SOC 3 Report

2022

Prepared for:

MarkLogic Corporation

REPORT ON MARKLOGIC CORPORATION'S DESCRIPTION OF ITS DATA HUB PLATFORM AS A SERVICE (PAAS) RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY, PROCESSING INTEGRITY, AND PRIVACY

MarkLogic®

MarkLogic Corporation

Assessment Dates: June 23, 2021, to June 22, 2022

Table of Contents

Section 1 - Assertion of MarkLogic Corporation’s Management

Assertion of MarkLogic Corporation’s Management

August 30, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within MarkLogic Corporation's ("MarkLogic", the "Company", or the "Service Organization") Data Hub Platform as a Service (PaaS) throughout the period June 23, 2021 to June 22, 2022 (description), to provide reasonable assurance that MarkLogic’s service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 23, 2021 to June 22, 2022 to provide reasonable assurance that MarkLogic’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (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). MarkLogic’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 23, 2021 to June 22, 2022 to provide reasonable assurance that MarkLogic’s service commitments and system requirements were achieved based on the applicable trust services criteria.

MarkLogic Corporation Management

Section 2 - Independent Service Auditor’s Report

To: MarkLogic Corporation

Scope

We have examined MarkLogic Corporation's (“MarkLogic", the “Company” or the “Service Organization”) accompanying assertion titled “Assertion of MarkLogic Corporations' Management” (assertion) that the controls within MarkLogic's Data Hub Platform as a Service (PaaS) (system) were effective throughout the period June 23, 2021 to June 22, 2022 to provide reasonable assurance that MarkLogic's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (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*).

Service Organization's Responsibilities

MarkLogic 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 MarkLogic's service commitments and system requirements were achieved. MarkLogic has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion MarkLogic is responsible for selecting, and identifying in it assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve MarkLogic's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve MarkLogic's service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

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 effectiveness 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, management's assertion that the controls within MarkLogic's Data Hub Platform as a Service (PaaS) were effective throughout the period June 23, 2021 to June 22, 2022 to provide reasonable assurance that MarkLogic's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Lazarus Alliance Compliance, LLC

Dover, DE
September 1, 2022

Attachment A - MarkLogic Corporation’s Description of the Boundaries of Its Data Hub Platform as a Service (PaaS)

Company Overview and Services Provided

MarkLogic is an operational and transactional Enterprise NoSQL database platform widely used by global organizations to integrate their most critical data.

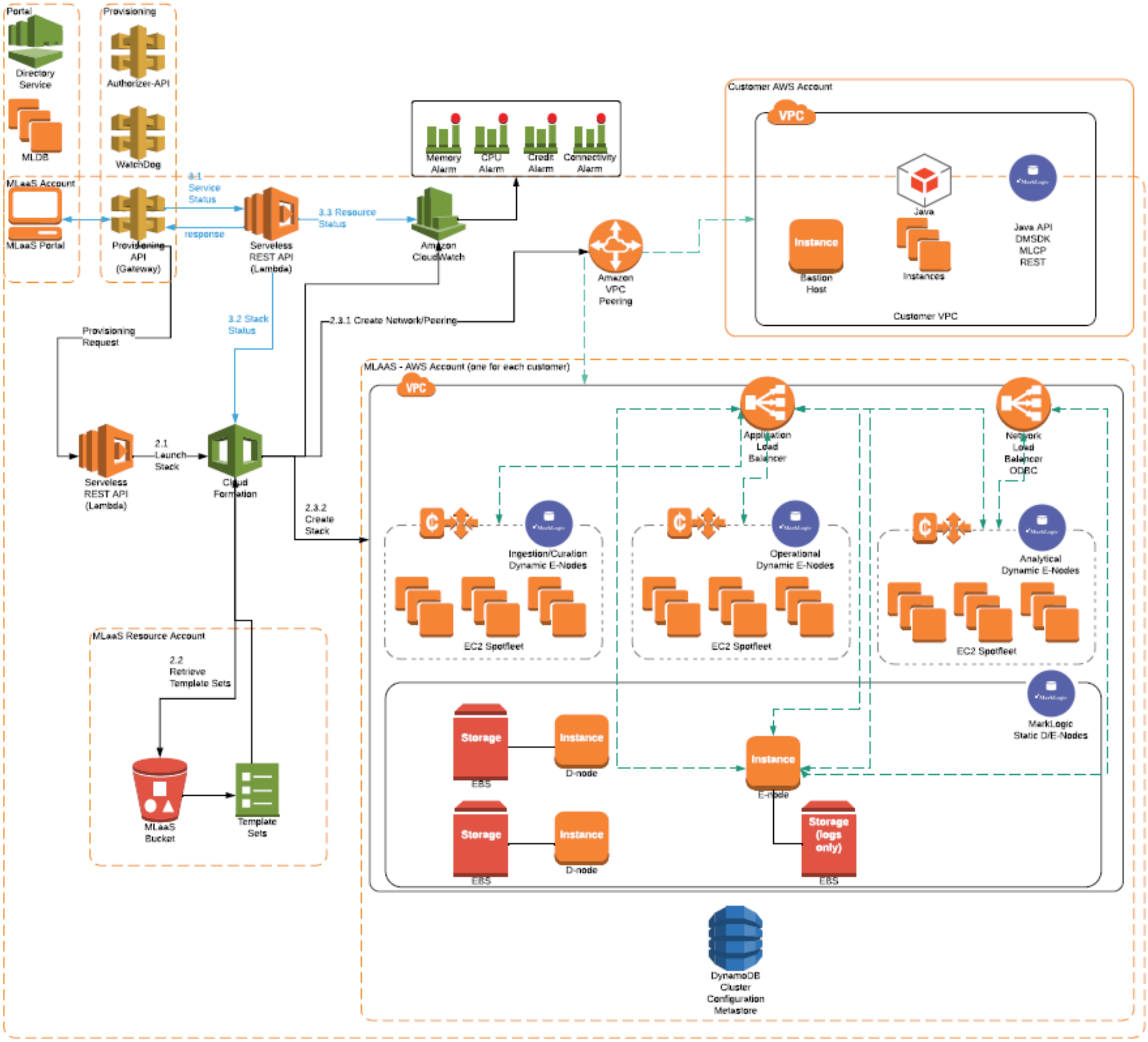
The Data Hub Service PaaS offers a complete Platform on AWS for customers to implement their applications on the MarkLogic database.

MarkLogic Data Hub Service is a fully automated cloud service to integrate data from silos. Based on the MarkLogic Data Hub, the service enables agile teams to immediately start integrating and curating data for both operational and analytical use. Delivered as a cloud service, it provides on-demand capacity, auto-scaling, automated database operations, and proven enterprise data security. Unlike other cloud services, however, it's cost-effective and predictable even as enterprise workloads fluctuate.

Some of the services offered are:

- Infrastructure implementation and management
- OS patch management
- Managed backups
- Managed Intrusion Protection System (IPS)
- Managed load balancing
- Individual VPC's per customer

System Overview Illustration



Infrastructure

The Data Hub Service PaaS is hosted in AWS IaaS where each customer has a dedicated instance of the service in their own VPC.

MarkLogic Development and Operations employees access the service environment via a Web Browser.

Data communications between MarkLogic facilities are encrypted with Cisco virtual private networking (VPN) technology using Advanced Encryption Standard 256-bit encryption to protect intra-company communications.

Software

The MarkLogic Data Hub Service is a fully automated cloud service to integrate data from silos. Based on the MarkLogic Data Hub, the service enables agile teams to immediately start integrating and curating data for both operational and analytical use. Delivered as a cloud service, it provides on-demand capacity, auto-scaling, automated database operations, and proven enterprise data security. Unlike other cloud services, however, it's cost-effective and predictable even as enterprise workloads fluctuate.

Some of the key features of the Data Hub Service are:

- **Automated Scalability:** MarkLogic Data Hub Service has the ability to auto-scale with user defined limits and thresholds. MarkLogic scales to meet demand — quickly, transparently, and automatically provisioning nodes as needed. The unique architecture does not require customers to migrate data, re-partition, re-balance, or repeat other operations required by other databases when scaling up.
- **Automated Upgrades:** MarkLogic Data Hub Service automates both installation and upgrades. This means no waiting or planning for downtime, whether for a small patch or a more significant release.
- **Automated Backups:** Backups are critical, but a chore. Automating backups removes the hassle and ensures the safety of customer data at all times.
- **Guaranteed Availability:** MarkLogic Data Hub Service is designed to meet high performance SLAs.
- **Secure By Default:** Effortlessly protects sensitive data. MarkLogic Data Hub Service automates security setup and provides end-to-end encryption for optimal data security and shareability.

The Data Hub Service is developed and maintained by MarkLogic's in-house software engineering group. The software engineering group enhances and maintains the Data Hub Service to provide service for the company's various customers. The Data Hub Service is available commercially on the AWS marketplace.

The Data Hub Service is a Platform as a Service built upon the MarkLogic NoSQL database in which the application's data is processed and stored. The information can be retrieved, reviewed, and reported as needed.

The MarkLogic Data Hub Service is accessible via the Service Portal application.

People

MarkLogic has a staff of approximately 350 employees organized in the following functional areas:

Corporate. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance and human resources.

Dev-Ops. Staff that administers the support and maintenance of the Data Hub Service.

Customer service representatives support the DHS to troubleshoot issues opened by customers via email or the web ticketing system.

Software Engineers design and develop the code for deployment of the Data Hub Service. A systems administrator will deploy the releases of the Data Hub Service and other software into the production environment.

Quality assurance tests the Data Hub Service for defects prior to each release.

IT. Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom.

The help desk group provides technical assistance to MarkLogic users.

The infrastructure, networking, and systems administration staff typically has no direct use of the Data Hub Service. Rather, it supports MarkLogic's IT infrastructure.

The software development staff develops and maintains the custom software for MarkLogic. This includes the Data Hub Service, supporting utilities, and the external websites that interact with the Data Hub Service. The staff includes software developers, database administration, software quality assurance, and technical writers.

The information security staff supports the Data Hub Service indirectly by monitoring internal and external security threats and maintaining current antivirus software.

The information security staff maintains the inventory of IT assets.

IT operations manage the user interfaces for the Data Hub Service. This includes processing user entity–supplied membership and eligibility files, producing encounter claims files, and other user-oriented data (capitation files, error reports, remittance advice, and so on).

IT staff maintain the voice communications environment, provide user support to MarkLogic, and resolve communication problems. This group does not directly use the

Data Hub Service, but it provides infrastructure support as well as disaster recovery assistance.

Data

Data, as defined by MarkLogic, constitutes the following:

- Employee Data
- Server logs
- BOD meeting minutes
- Contracts
- Engineering specifications
- Employment verification and background check records
- Financial records
- Intellectual Property Records
- Litigation Records
- Sales & Marketing records
- Personnel Files
- Policies and Procedures
- Stock Records
- System files
- Error logs

Processes and Procedures

MarkLogic communicates its policies and procedures to all employees annually. All relevant policies and procedures are available for review on the company's internal Wiki. MarkLogic policies and procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)
- Vendor Management

Attachment B – MarkLogic Corporation's Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

MarkLogic designs its processes and procedures in order to meet its objectives for its Data Hub Service (DHS). Those objectives are based on the service commitments that MarkLogic makes to user entities, the laws and regulations that govern the provision of DHS, and the financial, operational, and compliance requirements that MarkLogic has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the Data Hub Service that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role

Use of encryption technologies to protect customer data both at rest and in transit

MarkLogic establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in MarkLogic's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach on how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Data Hub Service.