant design and run in an active/passive (or active/active) configuration. Service's fail-over requirements are configured in a fail-over tool, and access is limited to authorized administrators to modify the configurations. **CCL-24** – DataGrid Elasticsearch cluster is backed up manually. **CCL-34** – NGP and DataGrid maintain an inventory of all Azure subscriptions in the Service Tree. An inventory of all resources residing within each NGP azure subscription is maintained within the Azure portal. Access to service tree and Azure portal is restricted to authorized individuals. **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** – The NGP and DataGrid BCPs are reviewed and tested 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.

Section IV: Supplemental information provided by Microsoft

Section IV: Supplemental information provided by Service Organization

The information included in Section IV of this report is presented by Microsoft to provide additional information to user entities and is not part of NGP-PIMS's description of the system. The information included here in Section IV 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 July 25, 2018)

DataGrid: ISO 27001 (Issue Date July 3, 2018)

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.

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-40 (DataGrid) – 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. Access at the application level will be removed within 10 days of the termination date.	No occurrence of terminations for the DataGrid system.
CCL-61 – WDG Security receives security and incident alerts on an ongoing basis. Notification of required actions and response efforts are communicated internally. Corrective action, if required, is 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-84.