Data Platform (xDP)

Security Statement

Data Classification: Public

November 2022

Table of Contents

Introduction

This statement provides a high level overview of the Information Technology (IT) Security Measures implemented for PricewaterhouseCoopers, LLP's Data Platform (xDP). Data Platform is a product/technology that securely stores, analyses and shares data both internally and externally with our clients and our firm.

In this overview, PricewaterhouseCoopers, LLP (PwC) refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network, as applicable. See www.pwc.com/structure for further details. This document is intended for current and potential clients of PwC member firms only (sometimes referred to as "Network Firms"). It must not be distributed further without the prior written consent of a PwC member firm.

This document is intended for information purposes only and is not a commitment to deliver any material, code, or functionality. The development, release, and timing of any feature or functionality for PwC's products remains at PwC's discretion. PwC may update this document from time to time.

System and Architecture Overview

Executive Summary

PwC's Data Platform is an intelligent, global data ecosystem that equips PwC's teams to harness the power of data more effectively and securely than ever before. Designed to meet client needs in all operational geographies, the Data Platform helps our engagement teams connect your business data with next-generation technology to uncover hidden risks and growth opportunities with speed and acuity. Using the Data Platform, our teams can generate quicker and deeper insights so we're prepared to make informed decisions and strategically move our business forward. Accessible by authorised PwC personnel only, the Data Platform facilitates the secure acquisition, storage, cataloging, analysis, modeling and sharing of client data.

User Experience

The Data Platform allows for:

- Data acquisition - rapid and secure access to data from client systems

- Ingestion, storage and cataloguing - the automation of manual processes via intelligent technologies and the ability to search and discover data via the use of a catalogue

- Transforming, modelling and analytics - a self-serve environment with a Workbench that enables PwC engagement teams to efficiently deliver high-quality insights within every client engagement

- Delivery and consumption - an application development framework with embedded machine learning / Artificial Intelligence (AI) capabilities and Application Programming Interface (API) provisioning

In the Data Platform, multiple data acquisition options are facilitated via:

- PwC Extract - securely extracts data from a client enterprise resource planning (ERP) system

- Web upload - manually uploads ad-hoc files via a secure web portal (Workbench)

- Internet of Things (IOT) pipeline - sets up event-driven ingestion pipelines

- External pipeline - sets up a scheduled ingestion pipeline from an internal or external source

- High-speed file transfer - a dropbox-like utility for uploading large data sets

- Fabric API - and extensible API framework enabling “bring-your-own” ingestion technologies

- Skylight - A UI portal, similar to the Workbench portal, that is used solely for sharing Data Platform features and capabilities with external non-PwC users. External users have access to this application using their PwC-provisioned username and password

Users access Data Platform using a laptop or desktop computer via a web browser. Smartphone web browsers and legacy web browsers are not supported at this time. Individual access to Data Platform must be requested and granted by the client team, and provisioned by a relevant administrator that is a member of the PwC engagement, support team, or designated client administrator team. Client data is secured and segregated under a tenant structure.

Architecture

PwC’s Data Platform is a global platform where authorised engagement teams can collect and store client data. The platform’s User Interface (UI) component, known as Workbench, is accessible through a browser-based application and adheres to the following browser-compatibilities:

- Targeted browser support: Google Chrome, Internet Explorer 11, and Edge (Windows 10)

- Targeted device profile: Desktop, Laptop, Tablet and Mobile using an adaptive UI model

The Data Platform can be accessed only by users with PwC accounts via the internal PwC network--i.e., the platform cannot be accessed directly via the public internet, without required PwC authentication. The Data Platform enforces user authentication and permits only PwC authorised users to access the Data Platform.

The Data Platform interacts with various PwC LoS applications and leverages PwC's common utility services, such as Identity and Access Management (PwC Identity) for user identity and authentication, API Management (APIM) for endpoint security, and log aggregation via the Security Information and Event Management (SIEM) system for application logging and monitoring, etc., thereby enabling PwC to have visibility into the platform and to achieve compliance with PwC Information Security Policy (ISP) and Controls Standard.

Embedded in the Data Platform design are controls to secure data in transit and data at rest. The platform stores client data within a “data lake,” which is physically manifested as encrypted storage and logically organised by client and the related engagement. The data lake is secured so that only specific authorised engagement team members can access it.

The backup and data recovery plan is built into the cloud service, which includes backups and high availability. The backup schedule below is defined for the automated backup of databases and virtual machines (VMs) and delivered by Microsoft for PwC.

- Full daily backup
- Five-minute incremental backup
- Transaction logs taken between incremental backups
- Backups retained for 30 days
- Daily VM snapshots taken and retained for 30 days

Data Platform is hosted on the PwC Microsoft Azure cloud network environment, built with standardised components within existing PwC managed cloud environments (see the *Physical and Environmental* section below for further information), using a tiered network architecture design. This environment features firewall segregation between tiers (presentation, application, and data), the Internet, and the internal PwC network. The platform and infrastructure are reviewed on a regular basis to assess compliance with the *PwC Information Security Policy*.

A user account is required to log in to Data Platform. Your system or tenant administrator will allocate a user account to you and provide login credentials (unless a single sign-on has been enabled for your organization).

The database houses user roles and permissions, live and historical asset execution details, and application configuration. User data stored in the database includes email address and client profile metadata.

A SOC2 assessed data platform (based on Microsoft Azure), houses data uploaded by clients and users. Individual records for each user are created within the database to store user uploaded data and system data generated against user uploaded data. System administrators manage the user permissions for accessing the application. No data will be retained for cloud-based assets outside of Data Platform.

A visual diagram that depicts the high-level architecture design for Data Platform is provided in the appendix.

Information Security and Governance

Information Security is a high priority for the PwC network. PwC is accountable to their people, clients, suppliers and other stakeholders to protect information that is entrusted to them.

PwC has established an Information Security Governance Program to maintain procedures for managing risks and delivering strategic recommendations for continuous improvement of the policy, controls, and supporting standards. This continuous improvement program focuses on ongoing identification of areas in the policy, controls, and standards for revision to align with business, technology, and information security strategy. Formal reviews of the program are conducted in two improvement cycles each year. The review process includes a collection of external and internal sources of information to identify emerging risks and candidates to improve information security policy and control standards.

PwC's *Information Security Policy* (*ISP*) outlines the minimum security requirements with which every PwC member firm must comply and is reviewed at least annually. PwC's *ISP* has been developed to safeguard the confidentiality, integrity, and availability of the information and technology assets used by the PwC member firms and is aligned with *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls* industry standard.

Risk Assessment

Risk management and risk assessment underpin PwC's Information Security Program. Key elements include asset inventory and valuation, risk assessment, risk assessment reports, risk treatment plans, and metrics. The Risk Management program defines processes that cover five cornerstones of risk: strategic, applications, infrastructure, third-party providers, and sourcing providers. Risks are assessed using Business Impact Analysis (BIA) on the potential loss of each information asset together with risk assessments of the likelihood of such losses. Information security risks are managed via risk registers in an Enterprise Governance, Risk Management, and Compliance (eGRC) system and are reviewed on a regular basis, together with remediation plans and mitigating controls, to decide upon whether to accept residual risks. For more information about security assessments, see the *Software Development Life Cycle* section below.

Asset Management

Responsibility for Assets

The PwC Technology organization has established and maintains asset inventory processes for information assets. These processes include the following key components:

- Identification of the asset, the information owner, and information custodian
- Determination of the data classification level
- Identification of security risk factors
- Business Impact Assessment (BIA)

Inventory and Classification

Information assets are identified through the asset inventory and classification processes. The information asset classification determines the required security controls to protect these assets and helps define which information-handling procedures are implemented. PwC partners, principals, and staff are educated on identifying and handling sensitive information. This education is both annual and in some circumstances project specific.

Under the PwC data classification framework, PwC operates a four-level data classification system comprising Public, Internal, Confidential and Highly Confidential. Classifying data helps everyone at PwC know how to protect the data entrusted to us. It also gives PwC a common framework to understand the characteristics of a given piece or set of data.

This knowledge helps PwC manage data throughout its lifecycle, and comply with legal, regulatory, and other data protection requirements. Teams are required to identify the types of data being collected and put controls in place to collect only data required to complete the activity, and to ensure that the controls applied are specific to the classification of the data. Internal, Confidential and Highly Confidential data can also be classified as restricted based on regulatory or legal requirements (e.g., General Data Protection Regulation, Health Insurance Portability and Accountability Act of 1996).

Data Platform is rated to store and exchange highly confidential data.

Physical and Environmental

The Data Platform is hosted in the PwC managed Microsoft Azure cloud as part of the PwC Global Hosting Service (GHS) Cloud Service. The platform instances are hosted in three Microsoft Azure regional hosting locations: Australia, the Western Europe and the United States.

The Data Platform instance used for a client engagement is based on several factors, such as the source location of client data, where the data will traverse, configuration in the application by the PwC engagement owner (based on contractual agreement with the client, etc.).

Each Data Platform instance has a data lake hosting the various data sets in a given instance. Data sets are hosted in a single Data Platform instance, and the data lake is hosted in a single region and peered across multiple availability zones. Data sets are logically separated from one another so only authorised PwC personnel can access and view them.

Microsoft is responsible for the physical security and utilities for its data centers and IT assets within those data centers. Please visit Microsoft Azure Regions for more information about Microsoft Cloud hosting locations.

Communications and Operations

Operations

The Data Platform operations team follows the standard IT operating procedure governance process and formal IT incident management procedures established and maintained by PwC. The governance process includes standard procedures, formal written response plan, formal review and approval processes, and revision management, including annual executive review of such policies and procedures. The incident management procedures define roles and responsibilities as well as reporting and escalation procedures for all priority levels of incidents. IT service monitoring is performed on a risk basis for all key IT systems, supported by timely reporting of issues; for example, status alerts incorporated into dashboard reports (or other monitoring tools) for IT operators. IT service monitoring reports are analyzed and reviewed by IT leadership on a timely basis for ongoing issue and trending analysis. Priority levels are defined and an escalation process is used to ensure issues are addressed in a timely manner. Industry standard preventative maintenance for hardware and software is formally planned and completed on a timely basis, taking into account business and user requirements. In addition, issues that may have an impact on client's ability to use the offering are communicated to client on a timely-basis.

Change Management

The formal change control process for Data Platform includes risk assessment, test and communication plans, management review, backout plans, and approval components. This process also incorporates separation of responsibilities for development, testing and migration responsibilities, separate logical environments for development, staging and production, and formal policies and procedures controlling all aspects of application development and maintenance, reviewed by executives on at least an annual basis. The change control process also includes testing sign-offs and authorizations for promotion to the production environment, and emergency procedures for changes that require immediate resolution.

Capacity Management

Capacity management plans have been established and capacity planning reports are reviewed on a continuous basis by the Data Platform programme management, architecture and operations team. The plans include capacity management across all layers of the platform including network, storage, infrastructure, database, and application.

All data is stored in a cloud object store and can be configured to work with a compute cluster of choice as needed. This provides scalable storage isolated from compute clusters and minimises the upfront capacity planning.

Network Security

The Data Platform implements end-to-end encryption for data in transit, which includes the platform's file upload capabilities. The platform observes end-to-end encryption using TLS v1.2 (HTTPS) with a 2048-bit Public Key (i.e., between browser and server AND between all server-side components/middleware).

Access to the Data Platform for authorised PwC users occurs after they're authenticated to the PwC network. This can occur from a PwC office or over a TLS 1.2 secure VPN connection.

Each PwC Azure region consists of a shared service network which hosts common infrastructure as well as separate network environments for pre-production. (e.g., development, QA, staging). The environments are segregated to provide visibility and control. Defence in depth is provided through the use of layered security controls, including web application firewalls, software firewalls and network security groups, to protect against attacks from inside and outside the network.

Segmentation within Azure uses virtual networks, subnets, routing and security groups to restrict cross-communication between components within a virtual network. This architecture applies granular boundaries to resources based on their application tier and only allows intended communication between specific applications.

Data Management

Each client's data is stored in a logically separated engagement container with access limited to authorised PwC engagement team members. Data is collected in the Data Platform for the purposes and duration of the client engagement and then appropriately purged on request or as per PwC retention policies and client contract stipulations.

The Data Platform utilises TDE (Transparent Data Encryption) to transparently encrypt all data at rest using industry standard encryption (e.g., 256-bit AES). The platform specifically uses a combination of Azure Server-side Encryption and PwC-managed key models coupled with application of policy based access controls via a centralised management environment. This delivers the ability to manage the full lifecycle of our keys, including storage, as well as providing protection of structured and unstructured data stores as well as running on servers to protect data-at-rest in files, volumes or databases.

All data in the Data Platform is further protected by two isolated data storage zones--one that only authorised systems can push data to raw storage and for scanning (RED) and another read/write zone that end-user applications can access once tokenization and data validation has occurred (BLUE). Once complete this allows for sensitive data to be de-identified (masked) on request for system processes and general users/applications that have to access it.

The Data Platform leverages cloud based technology for data protection purposes these include tools to support and enhance continuous compliance of the environment, container security and standardised infrastructure builds etc. Data protection practices are reviewed on a regular basis for compliance with applicable laws, industry standards and best practices. Formal Data Protection requirements such as Data Protection Risk Assessment (DPRA) and Data Protection Impact Assessment (DPIA) are in place to assist with appropriately assessing and classifying the data.

All Data Platform cloud storage resources are subject to secure destruction in accordance with PwC ISP and local laws and regulations, using various physical and logical measures when decommissioned.

Formal data protection requirements such as Data Protection Risk Assessment (DPRA) and Data Protection Impact Assessment (DPIA), if applicable, are in place to assist with appropriately assessing and classifying the data. All Data Platform cloud storage resources are subject to secure destruction in accordance with PwC's *ISP* and local laws and regulations, using various physical and logical measures when decommissioned.

Software Development Life Cycle

PwC follows a defined Software Development Life Cycle (SDLC) process, which has been approved by executive management, and reviewed at least annually. The SDLC for Data Platform includes integrated processes to identify and address potential security issues during the development life cycle. During software development, static code security assessments are performed as part of the overall code review process. Application testing is part of the overall SDLC process. Application security assessments are also performed following a defined application security assessment methodology. This methodology includes defined tests and tools to be used, as well as taxonomy for reporting. Risk treatment procedures are in place to address defects or vulnerabilities discovered in the various assessments in a timely manner.

Development Environments

Separate development, testing, stage, and production environments are maintained. Non-production environments are logically separated from production environments. Migration procedures are required to use the change control process when transferring changes from stage to the production environment, including appropriate segregation of responsibilities for managing such. Production data is not used in non-production environments.

Security Assessments

All PwC systems undergo a variety of risk reviews and assessments during the SDLC.

- **Application Readiness Assessment (ARA)**
  Subject matter specialists evaluate applications against an *Application Readiness Standard* to identify risks and provide recommended risk mitigation actions. The *Application Readiness Standard* outlines the minimum information protection requirements for technology systems that collect, process, and store PwC or client information, and is applicable to all Network Firms.

- **Code Review Service (CRS)**
  CRS provides a secure code learning platform and white box binary source code scan to promote secure coding. These services promote secure coding at all cycles of the SDLC and provide deep analyses in an offline

environment of compiled or ready-to-deploy applications to detect security flaws in the underlying code.

- **Security Readiness Testing (SRT)**
  SRT provides comprehensive security testing to ensure applications are ready and suitable for production according to PwC standards. These services include Dynamic Application Security Testing (DAST), Web, Mobile, and Thick Client Application Security Assessments and White and Black Box Penetration Testing.

Automated Routine Security Testing

In addition to the security review processes described above, the application code (current and new development) is scanned routinely with automated tools to identify security and open source component vulnerabilities. These scans are embedded within continuous integration/continuous delivery (CI/CD) processes and executed automatically. All findings are addressed prior to the release of any code in production.

Periodic Application Security Reviews

Periodic application security reviews are conducted to identify security weaknesses that could be exploited by motivated malicious individuals seeking to gain unauthorized access or perform malicious activities against PwC infrastructure. The review employs several processes and procedures to examine security controls built into the service. The examination includes testing that validates controls and provides evidence of compliance with security objectives, at the network, operating system, application, web service and database layers.

Web Service vulnerability identification occurs using web services application assessment tools and manual techniques. Vulnerabilities will also be identified through manual application security testing.

The Application Security Assessment (ASA) is performed leveraging processes and practices based on industry-recognized methodologies, including but not limited to: *The Open Source Security Testing Methodology Manual* (*OSSTMM*), the *Penetration Testing Execution Standard* (*PTES*) and the *Open Web Application Security Project* (*OWASP*) *Application Security Verification Standard* (*ASVS*). Assessments are conducted using industry-leading tools, in addition to advanced custom and proprietary tools and scripts.

The testing uses a combination of manual and tool-based testing to simulate attacks in an attempt to identify vulnerabilities. The vulnerability or weakness in an application can be a logic flaw, code bug, or architectural flaw that allows an attacker to access sensitive information or make the application act in a way it was not intended to be used.

Checks that are performed include the following:

- **Authentication Analysis**
  - Password management
  - Weak authentication methods
  - User enumeration
- **Authorization Analysis**
  - Forceful browsing
  - Parameter tampering
  - Separation of privileges
- **Disclosure of Information**
  - Client-side source code
- **Manipulation of Application Logic**
  - Email spamming
  - Privilege escalation
  - Unrestricted file upload
- **Session Management Analysis**
  - HTTP only attribute not set
  - Persistent cookies
- **Secure Communications Analysis**
  - Cross-site request forgery

    - Detailed error messages
    - Backup files
    - Access to source code

- **Input Validation and Data Sanitisation Analysis**
    - Cross-site scripting - reflected
    - Cross-site scripting - persistent
    - Structured Query Language (SQL) injection

    - Expired certificate
    - Communication not over Secure Sockets Layer (SSL)

Logging and Monitoring

PwC maintains system audit logs for servers and network devices that log the occurrence of system faults and security events, and facilitate the detection and examination of abnormal activities. Alerts are generated according to a predefined set of blacklist and anomalous triggers for external and internal threats, then actioned by analysts using a defined process. Additionally, all requests and responses to and from the Data Platform application programming interface (API) and user interface (UI) are recorded, as are requests and responses to and from external systems. All logs are collected in a central Security Information and Event Management (SIEM) system to prevent the modification or removal of administrator and user activities, and these logs are available to the administrators of the PwC Security Operations Center (SOC). All logging is performed on a 24/7/365 basis.

The Data Platform provides the logging and auditing features listed below. These features are available to the admins or on demand from the PwC Security Operations Centre (SOC).

- System faults - system faults and security events for servers and network devices

- Login history - history of all login attempts, including username, success/failure and time/date

- User setup audit trail - logs of group creation or deletion along with users added or removed from a group for a specific xDP instance (Singapore, the Netherlands and the United States)

- System and application management - logging of activity and event logs of system performance

- Document upload/download - logs user name, role, time/date, document name for each Data Platform instance

Access Management

PwC Users

PwC users access systems via PwC Managed devices connected to the PwC network. User access is based on responsibilities related to access management that are segregated, including a separate and dedicated security administration function and based on their involvement with respect to a given engagement and client. The concepts of “least-privilege” and “need-to-know” access are applied so that administrator and user access is commensurate with their defined responsibilities. Access management policies and procedures are approved by executive management, and are reviewed at least annually.

Authentication and Authorization

The Data Platform utilises the centralised PwC Identity and Access Management (PwC Identity) service for user identity and authentication. The service supports client Federated Identity Management (FIM) which allows clients to integrate their identities with our PwC Identity solution to facilitate ease of access and account generation.

Identity and authentication functions for both individual users and access to the Data Platform application UIs (User Interfaces) and APIs (Application Programming Interfaces) are managed using PwC Identity. This is used in conjunction with our authorisation API, it ensures that all file and data access is secured using a centralised RBAC mechanism.

Virtual private network (VPN) software is leveraged to enable secure, Internet-based remote access for PwC users. PwC VPN users authenticate using two-factor authentication consisting of a valid username/password and a corresponding digital certificate--both of which are required to create a VPN tunnel. VPN tunnels are secured using industry standard encryption (e.g. AES-256).

Privileged Access

Access to servers and other IT infrastructure in an administrator, root, or system-level capacity is limited to the appropriate internal PwC administration staff on a minimum-necessary, need-to-know basis. PwC follows a formal and documented process with approvals to grant or revoke access to PwC resources, which includes specific provisioning, de-provisioning and quarterly reconfirmations of access granted, as well as the use of security groups to manage segregation of duties. PwC has established documented procedures for secure creation and deletion of user accounts, including processes to disable and/or delete accounts for terminated personnel. Multi-Factor Authentication (MFA) is required for all privileged user accounts. PwC also forces separation between database administrators through deployment of separate teams to build and administer the different datasets. Additionally, PwC uses a centralized Privileged Access Management (PAM) system and processes to manage privileged access to systems which includes MFA, centralized logging, activity tracking and administrative session management access.

Leavers

When a PwC staff member leaves, their access is terminated in accordance with PwC's *ISP* and relevant PwC member firm departure procedures. For clients, the principal organization contact is responsible for notifying the relevant PwC support team contact when organization user access should be revoked from Data Platform.

Vulnerability Management

PwC has implemented policies, procedures, and guidelines based on industry best practices and standards, approved at the executive level and reviewed at least annually, that govern activities over threat and vulnerability management.

Multiple vulnerability scanning tools, including firewalls, anti-virus software, and intrusion detection systems (IDS), are used to assess the threat landscape of internal- and external-facing PwC network environments, and monitor on a 24/7/365 basis. These tools are selected and configured to match infrastructure requirements, and are updated on an ongoing basis. In addition, all configurations, including servers, firewalls, IDS and other critical infrastructure, are hardened and are subject to periodic internal evaluation and external penetration testing. Processes are established to assess, prioritize, and remediate vulnerabilities discovered.

Patch management processes are executed to assess and deploy operating system, anti-virus and application specific patches and updates. This process includes steps to evaluate vendor-supplied patches to determine servers that require patches and updates, to document procedures for patching and updating servers, and to deploy patches and updates in a timely manner to protect the PwC network infrastructure.

Patches and updates are assessed as they are released to determine their criticality. Patches released on a regular schedule are applied following their release; while off-cycle or other patches determined to be critical are applied as needed to reduce vulnerabilities. Deferrals for patch updates must be approved by PwC Network Information Security (NIS).

Information Security Incident Management

Data Platform is integrated into the PwC NIS *Threat Management Incident Response Framework* and its protocols are developed in accordance with PwC's *ISP* and applicable local laws and regulations.

Documented policies and procedures, approved by executive management, reviewed and updated on at least an annual basis, are followed for handling security incidents, including predefined roles and responsibilities, and a process to escalate security incidents.

If a security breach may contravene legal, regulatory, or contractual obligations, formal risk mitigation procedures will occur, which may include conducting an appropriate investigation and, where appropriate, disclosing the breach to interested parties, including regulators and law enforcement authorities.

Compliance

Third-Party Monitoring

PwC's Supplier Risk Management Office (SRMO) facilitates an integrated, comprehensive, and sustainable supplier risk assessment program designed to mitigate risks throughout the supplier lifecycle. Suppliers, such as third-party vendors and third-party subcontractors that help deliver the offering, are assessed across a wide range of risk categories including reputation, financial viability, legal, technology, security and regulatory compliance. Program elements include, but are not limited to:

- Suppliers are risk assessed during the initial onboarding process and re-assessed on a periodic basis. Risk assessment related information pertaining to each supplier includes supplier risk score, pending remediation items, and corrective action date and supplier risk assessment results are tracked and managed using a central repository managed by the SRMO. The scope and interval of periodic supplier assessments are based on the risk rating and profile of each supplier. The program operates a dynamic assessment calendar to schedule reviews, which can be adjusted to address priority risk concerns.

- PwC has a process for executing contracts with its suppliers. These contracts provide for the monitoring of suppliers via ongoing risk assessments and risk mitigation tasks throughout the supplier lifecycle. Various internal business owners responsible for the supplier relationship monitor and evaluate performance management and the quality of service delivery. Each ongoing monitoring process is tailored to each supplier based on its risk score, pending remediation items, and corrective action date. Appropriate mitigating controls must be selected for each identified risk and communicated to prospective suppliers during the selection process. These controls are reflected in supplier contracts as commitments and provide a basis on which the supplier is evaluated for ongoing compliance monitoring.

- PwC has implemented security controls designed to ensure that external parties/subcontractors provide services in a manner consistent with PwC's standards for the security of information systems. PwC requires that providers be aware of and contractually bound to adhere to information security requirements and restrictions. PwC's standard third-party agreements include security control requirements. These requirements, based on ISO 27002:2013 section 6.2, include and are not limited to: a documented information security policy, protection of information assets, physical protection controls, return or destruction of information, non-disclosure, security awareness training, change management, access control policy including the use of unique IDs, access authorization process, reporting and investigation of security breaches, right to monitor access, annual review of security requirements, escalation process and applicability to additional subcontractors.

In addition, PwC has implemented a Third Party Risk Management (TPRM) program to ensure that information security expectations are being met by the firm’s trusted third-party suppliers. The TPRM program is run by a dedicated team within the PwC NIS organization, which operates under the firm's Network Chief Information Security Officer (CISO).

Security Awareness

PwC provides its staff with information regarding their security responsibilities and the safe and acceptable use of PwC resources. This information is disseminated via newsletters, phishing simulations, mandatory annual compliance training and other communications to reinforce security awareness. Security awareness training is the responsibility of each member firm, and each member firm’s security awareness program is reviewed as part of the IT security reviews of member firms and external SOC assessment.

Information Security Review

Data Platform hosting locations are subject to periodic security reviews by Microsoft to test compliance with their ISP. PwC NIS performs an annual security monitoring assessment on Microsoft Azure. The assessment analyzes Microsoft’s compliance against PwC’s *ISP* based on their security compliance material and third-party audit reports (e.g., SOC 2 and ISO certification).

Microsoft Azure undergoes annual third-party audits by internationally recognized auditors for an independent validation of policies and procedures around protecting client data. Microsoft Azure has also achieved ISO 27001 (international information security standard) and adopted the world’s first codes of practice ISO/IEC 27017 (information security controls for cloud services) and ISO/IEC 27018 (privacy standard for cloud services).

Visit Microsoft Service Trust Portal for more information.

Open Source Software

Data Platform may include open source components, which are licensed for use and distribution by PwC under applicable open source licenses. Use of these open source components is governed by and subject to the terms and conditions of the applicable open source license.

Business Continuity Management

The Data Platform, which is hosted on Azure Cloud, relies on the high availability, disaster recovery and backup on Azure’s global network to stay compliant with each country’s or region’s legal and regulatory requirements according to the data’s location. The platform maintains important disaster recovery and business continuity plans that may be activated in the event of a significant business disruption. These plans are key components in maintaining emergency procedures and are required by industry regulations. The platform is built on redundant and highly available services within Azure Cloud.

The Data Platform has implemented the ability to have active failover for key components through the use of Azure Traffic Manager. Traffic manager is a DNS-based load balancer. This service allows the distribution of traffic to the public facing applications across the paired global Azure regions (currently running in US-East paired with US-West, West Europe paired with North Europe, AU East paired with an additional AU East Cluster).

The current configuration (see diagram below) allows for:

- Protection against single region failure. AKS (Azure Kubernetes Service) Active/Active environment

- Near 0 downtime upgrades - One environment is LIVE at all times

Data Platform disaster recovery plans are intended to permit the continuation of key business functions during most types of disruptions by resuming mission-critical functions, usually within the same business day as the disruption.

Appendix - Additional Information

Additional questions or concerns may be addressed by your PwC engagement team.

Additional information about PwC's IT security measures are available in the *PwC Information Security Policy (ISP) Security Statement*, which provides a summary overview of the IT security controls in PwC's *ISP* and applies to all PwC member firms for all information and systems.

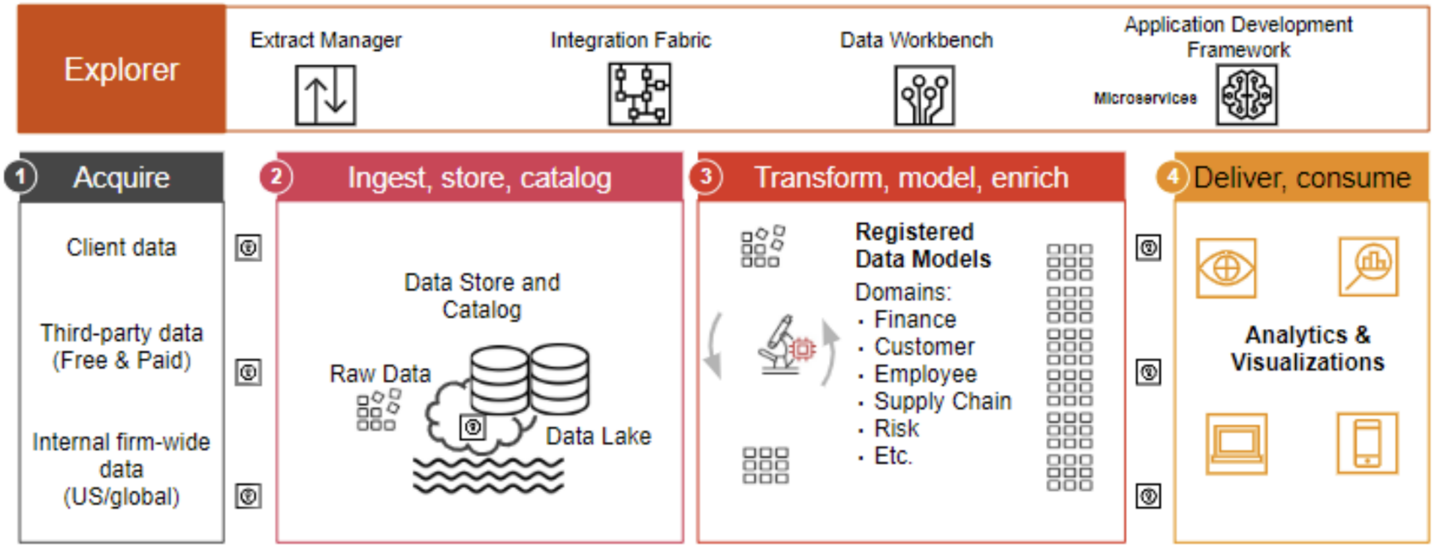
Accessing and use of Data Platform is subject to PwC's terms and conditions that must be agreed prior to any access or use. Access and use of Data Platform is subject to the agreement(s) between PwC and the client, which must be agreed prior to any access or use.

This document contains forward-looking statements. PwC undertakes no obligation to publicly update or revise any forward-looking statements. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations.

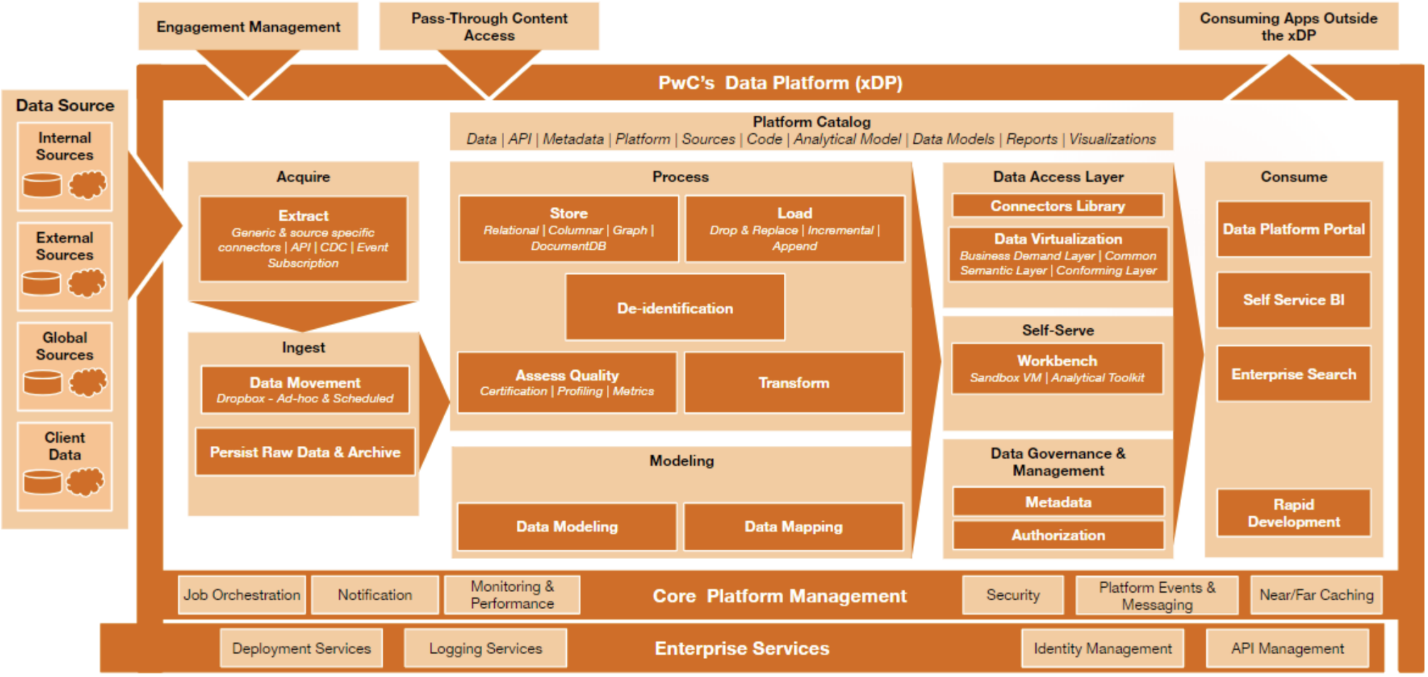
As described above, Data Platform is hosted by third-party cloud providers using e.g., PwC's Global Hosting Services (GHS). More information can be found at:

- Microsoft Azure Geographies: https://azure.microsoft.com/en-us/global-infrastructure/geographies
- Microsoft Trust Center: https://www.microsoft.com/en-us/trust-center
- Microsoft Compliance Guides: https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide
- Microsoft Security Operations: https://www.microsoft.com/en-us/security/business/operations

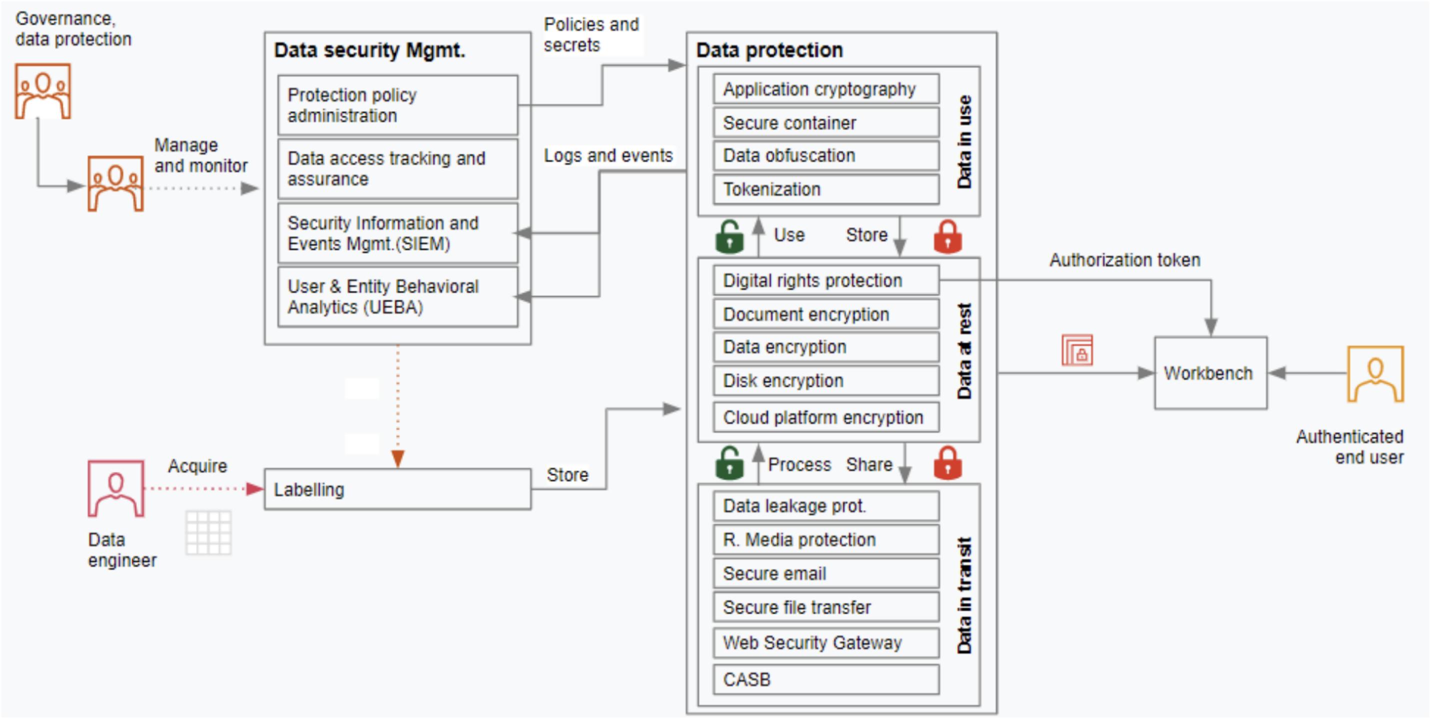
The following diagram depicts the high-level design for Data Platform - System Overview



The following diagram depicts the high-level design for Data Platform - Architecture



The following diagram depicts the high-level design for Communications and Operations - Data Management


Governance, data protection
Manage and monitor
Data security Mgmt.
Protection policy administration
Data access tracking and assurance
Security Information and Events Mgmt.(SIEM)
User & Entity Behavioral Analytics (UEBA)
Policies and secrets
Logs and events
Data protection
Application cryptography
Secure container
Data obfuscation
Tokenization
Data in use
Use
Store
Digital rights protection
Document encryption
Data encryption
Disk encryption
Cloud platform encryption
Data at rest
Process
Share
Data leakage prot.
R. Media protection
Secure email
Secure file transfer
Web Security Gateway
CASB
Data in transit
Authorization token
Workbench
Authenticated end user
Acquire
Labelling
Store
Data engineer