CORALOGIX

CORALOGIX LOG ANALYTICS SOLUTION

SERVICE ORGANIZATION CONTROL (SOC) 2 REPORT TYPE 2

REPORT ON CONTROLS RELEVANT TO SECURITY AND AVALIABLITY OF THE LOG ANALYTICS SOLUTION

FOR THE PERIOD
August 1, 2018 THROUGH July 31, 2019

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of
Coralogix
Menachem Begin 42 Tel Aviv

Scope

We have examined **Coralogix** accompanying description of **its Log analytics solution** throughout the period **August 1, 2018 to July 31, 2019**, 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) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period **August 1, 2018 to July 31, 2019,** to provide reasonable assurance that **Coralogix**'s service commitments and system requirements were achieved based on the trust services criteria relevant to **security and availability** *(applicable trust services criteria) se*t forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Trust Services Criteria).*

Coralogix uses **Subservice Organization** to host Coralogix's equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at **Coralogix**, to achieve **Coralogix**'s service commitments and system requirements based on the applicable trust services criteria. The description presents **Coralogix**'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of **Coralogix**'s controls. The description does not disclose the actual controls at the subservice organization(s). Our examination did not include the services provided by the subservice organization(s), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Coralogix 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 **Coralogix**'s service commitments and system requirements were achieved. **Coralogix** has provided the accompanying assertion, titled "Assertion of **Coralogix** Management" (assertion), about the description and the suitability of design and operating effectiveness of controls stated therein. **Coralogix** is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section IV.

Basis for Qualified Opinion

Our examination of suitability of the design and operating effectiveness of the service organization's controls included obtaining sufficient and appropriate evidence in order to provide a reasonable basis for our opinion. We obtained partial evidence of controls regarding formal approvals of system changes before migrating them into production environment.

Opinion

In our opinion, except for the matter described in the preceding paragraph, in all material respects,

a. the description presents **Coralogix**'s **Log analytics solution** that was designed and implemented throughout the period **August 1, 2018 to July 31, 2019** in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period **August 1, 2018 to July 31, 2019** to provide reasonable assurance that **Coralogix**'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of **Coralogix**, user entities of **Coralogix**'s **Log analytics solution** during some or all of the period **August 1, 2018 to July 31, 2019**, business partners of **Coralogix** subject to risks arising from interactions with the **Log analytics solution**, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Ziv Haft
Certified Public Accountants (Isr.)
BDO Member Form

12/08/19

II. CORALOGIX'S ASSERTION

Coralogix's Management Assertion Regarding Coralogix Log Analytics Solution regarding the Period from **August 1, 2018 to July 31, 2019**.

We have prepared the accompanying description of **Coralogix**'s (**"Coralogix"** or the "service organization") **Log analytics solution** "**Coralogix**'s **Description of its Log analytics solution"** throughout the period **August 1, 2018 to July 31, 2019** ("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 **Log analytics solution** that may be useful when assessing the risks arising from interactions with **Coralogix**'s **system**, particularly information about system controls that **Coralogix** has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to **security and availability** (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, (*AICPA, *Trust Services Criteria)*.

Coralogix uses **AWS**, a subservice organization to provide **cloud services**. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at **Coralogix**, to achieve **Coralogix**'s service commitments and system requirements based on the applicable trust services criteria. The description presents **Coralogix's** controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of **Coralogix**'s controls. The description does not extend to the actual controls at the subservice organization.

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

a. the description presents **Coralogix**'s **Log analytics solution** that was designed and implemented throughout the period **August 1, 2018 to July 31, 2019**, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period **August 1, 2018 to July 31, 2019** to provide reasonable assurance that **Coralogix**'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively through-out that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of **Coralogix**'s controls throughout that period.

c. The controls stated in the description operated effectively throughout the period **August 1, 2018 to July 31, 2019** to provide reasonable assurance that **Coralogix**'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of **CORALOGIX**'s controls operated effectively throughout that period.

CORALOGIX
Ariel Assaraf
Coralogix, INC.
EIN No. 82-5384825
(Date) 12/08/2019

III. DESCRIPTION OF THE SYSTEM

Company Overview

Coralogix is a DevOps enabler that aims to drastically improve continuous delivery & enhances production maintenance.

Using machine learning algorithms, Coralogix helps businesses reduce issue resolution time, increase system uptime, improve customer satisfaction and decrease maintenance costs.

Coralogix provides a SaaS platform that connects to any software system, gathers the emitted data and sends it to its cloud, once there, Coralogix learns the normal behavior of the system and maps the business flows of the application in an automated manner.

After a short learning period, Coralogix is able to shrink millions of semi structured raw data into a small, manageable & structured set, detect breakages within the business flows of the application and find actionable solutions to these issues.

Cloud environments and Open Source software have lowered the bar for anyone to implement software solutions. However, as software becomes more complex and at scale, the task of monitoring it is becoming increasingly difficult to manage.

Complex relationships between system components are frequently missed by the human eye, and small but important changes are neglected. This, along with the sheer amount of monitoring data, call for a new approach.

System Overview and Background

Coralogix is a SaaS analytics platform that utilizes machine learning algorithms to map the inner flows of any app and detect production malfunctions.

By using Coralogix, companies can perform continuous delivery without compromising software quality or stability.

Building a solution for these complex problems requires unique engineering of machine learning algorithms: smart enough to understand the deep app flows reflected by log records on the one hand, and lightweight enough to handle Big Data – the analysis of billions of log records generated every day.

Coralogix's capabilities include:

Loggregation:
Automatic clustering of log data back into its original patterns allows our users to view a narrow set of records instead of millions, dive into a single pattern's behavior, or drill into the different log variables in a single click.

Flow anomaly detection:
Coralogix maps the software flows and baseline behavior, automatically detects production problems and delivers pinpoint insights

Version tags:
'Tags' allows users to integrate their software build tools into Coralogix so that they can get Coralogix's insights in context of their new versions.

Alerts to email or Slack:
Real-time notifications on Activity / Inactivity to any email or Slack room.

Dashboard widgets
Coralogix allows the creation of dashboard widgets and statistical views for maximum control over the log data

Log query
Coralogix provides a powerful log query according to any condition and timeframe.

Real time Live tail
Application live tail from multiple machines and environments at once with the ability to filter it in real time to isolate the events.

A hosted Kibana

Coralogix provides a fully hosted Kibana for dashboards and data slicing tasks.

Various integrations

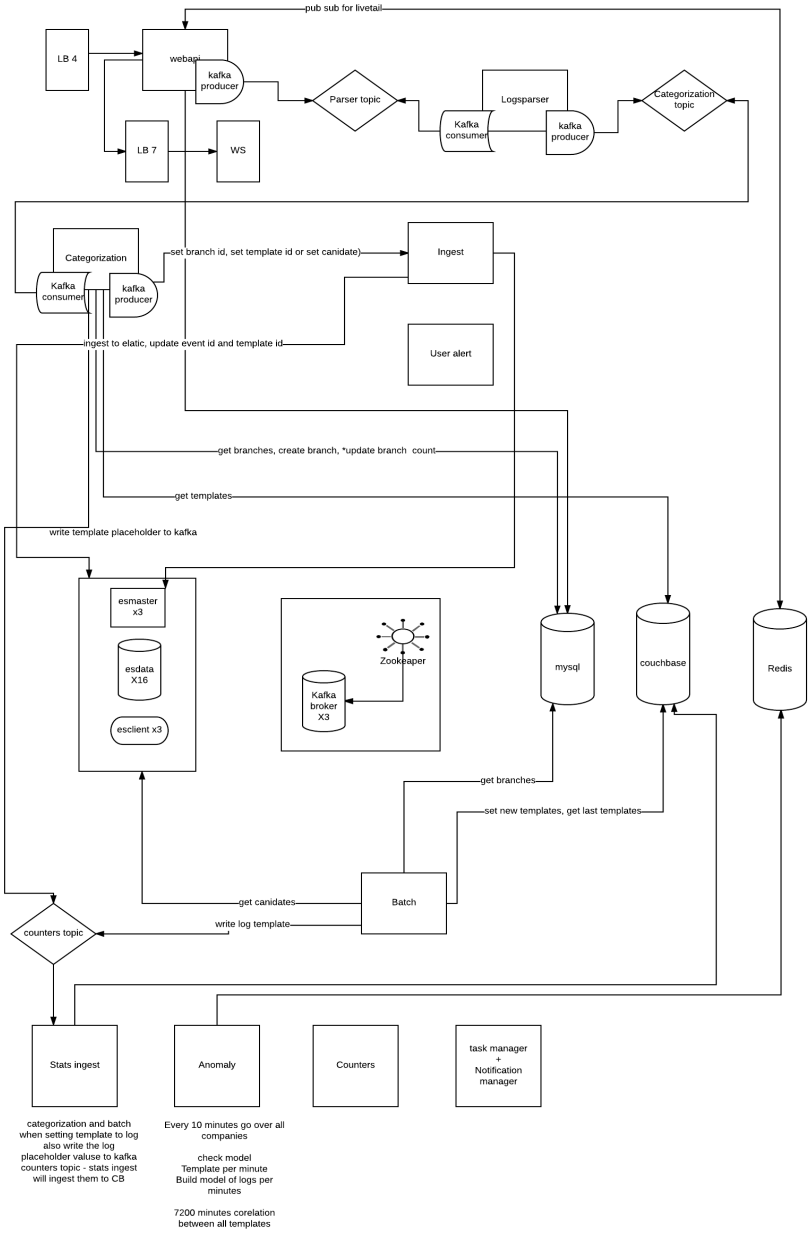
Coralogix supports all major coding languages with a log collection SDK, along with standard logging platforms and file reading agents.

Components of the System Providing Services

Infrastructure

Coralogix runs entirely on AWS virtual machines.

The topology of the setup is detailed below:



Software

Coralogix is using the following OSS technologies as part of its infrastructure:

- Apache Kafka – An OSS distributed persistent queue for large scale environments.
- Elasticsearch – An OSS indexing platform for storing and querying text data.
- Redis – A distributed caching system for storing short term statistics.
- Couchbase – NoSQL key value database for storing long term models and statistics.
- Celery – Task scheduler for controlling offline processes.
- Rabbitmq – Distributed queuing system for celery.

Coralogix's algorithms are proprietary and were written entirely by the company.

People

CEO- General company management and periodic risk assessment

CPO- Feature and roadmap definition and version release management

CTO- Managing the engineering team and assessing new technologies and tech risks

Chief data scientist – Responsible for data and access management, granting permissions to sensitive components, evaluating and selecting big data technologies.

Procedures

Coralogix has a written data security policy regarding to the following matters:

- The company's security layers.
- Wireless security.
- Remote access.
- Responding to security events.
- Passwords.
- Risk assessments.
- Backup and Recovery.
- - User Management.
- Physical server security (relying on AWS SOC2 compliance).

Furthermore, Coralogix has a written Version of Change Management Procedure, specifying the required procedure in case of version upgrades/bug fixes. Any version upgrade needs to be performed according to this procedure.

Organizational Structure

Coralogix's organizational structure defines roles & responsibilities,reporting lines, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security and availability.

Employees

Coralogix takes the following measures regarding hiring new employees:

- As part of the hiring process, Coralogix's CTO, CPO, Chief Data Scientist and CEO interview new employees both personally and professionally.
- The screening process includes professional verbal tests and home assignments.
- All employees are trained in the field of expertise, and have a vast experience of at least 8 years in their field.
- Each new employee is required to provide two references from their previous job.
- Every employee at Coralogix is signed on a detailed contract in which his job responsibilities, direct reporting lines and obligations are specified.
- Each employee gets a detailed description of his roles and responsibility during his hiring process and it is defined in his contract.
- Granting access to new employees is made according to the requirements of the CEO, who is responsible for finalizing the hiring process.

Furthermore, Coralogix takes the following measures regarding to maintaining its human resources:

- Employees are being evaluated on a quarterly basis by the CTO, while the CTO himself is being evaluated by the CEO on a monthly basis.

- Coralogix employees have an open account at online tech universities where they can acquire professional knowledge in various areas.
- Coralogix has a detailed technical overview document, which every employee is obliged to review and be tested on.

When an employee leaves the company, all of their access keys and permissions are terminated on the day of their departure.

Information and communication:

- The company provides 18/7 support on its in-app/on-site customer communication platform
- The company available at info@coralogix.com
- The company's SLA is detailed on its public website under "Terms and conditions".
- The company provides up-to-date technical tutorials and integration tutorials in its website.
- Once a user signs up to Coralogix's services, he receives an authentication email which is required to activate the account. In addition, the newly signed up user receives an email specifying the Coralogix representative who will assist him.
- Every new user can schedule a 1:1 online demo with the company's technical department.
- The company informs its customers on new features on a monthly basis on its newsletter.

Technical Support Problem Severity Levels

For support, customers may reach out to Coralogix via our in-app/website chat.

Problem Severity Level1:

1) Description: This Problem Severity Level is associated with: (a) Services, as a whole, are non-functional or are not accessible; (b) unauthorized exposure of all of part of Subscriber Data; or, (c) loss or corruption of all or part of Subscriber Data.
2) Request Response Time: 30 minutes.
3) Request Resolution Time: 2 hours.

Problem Severity Level2:

1) Description: This Problem Severity Level is associated with significant and / or ongoing interruption of an Authorized User's use of a critical function (as determined by the Authorized User) of the Services and for which no acceptable (as determined by the Authorized User) work-around is available.
2) Request Response Time: 1 hour.
3) Request Resolution Time: 4 hours.

Problem Severity Level3:

1) Description: This Problem Severity Level is associated with: (a) minor and / or limited interruption of an Authorized User's use of a non-critical function (as determined by the Authorized User) of the Services; or, (b) problems which are not included in Problem Severity Levels 1 or 2.
2) Request Response Time: 8 hours.
3) Request Resolution Time: 24 hours.

Problem Severity Level 4:

1) Description: This Problem Severity Level is associated with: (a) general questions pertaining to the Services; or, (b) problems which are not included in Problem Severity Levels 1, 2, or 3.
2) Request Response Time: 8 hours.
3) Request Resolution Time: 48 hours.

Customization / Integration Services. The provider is not committed to provide any Customization / Integration Services.

Training Services. The provider is not committed to provide any training Services.

Business continuity plan:

Coralogix is reliant on AWS's infrastructure for its data and availability.

In case of disaster to AWS, the company will be able to be back online within 24 hours on another cloud service, without guarantee of the previous data availability.

Data

- Coralogix stores software log data, whether from proprietary applications, OSS applications used on customers environments, or server logs.
- All the data is sent and stored on AWS.
- All the databases and indexes are backed up daily for disaster recovery.
- The backup procedure is tested once a year on the production identical staging environment, to the data indexes as well as the SQL databases.

Subservice Organizations and other parties:

AWS: Virtual machines, used for our infrastructure compute and storage.

Supplemental Controls over Subservice

AWS SOC2 report is enclosed. The company's CPO assess its compliance and its impact on the company annually.

Risk Assessment

Coralogix has a weekly CTO/CEO risk management meeting in which they assess the possible risks, analyze them and build a mitigation plan for each risk.

Once a risk is identified, the company CTO is responsible to break it down into tasks in order to mitigate the risk.

Control activities:

Coralogix performs periodic performance and security risk assessment meetings in order to evaluate the upcoming challenges and make sure that the company's procedures are followed.

Information systems

Coralogix uses AWS's virtual machines running on Linux operating system. These systems are used to:

1) Store the customers' log data in indexes ready for querying.
2) Analyze the customers' data structure and alert on anomalies.
3) Monitor the data and alert on predefined rules created by the customer.

The data sent to Coralogix contains free text inserted into the code as a log print by the customers engineering team. We recommend not to include confidential or sensitive data and provide tools to eliminate such data.

Coralogix is responsible for the data security and availability and takes measures to assure them, such as:

1) Data replications for disaster recovery
2) Persistent queues for data storing during network problems
3) Coralogix's web platform is completely cached on Cloudflare so that if the application is down, users can still use the system regularly using Cloudflare's "Always online" feature.
4) Parsing engine for sensitive log data cleanup rules by the customer
5) Limited access to the data center, using a private key allocated per developer and only to developers who are mandatory to access the system.
6) Data can be accessed either from the secured Coralogix UI or via our SSL API which requires a private key connection.
7) The entire system is hidden behind Cloudflare which protects it from DDos attacks.
8) Each personal computer in the company is protected by an anti virus program.
9) The company performs a bi-annual security check, performed by a full stack developer fully dedicated to network and software security.
10) Coralogix handles security threats received from "Cloudflare" or AWS as top priority by a dedicated developer reporting to the company's CEO.

Coralogix’s servers are hosted with AWS and rely on their physical protection layer.

Monitoring & Control environment:

- The company is performing periodic penetration tests, so far with no major findings, and makes sure that all found breaches are fixed.
- The company receives security alerts from AWS and acts in order to mitigate them.
- The company has created its own monitoring tool which samples the system and notifies on degradation in performance.
- The company records its entire log data and saves it for a period of 14 days.
- The company monitors the data flow stability & integrity as part of a 24/7 automation process.
- Coralogix has a 24/7 domain communication monitoring with real time alerts in case that there are communication issues to the domain from any geographical area.
- The company uses Cloudflare to identify the numbers of suspicious IP's accessing the system and be notified whether there is an abnormal activity.
- The company decides on production upgrades according to the performed tests.
- Each one of the R&D, is notified by email on every new code push.
- Every deployment of a new code has to be authorized by the CTO and accompanied by him.

Operations

- The company runs a monthly sprint meeting with the company CTO, CPO, and CEO in order to evaluate the past sprint's performance and plan the next release.
- Each version in Coralogix is tested on a local environment for a few days, then moved to a staging environment which is identical to the production environment and tested for load , security and functionality.

User Complementary Controls

Coralogix's controls were designed with the assumption that certain controls are in operation within the user entity organizations. This section describes those controls that should be in operation at user entity organizations to complement the controls of Coralogix.

The following list contains controls Coralogix assumes its user entities have implemented. User organization auditors should determine whether the user entities have established sufficient controls in these areas:

1) Customer are responsible to define strong passwords and periodically replace them.
2) Customers are responsible to send access invites only to certified people in the organization, give them appropriate permissions and delete their users when they leave the company.
3) Customers are responsible to clean their logs of highly confidential data such as credit card numbers, ID's and contact information.

IV. APPLICABLE TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Information Provided by the Service Auditor

This report is intended to provide information to the management of **Coralogix**, user entities of its **Log analytics solution**, and prospective user entities, independent auditors and practitioners providing services to those entities, who have a sufficient understanding to consider it, along with other information including information about the controls implemented by the user entity. This report is intended to provide information about the suitability of the design and operating effectiveness of the controls implemented to achieve the service commitments and system requirements based on the criteria relevant to the **security and availability** set forth in TSP section 100, 2017, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("AICPA, *Trust Services Criteria*") ("applicable trust services criteria"), throughout the period **August 1, 2018 to July 31, 2019**

Although the applicable trust services criteria and related controls, and management responses to deviations, if any, are presented in this section, they are an integral part of **Coralogix**'s description of its **Log analytics solution** throughout the period **August 1, 2018 to July 31, 2019**.

The examination was performed in accordance with the criteria set forth in DC section 200, 2018 *Description Criteria for a Description of the Service Organization's System in a SOC 2® Report*. It is each user entity's responsibility to evaluate this information in relation to the internal control structure in place at each user entity in order to assess the total internal control structure. If an effective internal control structure is not in place at user entities, the **Coralogix** controls may not compensate for such weaknesses.

This description is intended to focus on **Coralogix**'s controls surrounding the **Log analytics solution** throughout the period **August 1, 2018 to July 31, 2019, 20XX**; it does not encompass all aspects of the services provided or controls performed by **Coralogix**. Unique processes or control situations not described in the report are outside the scope of this report.

Tests of Controls

Our examination of the description of the service organization's **Log analytics solution** and the suitability of the design and operating effectiveness of the controls to achieve the related service commitments and system requirements based on the services criteria stated in the description involved performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design and operating effectiveness of those controls to achieve the related service commitments and system requirements based on the services criteria 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 or operating effectively to achieve the related service commitments and system requirements based on the services stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related service commitments and system requirements based on the services criteria stated in the description were achieved throughout the period **August 1, 2018 to July 31, 2019**

Our tests of controls were designed to cover a representative number of activities throughout the period **August 1, 2018 to July 31, 2019**, for each of the controls listed in section IV, which are designed to achieve the related service commitments and system requirements based on the services specified control criteria. In selecting particular tests of controls, we considered: (a) the nature of the controls being tested, (b) the types and competence of available evidential matter, (c) the criteria to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

BDO ISRAEL testing of controls was restricted to the controls specified by **Coralogix** in section IV, and was not extended to controls in effect at user locations or other controls which were not documented as tested under each control criteria listed in section IV. The description of BDO USA, LLP's tests of controls and results of those tests are presented in this section of the report. The description of the tests of controls and the results of those tests are the responsibility of BDO USA, LLP and should be considered information provided by BDO USA, LLP.

Types of testing methods include:

Type	Description
Inquiry	Made inquiries of appropriate personnel and corroborated responses with management.
Observation	Observed the application, performance, or existence of the specific control(s) as represented by management.
Inspection	Inspected documents and records indicating performance of the control.
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation.

Information Provided by the Entity

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Controls Mapped to the Security & Availability Principles and Criterion

Security Principle: The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.

Availability Principle: The system is available for operation and use to meet the entity's commitments and system requirements.

TSC Ref. #	Criteria	Control Activity
	CONTROL ENVIRONMENT	
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CORAL2 CORAL3 CORAL4 CORAL5
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CORAL1 CORAL2
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CORAL3 CORAL4
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CORAL4 CORAL6 CORAL7 CORAL9
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CORAL3 CORAL4 CORAL10
	COMMUNICATION AND INFORMATION	
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CORAL13 CORAL14 CORAL15 CORAL16
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CORAL16 CORAL17 CORAL18 CORAL66

TSC Ref. #	Criteria	Control Activity
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CORAl16 CORAL19 CORAL20 CORAL21 CORAL22 CORAL66
	RISK ASSESSMENT	
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CORAL25 CORAL26
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CORAL26
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CORAL27 CORAL66
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CORAL28
	MONITORING ACTIVITIES	
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CORAL29 CORAL30 CORAL31 CORAL32 CORAL65
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	CORAL31
	CONTROL ACTIVITIES	

TSC Ref. #	Criteria	Control Activity
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CORAL33 CORAL34
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CORAL35 CORAL36 CORAL37 CORAL38
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CORAL4 CORAL34 CORAL39 CORAL40
	LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CORAL42 CORAL43 CORAL44 CORAL45 CORAL46 CORAL47
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CORAL48
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CORAL37 CORAL49 CORAL50 CORAL51
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities,	CORAL69

TSC Ref. #	Criteria	Control Activity
	back-up media storage, and other sensitive locations) to Authorized personnel to meet the entity's objectives.	
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives	CORAL69
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CORAL52
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CORAL53 CORAL54
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives	CORAL55
	SYSTEM OPERATIONS	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CORAL47 CORAL56
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	CORAL57 CORAL58
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CORAL31 CORAL32

TSC Ref. #	Criteria	Control Activity
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CORAL32 CORAL59 CORAL60 CORAL65
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	CORAL31
	CHANGE MANAGEMENT	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CORAL61
	RISK MITIGATION	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CORAL26 CORAL62
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	CORAL26 CORAL69
	ADDITIONAL CRITERIA FOR AVAILABILITY	
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	CORAL65 CORAL66
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	CORAL63 CORAL65 CORAL67 CORAL68
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	CORAL64

Security & Availability Principles and Criterion Mapped to Coralogix Controls & Auditor Testing Performed and Results

Security Principle: The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.

Availability Principle: The system is available for operation and use to meet the entity's commitments and system requirements.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL1	The board will be formed in an independent manner from management.	Inspected the board members and the process of forming it to verify his independents from management.	CC1.2	No exceptions noted.
CORAL2	The board congregate minimum twice in a year to set policies, that ensure ethical behavior, secure customers' data, and to enforce these policies.	Observed a sample of board meetings minutes regarding setting policies and ensuring ethical behavior. Observed companies' code of ethics signed by management.	CC1.1 CC1.2	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL3	The company organizational structure defines roles, responsibilities and reporting lines in aspects of design, development, implementation, operation, maintenance and monitoring of the system, enabling it to meet its commitments and requirements as they relate to security and availability.	Obtained the company's organizational chart which includes roles and reporting hierarchy.	CC1.1, CC1.3, CC1.5	No exceptions noted.
CORAL4	Each employee gets a detailed description of his role and responsibility during his hiring process and it is stated in his contract, the contract include term of probation, suspension, and termination as potential sanctions for employee misconduct. On a long term contractors sign a Confidentiality agreement as well as an Information Technology Acceptable Use Acknowledgement upon employment signifying that they have read, understand, and will follow applicable policies and procedures.	Inquired the CPO about the company's hiring process in order to ensure new employees get a detailed description of their role and responsibility. Observed a sample of a hiring contract inspected that the employees detailed description of their role and job responsibilities are specified.	CC1.1, CC1.3, CC1.5, CC1.4, CC5.3	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL5	The company Data Classification Policy establishes an information security classification schema that describes the security labeling and handling of Confidential Information.	Inspected the company Data Classification Policy to determine it established an information security classification schema.	CC1.1	No exceptions noted.
CORAL6	As part of the hiring process, each candidate is interviewed both personally and professionally by the Coralogix CTO, CPO, and CIO. Key employees (CTO, VP's) are also interviewed by 2 board members at least for external reference. All employees are trained in the area of their expertise, and have a vast experience of at least 2 years in their field.	Inquired the CEO regarding the hiring process. each candidate is interviewed both personally and professionally by the Coralogix CTO, CPO or CIO	CC1.4	Exceptions noted. No Documentation found for candidates interviews.
CORAL7	As part of the hiring process, each candidate is tested on both verbal tests and home assignments.	Inquired the CIO regarding candidates sorting process and he declared that the sorting process include a professional verbal tests and home assignments. Inspected home assignment which designate for new candidates.	CC1.4	Exceptions noted. No Documentation found for candidates home assignments.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL8	Coralogix has a detailed technical overview document, which every Coralogix employee is obliged to go over.	Inquired the CIO regarding employee's technical document overview. Every employee gets review of the products and relevant technical details.		Exceptions noted. No Documentation found for employees technical overview.
CORAL9	New Employees and long term contractors sign a Confidentiality Agreement upon employment signifying that they have read, understand, and will follow applicable policies and procedures.	Observed a sample of contract which contains a Confidentiality Agreement.	CC1.4	No exceptions noted.
CORAL10	Employees are evaluated on a weekly basis by the CTO, In these evaluations the employees get feedback both on their professional performance as well as on their performance.	Observed a sample of employee evaluations. Professional assessment is done on a weekly basis. And a social band once a quarter.	CC1.5	No exceptions noted.
CORAL11	Confidentiality policy changes are informed to the Company's customers, by email or the company's website.	No Confidentiality policy changes were during the period the report.	C1.6	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL12	The company has a documented data retention policy that documents the requirements for retaining confidential information. Confidential information is removed from company's environment in accordance with the data retention policy.	Obtained Business Continuity Plan policy, signed by the management. Obtained documentation for data retention derail the company preformed.	C1.7	No exceptions noted.
CORAL13	The company's SLA is detailed on the company's website on "Terms & Conditions" section.	Inspected the company's SLA "Terms & Conditions" section on the website in order to ensure it comprises the company's SLA. Obtained a sample of correspondences between the company's representatives and customers about technical support problems and found the response and resolution time complies with the described in the company's SLA.	CC2.1	No exceptions noted.
CORAL14	As part of the development process, the company preform weekly meetings to manage the priority and risk management of the developments.	Inspected a sample of summaries from scrum meeting which determine on the e priority and risk management of the developments.	CC2.1	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL15	Firewall is in place to control network traffic and prevent unauthorized traffic from passing between the cloud and external networks.	Inspected firewall settings are in place, and verified that only the CIO is able to change settings.	CC2.1	No exceptions noted.
CORAL16	The Company has classified its data into the following data types in the responsibility of AWS: 1. Public 2. Internal 3. Confidential 4. Restricted 5. Customer Data	Inspected the Coralogix Overall Security Policy and verified the company had classified its data into different types. observed folders restrictions for each classified data and verified it is restricted only to necessary personnel.	CC2.1, CC2.2, CC2.3, CC2.6	No exceptions noted.
CORAL17	The company has both written and video tutorials of the product features and implementations that are published at the company's website.	Inspected both the written and video tutorials that are featured on the company's website.	cc2.2	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL18	The company employees have to review the study material according to a professional document that is provided to them. And to complete tasks in order to acquire the necessary knowledge in the company.	Obtained a screenshot from Udemy website which shows the courses that the employees studied.	CC2.2	Exceptions noted There is no personal monitoring of employee training if required
CORAL19	Employees are required to attend security awareness training upon hire and annually thereafter.	Obtained Security training kit. Training was not performed yet	CC2.3	exceptions noted: Training was not performed yet
CORAL20	Every new user can schedule a 1:1 online demo with one of the company's technical team members. Throughout the online demo, the technician notifies the users regarding their commitments and responsibilities.	Observed an example of email sent to new users when they are first signed in, hence ensuring that they are aware of the possibility to schedule an 1:1 online demo with one of the company's technical team members.	CC2.3	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL21	Internal and external users are informed of relevant incidents as defined in the Security Incident Management Policy.	Inspected the Security Incident Management policy to determine it defined procedures on reporting incidents to internal and external users.	CC2.3	No exceptions noted.
CORAL22	Master service agreements are in place to communicate the security, availability and confidentiality responsibilities and commitments with clients and vendors.	Inspected the master service agreement in place with a sample of client and vendors to determine the security, availability and confidentiality responsibilities and commitments were communicated to clients and vendors.	CC2.3	No exceptions noted.
CORAL23	The Incident Management Policy is posted on company's drive and available to entity internal users on how to report, assess and respond to incidents.	Inspected company's policy and procedure repository on Coralogix's drive to determine the Incident Management Policy was available to internal users. Inspected the Incident Management Policy to determine it contained documentation on how to report, assess and respond to incidents.	CC2.5	No exceptions noted.
CORAL24	All changes in new releases are published in a release notes on the company's support website. Any upgrade/change activity is coordinated with the relevant customers. System changes that may	Observed the Coralogix's Support website and confirmed that changes in new releases are published in a release notes.	CC2.6	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
	affect customers are communicated to clients via email.			
CORAL25	Coralogix has a weekly CTO/CEO risk management meeting where they assess the possible risks, analyze them and build a mitigation plan for each risk.	obtained and inspected a sample of weekly risk management meetings summaries, including the risks that have been brought up and their relevant mitigations	CC3.1	No exceptions noted.
CORAL26	The company perform an annual risk assessment in order to identify and evaluates the risks that threaten its commitments and requirements as they relate to security and availability. Mitigation strategies are implemented, as needed, based on identified risks.	Obtained an annual risk assessment report reviewed by the management, and includes remediation strategies as needed.	CC3.1	No exceptions noted.
CORAL27	During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.	Observed the annual business planning and budgeting and verified it contains Planning versus execution process.	CC3.3	No exceptions noted.
CORAL28	The company decides on production upgrades according to the performed tests' results.	Obtained documentation of preformed tests for sample of code changes and inspected the changes done and approved before the release to production environment.	CC3.4	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL29	Coralogix monitors the data flow stability & integrity automatically by using Elasticsearch Cluster Monitor which sends data every minute in order to track data flow delays.	Inspected an example of an alert and verified that the automatic emails alert were sent to the relevant personnel. Obtained and reviewed the system's code for sending the SDK PILL every minute and the defined factors to receive alerts via email when needed. In addition, obtained screenshots of the queue system showing how many messages are queued and indicates if the queue is not shortened, as a result of delays in the data flow. If a queue gets longer than a certain standard, the system alerts by means of a backlog.	CC4.1	No exceptions noted.
CORAL30	Each version in the company is tested on a test environment, then moved to a staging environment, and pushed to the production environment automatically.	Perform test of releasing new change to the production environment, and verify that all steps are automated and mandatory.	CC4.1	No exceptions noted.
CORAL31	An intrusion prevention system is in place to monitor for malicious and unauthorized activity and alerts are sent to management when incidents are identified.	The company uses Security Union for monitoring malicious and unauthorized activity. Observed the monitoring rolls and the interface with Grafana system in order to send alerts if necessary.	CC4.1, CC4.2	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL32	the company performs an overview of security and IT incidents meetings to investigated and resolve the incidents in a timely manner.	Inspected reports for a sample of Coralogix'S management review meetings of security and IT incidents, verified that all critical issues are resolved in a timely manner.	CC4.1,CC7.4	No exceptions noted.
CORAL33	Mobile devices that have access to company resources are configured with passwords according to the defined password security standards. The company has the ability to remotely wipe mobile devices with access to company resources.	Inspected the password strength and security standard to determine users were required to have passwords enabled on mobile devices that have access to company resources.	CC5.1	No exceptions noted.
CORAL34	Internal users authenticate to the applications, databases, and operating systems with unique user IDs.	Inspected user IDs for the applications, databases, and operating systems to determine unique user IDs were assigned to users.	CC5.1, CC5.3	No exceptions noted.
CORAL35	Terminated employees access is disabled by system administrators within three business days of the employee's last day.	Inspected termination notifications for a selection of terminated employees to determine accounts were disabled within three business days of the employee's last day.	CC5.2	No exceptions noted.
CORAL36	A deployment of a new code is documented and approved.	Obtained a sample of code changes deployed into the production environment Verified each change documented and approved.	CC5.2	Exceptions noted. The company doesn't link between the Jira documentation and the specific change pused to the git, therefore, the test could not verify all

Number	Control	Test Performed 2019	Criteria	Test Result
				changes are documented.
CORAL37	New user access to the company systems is documented and approved by management prior to the user obtaining access.	Inspected emails which document the access of new users to the system.	CC5.2, CC6.3	No exceptions noted.
CORAL38	The company uses its own log management platform (the company system) to collect and analyze our log data and be notified on broken flows or predefined alerts.	Obtained a screenshot of Coralogix's log management platform which is being used to collect and analyze their log data and be notified if there are broken flows or predefined alerts.	CC5.2,	No exceptions noted.
CORAL39	The company has a written Version Change Management procedure, specifying the required procedure in case of version upgrades/bug fixes. Any version upgrade must be performed according to the procedure.	Obtained the company's Version Change Management procedure, verified it refers to the following matters: - Version upgrade cycle, including performing tests on a separate environment prior to deploying new codes into production. - Urgent code fixes. - Deploying new codes/bug fixes into production by the relevant developer in the presence of the company's CTO.	CC5.3	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL40	Prior migration of a new code push to production, each R&D member is notified by email.	Inspected emails which notified to the R&D team regarding codes before transferred to production	CC5.3	No exceptions noted.
CORAL41	Antivirus is installed on workstations and cloud servers to monitor for viruses and malicious software.	Inspected the Web Root dashboard to determine anti-virus was installed on workstations and servers	CC5.8,CC5.6	No exceptions noted.
CORAL42	All data is sent to Coralogix by HTTPS.	Inquired the CPO and observed the company's URL and API method to ensure all data is being sent to Coralogix securely by HTTPS.	CC6.1	No exceptions noted.
CORAL43	Customer's emails are authenticated with a unique number identifier in every signup.	Observed the registration process of new customers and noticed that within the registration process an authentication email is sent to the customer.	CC6.1	No exceptions noted.
CORAL44	Penetration tests have been performed via an external consultant, and found no critical issues.	Obtained documentation of a penetration test's results from August 2018. Inspected the results, their severities and suggested remedies for every issue, if needed.	CC6.1	No exceptions noted.
CORAL45	Backups are monitored for successful completion by management. If a backup fails in two consecutive occurrences, a ticket is created to track the issue to completion.	Inspected the configurations from the monitoring tool to determine it was configured to generate alerts when a failed backup was detected.	CC6.1	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL46	The technology team holds a weekly meeting to review security, availability, and confidentiality incidents and system changes for remediation.	Inspected a sample of mitting summery of the technology team for a selection of weeks, to determine the technology team held meetings on a weekly basis to review security, availability, and confidentiality incidents and system changes for remediation.	CC6.1	No exceptions noted.
CORAL47	Access and the ability to make changes to production is limited to CIO only.	Inspected The Permissions for production and development groups and confirmed that there is no overlap between the two groups.	CC6.1,CC7.1	No exceptions noted.
CORAL48	Once a user signs up, he gets an email specifying the Coralogix representative who will be supporting him. For support, customers may reach out to Coralogix via company's in-app/website chat.	Observed an example of email sent to new users when they are signed in, thus ensuring that they are notified regarding the representative whom will be supporting them. Observed the company's website in order to ensure the company has in-app/website chat for customer support.	CC6.2	No exceptions noted.
CORAL49	Privileged access to backend servers and databases, confidential resources and administrator accounts is restricted to CIO.	Inspected a screenshot of the Admin group and found that only the CIO is recognized as the admin. The admin has full Permissions to the dev and production.	CC6.3	No exceptions noted.
CORAL50	Every new employee gets access according to his job position. Access is granted by the company's CIO.	Reviewed all permissions groups and that in each group only the members of the group have access to their environment.	CC6.3	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL51	Coralogix allows password recovery by email.	Obtained documentation of password recovery process by email.	CC6.3	No exceptions noted.
CORAL52	Clients access our UI via Cloud flare in order to not expose the company's server IPs	Obtained a screenshot showing that pinging to Coralogix's server returns Cloud flare's IP address.	CC6.6	No exceptions noted.
CORAL53	Entity policies prohibit the transmission of restricted and confidential information over the Internet or other public communications paths unless it is encrypted.	Inspected the Data Protection Standard to determine that Coralogix prohibited the transmission of restricted and confidential information over the Internet or other public communications paths unless it was encrypted.	CC6.7	No exceptions noted.
CORAL54	The backups are performed by AWS and in their responsibility. The company connect with AWS to obtain the backup and encryption service.	Inspected A document that detail the service of AWS, prior to the connecting between the company's.	CC6.7	No exceptions noted.
CORAL55	The company customers send their data to the company using a secured SSL connection and a private data-sending key generated to each customer by the company. Information transmitted by web based applications is protected through the use of TLS encryption.	Inspected a report of quality's that constantly monitors and checks the SSL in the report you can see that they support TLS.	CC6.8	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL56	The company uses Cloud flare to identify the number of suspicious IP's accessing the system and be notified whether there is an abnormal activity. The entire system is hidden behind "Cloud flare" which protects the company from Dodos attacks.	Obtained screenshots from Cloud flare showing suspicious IP's access tracking. Inquired the company's CPO and he declared there were no abnormal activities during the audit period that required any special actions to be taken. Inspected DNS and DDOS services The service is fully handled by Cloud flare.	CC7.1	No exceptions noted.
CORAL57	The company uses a incident monitoring AWS service, the Incidents are forwarded to the company and are handled by the relevant cause. In case of critical incident the pagerDuty is been activate.	Obtained an alert sent from the pagerDuty and managed by the relevant authority.	CC7.2	No exceptions noted.
CORAL58	Coralogix has a 24/7 domain communication monitoring system with real time alerts. Up time monitoring is published to all customers in the coralogix website, and contains incident report in a case of incident.	Inspected a system called PagerDuty. The system is used to manage alerts and notify the relevant authority. Observed the up time monitoring published to all customers in the coralogix website, and verified it contains incident report.	CC7.2	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL59	Prior changes implementation in the prod environment, automation tests are performed.	Obtained scrip of automation tests performed prior the release to the production environment Inspected the automate process of release changes to production environment and verified unit and automate tests are mandatory.	CC7.4	No exceptions noted.
CORAL60	Code changes must be reviewed by a peer programmer who is not responsible for the change.	obtained a sample of Code changes, for each change inspected, The code was reviewed by a peer programmer.	CC7.4	No exceptions noted.
CORAL61	The company runs a monthly sprint meeting with the company CTO, CPO, and CEO in order to evaluate the past sprint's performance and plan the next release.	Obtained a sample of sprint meeting summaries. The meetings are conducted in a computerized meeting management tool that shared with all relevant users.	CC8.1	No exceptions noted.
CORAL62	The company has a written data security policy which s Policy, which regards to the following matters: - company's security layers. - Wireless security. - Remote access. - Responding to security events. - Passwords. - Risk assessments. - Backup and Recovery. - User Management.	Obtained and inspected the company's Data Security Policy, which regards to the following matters and has been signed by the CEO.	CC9.1	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL63	All the databases and indexes are backed up daily for disaster recovery.	Obtained documentation of the backup definition and found all the databases and indexes are backed up daily. In addition, obtained documentation of storing backups on a separated storage.	A1.2	No exceptions noted.
CORAL64	The data indexes and SQL databases backup procedure is tested once a year in the production identical staging environment.	A report was received documenting the SQL check made in January. And shows a low level of risk.	A1.3	No exceptions noted.
CORAL65	All changes in new releases are published in a release notes on support website. Any upgrade/change activity is coordinated with the relevant customers. System changes that may affect customers are communicated to clients via email.	Obtained a sample of an email which sent to the customer about all changes in new releases.	A1.1, A1.2, CC2.6, CC4.1, CC7.4	No exceptions noted.
CORAL66	There is a precise policy for answering the customer. Plus instructions for action.	Obtained a sample of correspondence between a client and the support team. Until the incident was resolved.	A1.1, CC2.2, CC2.3, CC2.5, CC3.3	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL67	In order not to lose information the company uses a queue system called Kafka which backs up the information in the queue. If there is a fault, the information can be recovered from the application.	Obtained a screenshot which shows the monitoring of the backups.	A1.2	No exceptions noted.
CORAL68	All the log data stored in Coralogix's servers is replicated into wo complete replications, thus allowing our index servers to be redundant to servers in availability.	There is a use in elastic search product is used, the product replicates information and saves it to two servers for backup and continuous operation of the system.	A1.2	No exceptions noted.

Number	Control	Test Performed 2019	Criteria	Test Result
CORAL69	The CIO analyze SOC 2 type 2 reports from sub service organizations, Mitigation strategies are implemented, as needed, based on identified exceptions.	Observed the AWS SOC2 type 2 report and confirmed it was analyzed by the CIO.	CC9.2	No exceptions noted.

--- End of Report ---