

Electronic Application Management System

SOC 2 Type 1

February 2020



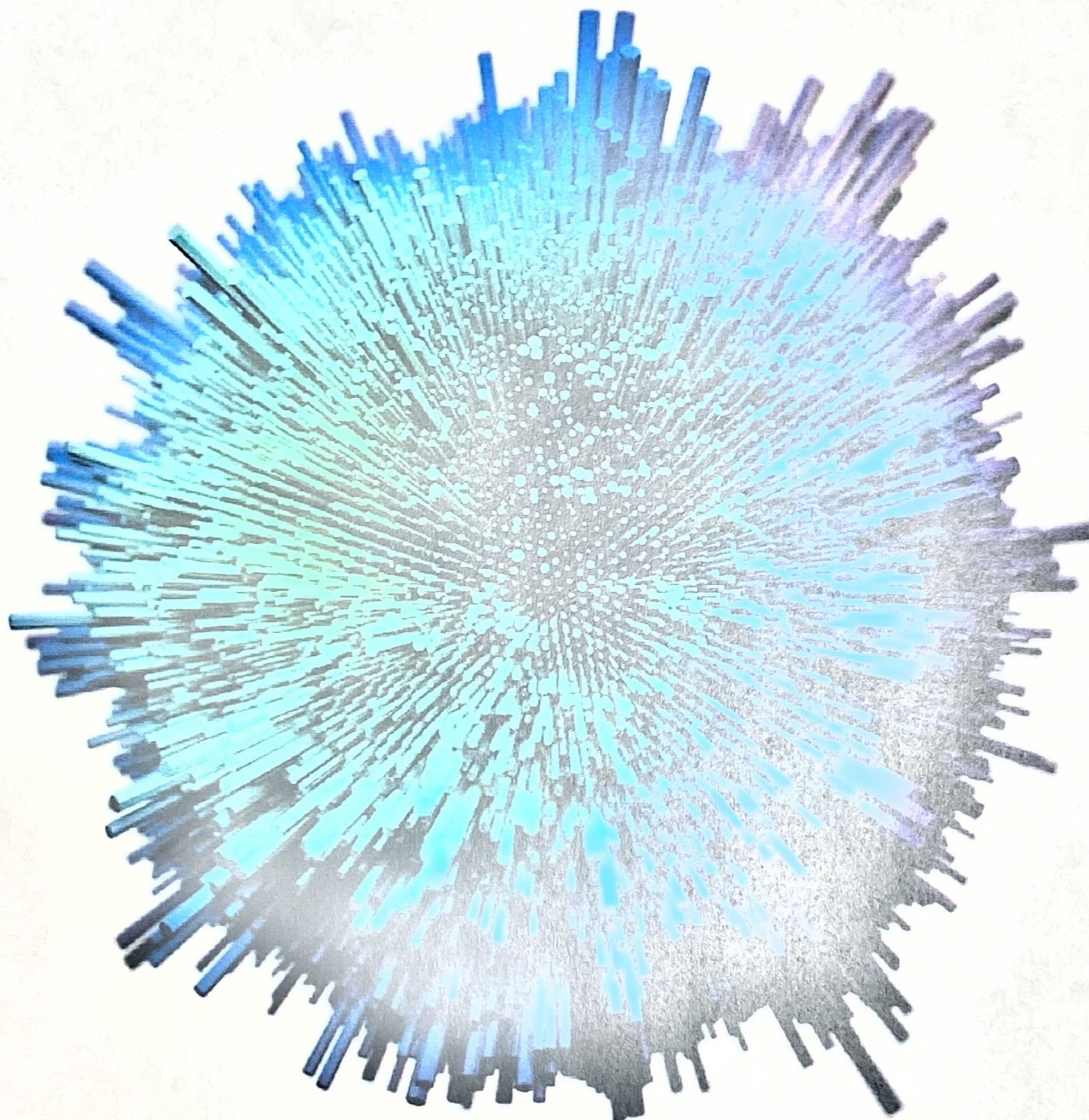
Deloitte.

Issued to:



AZARIŞIQ
AÇIQ SƏHMDAR CƏMİYYƏTİ

Deloitte.



JSC "Azerishiq"

Electronic Application Management System

Report on Controls at System and Organization
Relevant to Security

February 2020

Contents

Glossary	3
Introduction	5
Executive Summary.....	6
Procedures performed by Independent Service Auditor	7

Glossary

Acronym	Description
AICPA	American Institute of Certified Public Accountants
COSO	Committee of Sponsoring Organizations of the Treadway Commission
SLA	Service Level Agreement
ASAN	State agency for public services to citizens of Azerbaijan
Firewall	Network security system that monitors and controls incoming and outgoing network traffic
IPS	Intrusion Prevention System, an automated network security device used to monitor and respond to potential threats
GUI	Graphical User Interface
URL	Uniform Resource Locator, a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it
Policy	Principles, rules, and guidelines formulated or adopted by an organization
Procedure	Specific method employed to express policies in action
Windows AD	Windows Active Directory, a system to manage permissions and access to networked resources
Unix CentOS	Linux operating system
MySQL	An open-source relational database management system
UAT	User Acceptance Testing
Encryption	Process of using an algorithm to transform information to make it unreadable for unauthorized users
VPN	Virtual Private Network, an encrypted connection over the Internet from a device to a network
SSL	Secure Sockets Layer, a security technology for establishing an encrypted connection

Acronym	Description
SFTP	Secure File Transfer Protocol, a network protocol used for secure file transfer
DDOS	Distributed denial-of-service attack
GPO	A set of Group Policy configurations called Group Policy Object
RPO	Recovery Point Objective
RTO	Recovery Time Objective
NIST	National Institute of Standards and Technology

Introduction

This document is a report as a result of diagnostics of Open Joint-Stock Company "Azerishiq"'s (hereinafter – Company) Electronic Application Management System (hereinafter – System) in compliance with security requirements based on Trust Services Criteria for Security (AICPA, Trust Services Criteria).

Goals and objectives

The main objective of the Project was to perform diagnostics of internal regulatory documents, infrastructure, and processes of the Company in the following domains of security requirements:

- Common Criteria Related to Control Environment
- Common Criteria Related to Communication and Information
- Common Criteria Related to Risk Assessment
- Common Criteria Related to Monitoring Activities
- Common Criteria Related to Control Activities
- Common Criteria Related to Logical and physical access control
- Common Criteria Related to System Operations
- Common Criteria Related to Change management
- Common Criteria Related to Risk mitigation

Executive Summary

Azerishiq OJSC engaged Deloitte & Touche LLAC (hereinafter – “Deloitte”) to assess the level of compliance of Electronic Application Management System developed by Technofusion LLC with the security requirements based on Trust Services Criteria (<https://www.aicpa.org/>).

Scope

We have examined the “Electronic Application Management System” developed by Technofusion LLC for Azerishiq OJSC and the suitability of the design and implementation of controls to meet the security requirements for February, 2020. The description indicates that certain applicable criteria can be achieved only if complementary user-entity controls contemplated in the design of Company controls are suitably designed and implemented effectively, along with related controls at the service organization. We have not evaluated the suitability of the operational effectiveness of the controls.

Our procedures included assessing the risks that the information is not fairly presented and that the controls were not suitably designed or implemented effectively to meet the applicable criteria. We believe that the evidence we obtained is sufficient and appropriate.

Inherent limitations

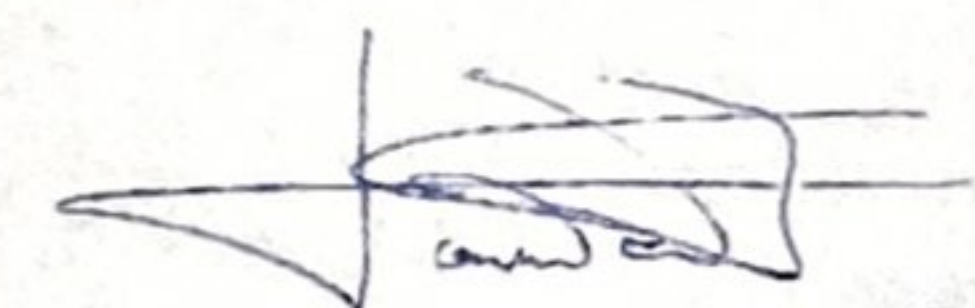
Because of their nature and inherent limitations, controls at a service organization may not always implemented effectively to meet the applicable requirements. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or implementation of the controls to meet the applicable criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Intended use

This report and the description of controls and results thereof are intended solely for the information and use of Azerishiq; subsidiaries and affiliates of Azerishiq’s System related to security during February 2020; and prospective subsidiaries and affiliates, independent auditors and practitioners providing services to such subsidiaries and affiliates, 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 subsidiaries and affiliates, subservice organizations, and other parties
- Internal control and System limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The risks that may threaten the achievement of the applicable 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.



Tural Hajiyev, Director

Deloitte Azerbaijan