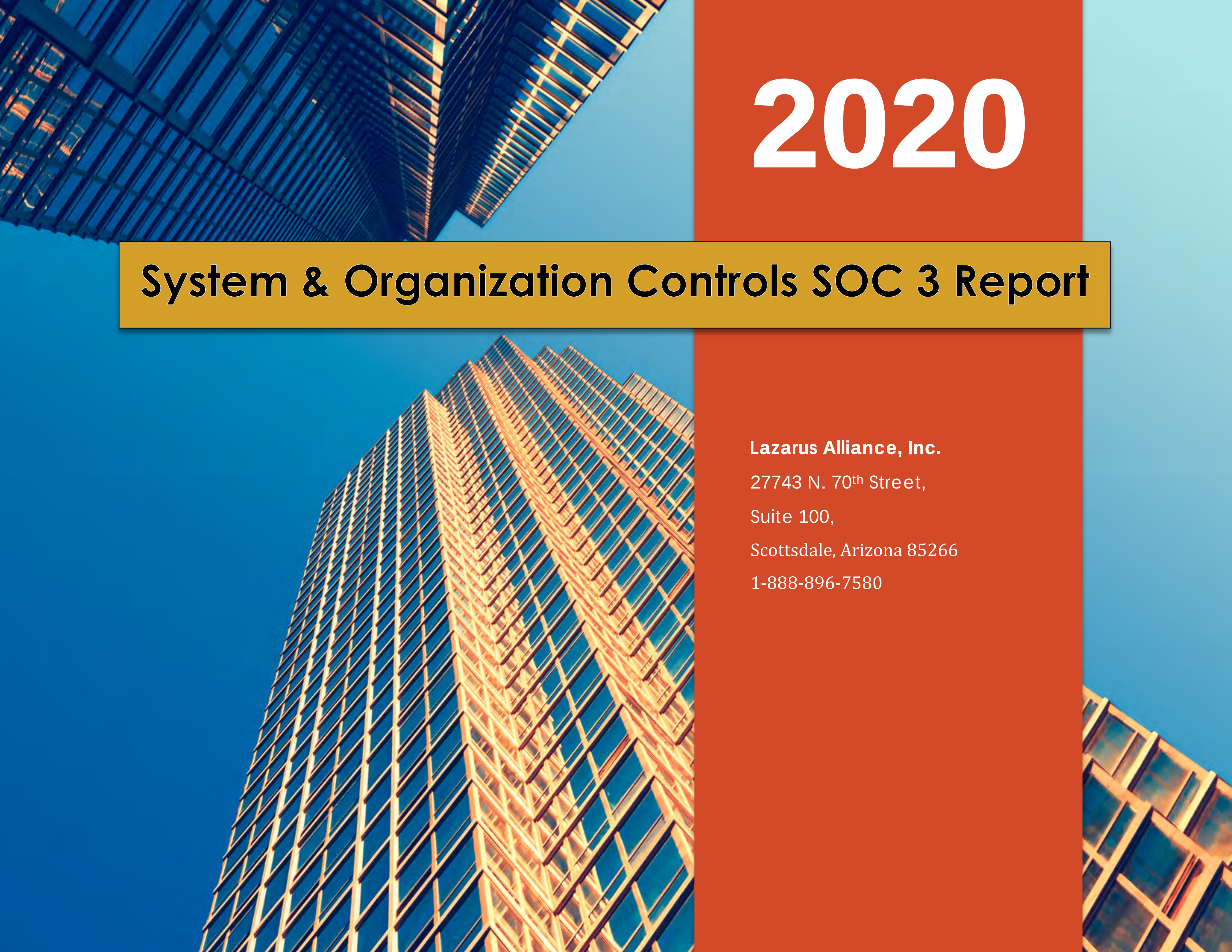


2020

System & Organization Controls SOC 3 Report

Lazarus Alliance, Inc.

27743 N. 70th Street,

Suite 100,

Scottsdale, Arizona 85266

1-888-896-7580

08-07-2020

REPORT ON COMPANY'S DESCRIPTION OF ITS BUSINESS PLATFORM SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, PRIVACY, AVAILABILITY, INTEGRITY AND CONFIDENTIALITY

MarkLogic Corporation

Assessment Dates: 10-01-2019 - 06-07-2020

Table of Contents

Section 1 - Assertion of Company's Service Organization Management

08-07-2020

Assertion of MarkLogic Corporation Service Organization Management

We have prepared the accompanying description in section 3 titled "MarkLogic Corporation's Service Organization's Description of its Data Hub Platform as a Service (PaaS) throughout the period June 7, 2019, through June 8, 2020" (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 MarkLogic users with information about the Data Hub PaaS platform that may be useful when assessing the risks arising from interactions with MarkLogic Service Organization's (MarkLogic) system, particularly information about system controls that MarkLogic 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 (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).

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

a. The description presents MarkLogic's Data Hub Service PaaS platform that was designed and implemented throughout the period June 7, 2019, through June 8, 2020, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period June 7, 2019, through June 8, 2020, to provide reasonable assurance that MarkLogic.'s service commitments and system requirements would be achieved based on the applicable trust service criteria, if its controls operated effectively throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2019, until June 7, 2020, to provide reasonable assurance that MarkLogic's service commitments and system requirements were achieved based on the applicable trust service criteria.

We have prepared the accompanying description in section 3 titled "MarkLogic Corporation Service Organization's Description of Its service application system throughout the period June 7, 2019, through June 8, 2020, (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 service application system that may be useful when assessing the risks arising from interactions with MarkLogic Corporation Service Organization's (MarkLogic Corporation's) system, particularly information about system controls that MarkLogic Corporation 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 (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).

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

- the description presents MarkLogic Corporation's service application system that was designed and implemented throughout the period June 7, 2019, through June 8, 2020, in accordance with the description criteria.

- the controls stated in the description were suitably designed throughout the period June 7, 2019, through June 8, 2020, to provide reasonable assurance that MarkLogic Corporation's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

- the controls stated in the description operated effectively throughout the period June 7, 2019, through June 8, 2020, to provide reasonable assurance that MarkLogic Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria.

Section 2 - Independent Service Auditor's Report

Independent Service Auditor's Report

To: *MarkLogic Corporation* Service Organization

Scope

We have examined MarkLogic Corporation's (“"MarkLogic", the “Company” or the “Service Organization”) description of its Platform as a Service (PaaS) offering throughout the period from June 7, 2019, through June 8, 2020 (the “Description”) based on the criteria for a description of a service organization’s system set forth in DC Section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 ® Report (“description criteria”) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period from June 7, 2019, through June 8, 2020 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.

MarkLogic uses Amazon Web Services (AWS) Infrastructure as a Service (IaaS) platform for clients’ hosted production infrastructure and backup services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description presents MarkLogic system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain appliable trust services criteria. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

MarkLogic has provided an assertion about the fair presentation of the description and the suitability of the design of the controls to achieve the related control objectives stated in the description. MarkLogic is responsible for preparing the description and for its assertion, including the completeness, accuracy and method of presentation of the description and the assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives, selecting the criteria and designing, implementing and documenting controls to achieve the related control objectives stated in the description.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination 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, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description of the assessment period. An examination of a description of a service organization's system and the suitability of the design of the service organization's controls to achieve the related control objectives stated in the description involves the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed and operating effectively to achieve the related control objectives stated in the description. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Management's assertion in this report. 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 system and the suitability of the design and operating effectiveness of those controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that the Description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.

- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.

- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- Evaluating the overall presentation of the Description.

Inherent Limitations

The Description is prepared to meet the common needs of abroad range of report users and may not, therefore, include every aspect of the system that induvial 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 always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls reviewed are listed in section titled Control Objectives and Related Controls.

Opinion

In our opinion, in all material respects,

a. The description presents the system that was designed and implemented throughout the period June 7, 2019, through June 8, 2020 in accordance with the description criteria

b. The controls stated in the Description were suitably designed throughout the period June 7, 2019, through June 8, 2020 to provide reasonable assurance that MarkLogic's service commitments and system requirements would be achieved based upon the applicable trust services criteria, if the controls operated effectively throughout that period and subservice organization and user entities applied the complementary user entity controls assumed in the design of MarkLogic Corporation controls throughout that period.

c. The controls stated in the Description operated effectively throughout the period June 7, 2019, through June 8, 2020 to provide reasonable assurance that MarkLogic's service commitments and system requirements were achieved based on the appliable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of MarkLogic's controls operated effectively throughout that period.

Restricted Use

This report and the description of tests of controls and results thereof are intended solely for the information and use of MarkLogic Corporation user entities of MarkLogic's Data Hub Platform as a Service (PaaS) during some or all of the period June 7, 2019, through June 8, 2020; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, or other parties.
- Internal control and its limitations.
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.

- The applicable trust services criteria.

- The risks that may threaten the achievement of the applicable trust services criteria 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. This report and the description of the suitability of the design and operating effectiveness of controls in this report are intended solely for the information and use of MarkLogic's Data Hub Platform as a Service (PaaS) for the assessment period and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about the controls implemented by user entities themselves, when assessing the risks and regulatory compliance of non-financial reporting controls. This report is not intended to be and should not be used by anyone other than those specified parties.

Sincerely,

Lazarus Alliance Compliance, LLC

Section 3 - Service Organization's Description of Its Business Platform System

MarkLogic Corporation’s Assertion

This report on the internal controls placed in operation is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of MarkLogic Corporation's controls that may be relevant to a user organization’s internal control structure. This report, when combined with an understanding of the policies and procedures at user organizations, is intended to assist user auditors in planning the audit of the user organization and in assessing control risk for assertions that may be affected by policies and procedures of MarkLogic.’s Data Hub Service PaaS platform. This report describes the system and control structure of MarkLogic Corporation as it relates to it's Data Hub Service PaaS platform. It is intended to assist MarkLogic customers and its independent auditors in determining the adequacy of the internal controls that are outsourced to MarkLogic Corporation and are relevant to customers’ internal control structures as it relates to regulatory compliance risks. This document was prepared in accordance with the guidance contained in the American Institute of Certified Public Accountants AT-101 Service Organization Control (SOC) 2 control framework. This description is intended to focus on the internal control structure of MarkLogic Corporation that is relevant to its Data Hub Service PaaS platform customers only and does not encompass all aspects of the services provided or procedures followed by MarkLogic Corporation.

Management representative,

Jim Clark

VP - Engineering

06-07-2020

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:

o Infrastructure implementation and management

o OS patch management

o Managed backups

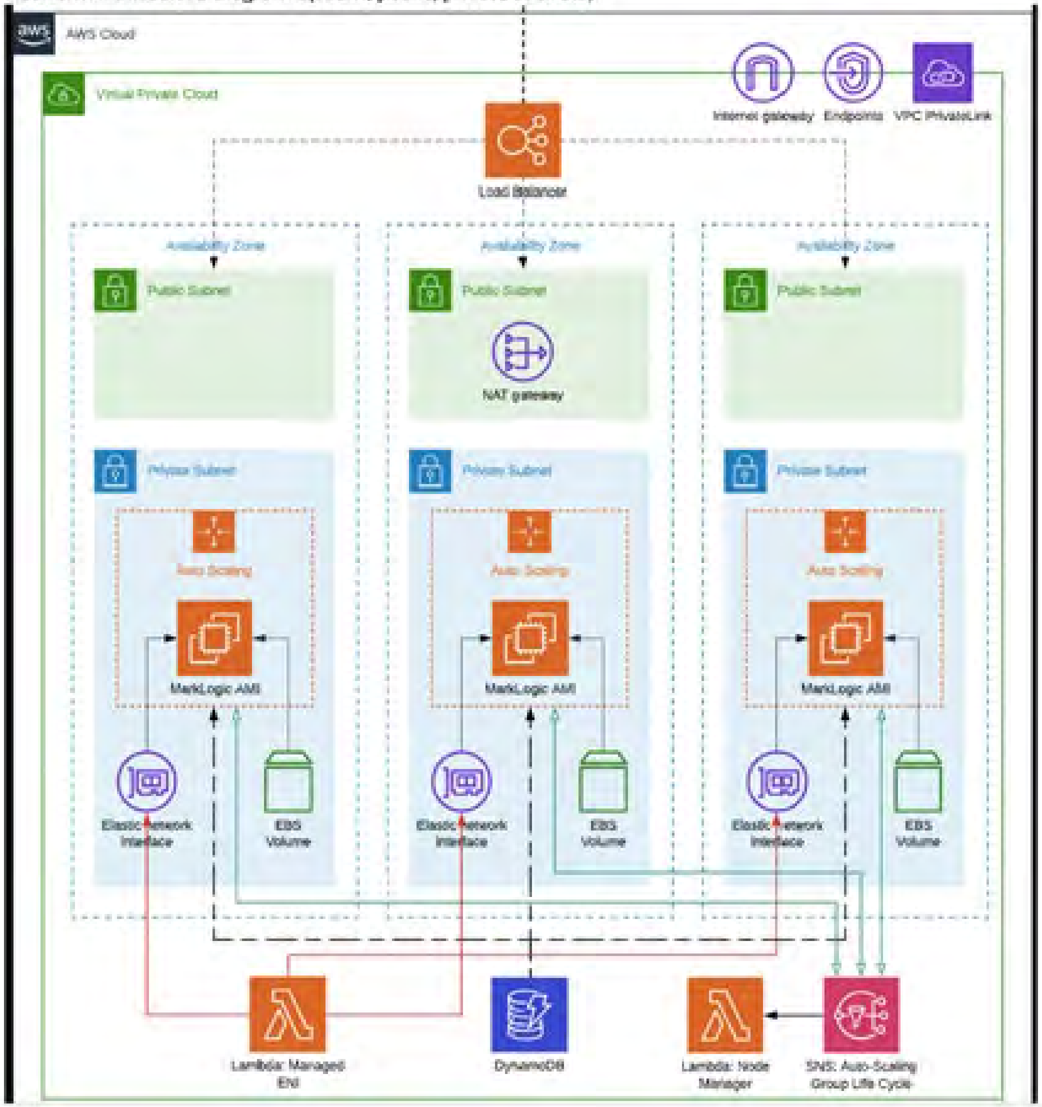
o Managed Intrusion Protection System (IPS)

o Managed load balancing

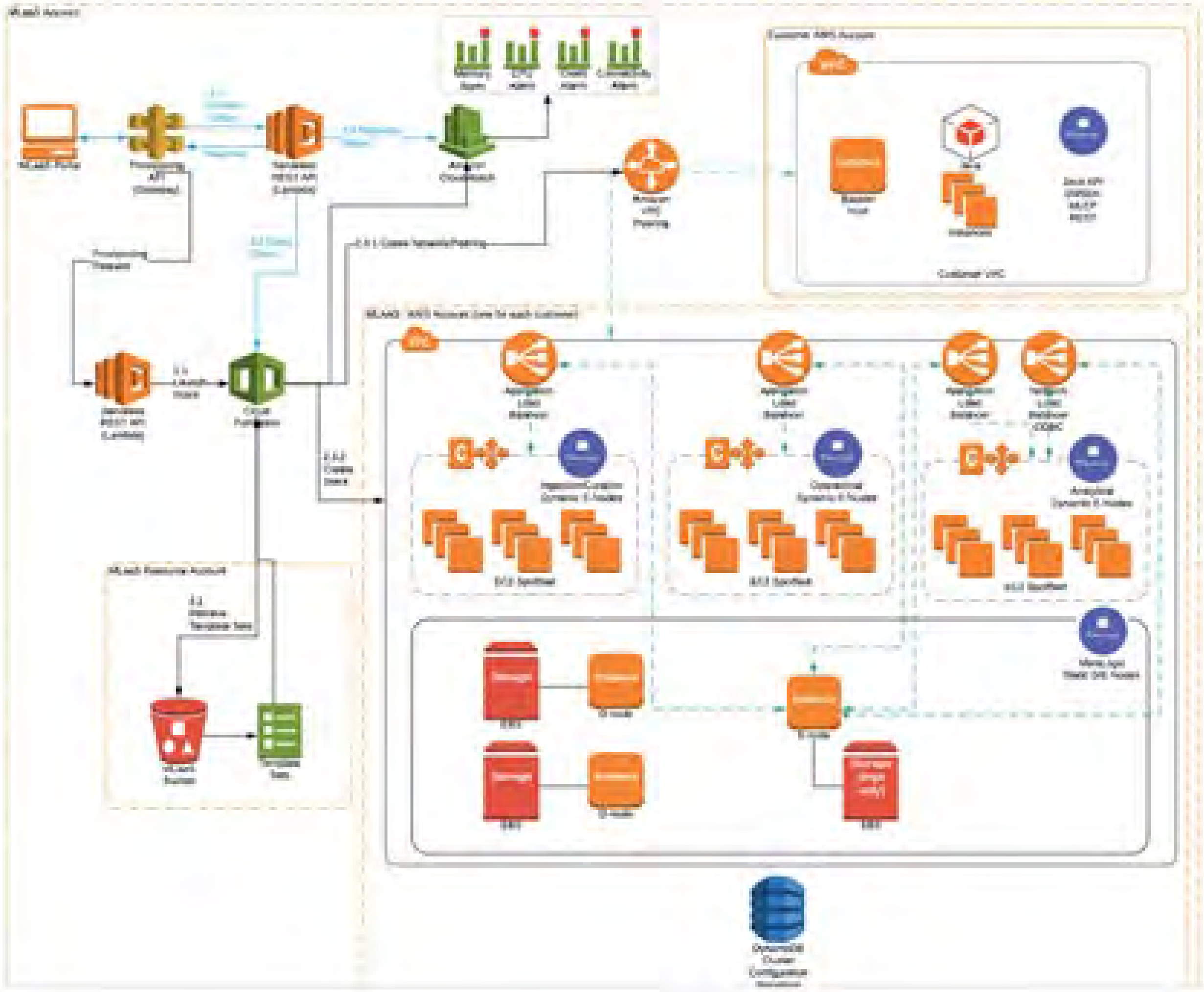
o Individual VPC's per customer

System Overview Illustration

Network Architecture Diagram 2(zoom, public/private subnets):



Network Architecture Diagram 1:



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.

Components of the System Used to Provide the Services

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 fetuare of the Data Hub Service are:

- **Automated Scalability** — MarkLogic Data Hub Service is unmatched in the ability to auto-scale. User define 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 and provides 99.95% availability.
- **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.

MarkLogic has a staff of approximately 500 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 on the MarkLogic Infrastructure, Servers and other computers.
- 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 comapny'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)

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

Control Environment

Management's Philosophy and Operating Style

MarkLogic's control environment reflects the philosophy of senior management concerning the importance of security of data and information. MarkLogic's Audit Committee meets quarterly and reports to the board annually. The committee, under the direction of the MarkLogic board, oversees the security activities of MarkLogic. The committee is charged with establishing overall security policies and procedures for MarkLogic. The importance of security is emphasized within MarkLogic through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, MarkLogic has taken into consideration the relevance of controls to meet the relevant trust criteria.

Security Management

MarkLogic has a dedicated information security team consisting of a security officer and a senior security specialist responsible for management of information security throughout the organization. They maintain security credentials and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing MarkLogic's information security policies. The information security policy is reviewed annually by the security officer, CFO, and other members of the Executive Management staff.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies.

Security Policies

The following security policies and related processes are in place:

- Data classification and business impact assessment
- Selection, documentation, and implementation of security controls
- Assessment of security controls
- User access authorization and provisioning
- Removal of user access
- Monitoring of security controls
- Security management
- Records Retention and Destruction
- Security Breach Incident Response
- Change Management
- Physical and Remote Access

Personnel Security

Background checks are performed on new information security employees, who are also required to review and acknowledge their receipt of relevant security policies. The new positions are supported by job descriptions. Once employed, employees are subject to MarkLogic's procedures for accessing systems and sanctions for violating MarkLogic’s information security policy. Employees are instructed to report potential security incidents to the help desk.

MarkLogic's business associate agreement instructs employees to notify the IT department if they become aware of a possible security breach.

Physical Security and Environmental Controls

The Data Hub Service runs in exclusively in AWS IaaS. All physical and envronmental controls are inherited from AWS.

Change Management

MarkLogic has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The IT management team meets on a regular basis to review and schedule changes to the IT environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, most developers do not have the ability to migrate changes into production environments. However some leads who are responsible for deploying code into production have the ability to make changes to the code when required.

MarkLogic has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

MarkLogic uses a standardized build checklist to help secure its servers, and it conducts monthly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with MarkLogic's patch management process.

System Monitoring

The security administration team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed daily by the security administration team using a security incident and event monitoring custom solution.

Security events requiring further investigation are tracked using a help desk ticket and monitored until resolved

Problem Management

Security incidents and other IT-related problems are reported to the help desk. Issues are tracked using a help desk ticket and monitored until resolved.

Data Backup and Recovery

The MarkLogic Data Hub Service backs up each customer's data to a dedicated S3 bucket in AWS. Access to backups is restricted to authorized personnel.

System Account Management

MarkLogic has implemented role-based security to limit and control access to the Service Portal and to each instance of the Data Hub Service. Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel.

The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

The human resources department provides IT personnel with an employee termination notification when an employee is terminated. IT reconciles the termination notice with current access privileges to determine if access has been appropriately removed or disabled.

Administrative access to Active Directory, Unix, and other applications is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users, as well as to the facility services. Password parameters consist of the following:

- Passwords contain a minimum of eight characters, including one non-alphanumeric character.
- Passwords expire every 90 days for privileged and non-privileged accounts.
- Privileged and non-privileged users cannot reuse the last five passwords.

Risk Assessment Process

MarkLogic regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security based on the applicable trust services criteria set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information security team assesses security risks on an ongoing basis. This is done through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.

An IT strategic plan is developed annually and is communicated to and approved by senior management and the Security Steering Committee. As part of this plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed.

Senior management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on MarkLogic's security policies.

Changes in security threats and risks are reviewed by MarkLogic, and updates to existing control activities and information security policies are performed as necessary.

Information and Communication Systems

MarkLogic has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

Monitoring Controls

In addition to the daily oversight, monthly vulnerability assessments, and use of automated InfoSec alert monitoring, management provides further security monitoring through the internal audit department, which performs periodic audits to include information security assessments.

Complimentary User Entity Controls

MarkLogic Data Hub Service controls were designed with assumption that certain controls would be implemented by user entities. In certain situations, the application of specific control at user entities is necessary to achieve certain criteria included in this report. The following complimentary user entity control considerations should not be regarded as comprehensive list of all controls that should be employed by user entities. There may be additional controls at the user entities that would be appropriate for the processing of client transactions that are not identified in this report. User entities are responsible for implementing such controls.

- Access to MarkLogic Data Hub Service is restricted to authorized and appropriate personnel (CC6.2, CC6.3)

- Credentials and passwords for accessing MarkLogic Data Hub Service are maintained, protected, and restricted to authorized parties (CC6.2, CC6.3)

- User entities are responsible for designating and maintaining administrators for the Company portal to manage the creation, access, and removal of their authorized users (CC1.3, CC5.2)

- Firewalls and other logical access controls are monitored and managed by user entity personnel (CC7.1, CC7.2, CC6.6)

- Incidents and complaints are escalated and communicated to the MarkLogic team via support portal for investigation (CC7.3, CC7.4, CC7.5)

- User organizations sending data to MarkLogic Data Hub Service, data should be protected by appropriate methods to ensure confidentially, privacy, integrity, availability and non-repudiation (CC6.1, CC6.6, CC6.7)

- User entities are responsible for adhering to the terms and conditions stated within their contracts with MarkLogic (CC2.3)