

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

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

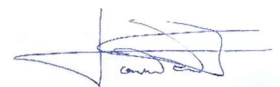
Because of their nature and inherent limitations, controls at a service organization may not always implemented effectively to meet the applicable requirements. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability 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

Procedures performed by Independent Service Auditor

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
CONTROL ENVIRONMENT					
C_ENV_01	CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The Company has documented the code of business conduct and ethical standards, which reviewed, updated if applicable, and approved by the board of directors and senior management annually.	1. We conducted an interview with Araz Mammadzade, Head of education center of the Company, and discussed the control design. 2. We inspected the code of business conduct and ethical standards of the Company noting following: - Conduct and standards outlines the service organization's commitments to integrity and ethical values - Conduct and standards updated and approved by the board of directors and senior management within the examination period.	No exceptions noted.
C_ENV_02			Personnel should pass the trainings, confirmed the control procedure design, and formally reaffirm them annually thereafter.	1. We conducted an interview with Araz Mammadzade, Head of education center of the Company, and discussed the control design. 2. We requested the list of trainings that employees should pass, and confirmed that among of this trainings Company provides information about ethical behavior and standards.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
CONTROL ENVIRONMENT					
C_ENV_04	CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities documented and reviewed annually.	We inspected sample of job descriptions to determine that executive management roles and responsibilities documented and reviewed annually.	No exceptions noted.
C_ENV_05			Executive management maintains independence from those that operate the key controls within the environment.	We obtained and inspected the organizational chart to determine that executive management maintained independence from those that operated the key controls within the environment.	No exceptions noted.
C_ENV_06	CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at the various levels of the organization and requirements relevant to security. Personnel are required to sign a copy of their job description to acknowledge their understanding of their responsibilities. Reporting relationships and organizational structures reviewed periodically by senior management and the board of directors as part of organizational planning and adjusted as needed based on changing commitments and requirements.	<ol style="list-style-type: none"> 1. We conducted an interview with management regarding communication of organizational charts. 2. We requested organizational charts to determine that organizational charts are in place to communicate key areas of authority and responsibility and updated as needed. 3. For a selection of IT personnel, we requested the file copy of job descriptions. 	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
CONTROL ENVIRONMENT					
C_ENV_07	CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The experience and training of candidates, whether an employee, contractor, or vendor employee, for employment of transfer are evaluated before they assume the responsibilities of their position to support the achievement of objectives. Existing personnel evaluated at least annually.	We conducted an interview with Sevil Huseynova, Head of Human Resource Department, and discussed the control design.	No exceptions noted.
C_ENV_08			Management establishes requisite skillsets for personnel, and provides continued training about its commitments and requirements for personnel to support the achievement of objectives. Management monitors compliance with training requirements.	<ol style="list-style-type: none"> 1. We conducted an interview with Araz Mammadzade, Head of education center of the Company, and discussed the control design. 2. As a part of testing approach, we obtained the dates and attendance sheets for role-specific trainings and determined that the employees had signed the attendance sheet for training sessions on the specified dates. 3. We obtained the dates and attendance sheets for the trainings and ensured that security training conducted annually. 	No exceptions noted.
C_ENV_9	CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The Company management and the board of directors perform annual performance evaluations to communicate and hold individuals accountable for performance of internal control responsibilities. The manager and employee sign the performance evaluation. Corrective actions, including training or sanctions, as necessary.	We conducted an interview with Sevil Huseynova, Head of Human Resource Department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
CONTROL ENVIRONMENT					
C_ENV_10			Each the Company department, such as Software Development, Information Security, Infrastructure, Networking and Systems Administration, IT Operations, Help Desk, Human Resources, Legal, Compliance, Internal Audit, Finance, Customer Support, IT Operations, hold periodic meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of department's responsibilities.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design. We did not inspect the management meeting minutes to determine that management met on a weekly basis to discuss entity business objectives, because requested data was not provided.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
COMMUNICATION AND INFORMATION					
C_COM_01	CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The Company has implemented various processes and procedures relevant to security to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. The Company has logical and physical security, change management, incident monitoring, and data classification, integrity, and retention controls, as necessary, with checks and balances woven into each applicable process to ensure quality of processing.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_COM_02	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.	The Company has incident response policies and procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management and the board of directors as necessary.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_COM_03			Internal and external users informed on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
COMMUNICATION AND INFORMATION					
C_COM_04			Personnel are required to attend annual security, confidentiality, and privacy training.	<p>1. We conducted an interview with Araz Mammadzade, Head of education center of the Company, and discussed the control design.</p> <p>2. We obtained the dates of trainings and attendance sheets for the annual security training, as well as the list of quarterly security compliance updates for employees and determined that employees had signed the attendance sheets for training sessions.</p>	No exceptions noted.
C_COM_05	CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	System descriptions made available to authorized external users that delineate the boundaries of the system and describe relevant system components as well as the purpose and design of the system. Documentation of the system description made available to authorized external users via the entity's customer-facing website.	<p>1. We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.</p> <p>2. We ensured that instructions and guidelines about design and operation of the system are publicly available in the official website of the Company: https://www.azerishiq.az/</p> <p>Internal Users:</p> <p>1. According to the interview with Galib Hamidov an induction training is conducted for the new hires who will work with the system as part of their job duties (e.g. operators). During training entity's commitments, system design and functionality presented. Training effectiveness and knowledge level of employees are evaluated based on testing results.</p>	No exceptions noted.
C_COM_06			Before personal information is collected, the entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, breach notification requirements, and disposal of personal information.	<p>1. We conducted an interview with Galib Hamidov, Head of IT department and discussed the control design.</p> <p>2. We determined that all new customer contracts include the section regarding personal data collection and the customer are required to sign this section to agree on personal data collection.</p>	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
COMMUNICATION AND INFORMATION					
C_COM_07			<p>IT management prior to initiating service approves new client contracts. The client and IT management sign a Service Level Agreement (SLA).</p> <p>Service level agreements with the third-parties includes:</p> <ul style="list-style-type: none"> -Scope of business relationship and services offered -Information security requirements (confidentiality, privacy) -Notification of any changes controlled by the provider with the impact to the entity -Timely notification of security or operational incidents -Assessment and independent verification of compliance with agreement provisions and/or terms. 	<ol style="list-style-type: none"> 1. We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design. 2. We obtained SLA with third-party company and determined that agreement includes: <ul style="list-style-type: none"> -Scope of business relationship and services offered -Information security requirements (confidentiality, privacy) -Notification of any changes controlled by the provider with the impact to the entity -Timely notification of security or operational incidents -Assessment and independent verification of compliance with agreement provisions and/or terms. 	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
RISK ASSESSMENT					
C_RSK_01	CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Documented policies and procedures are in place to guide personnel when performing the risk assessment process.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_RSK_02	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.	A formal risk assessment performed on an annual basis to identify threats that could impair systems security commitments and requirements. Management develops risk mitigation strategies to address risks identified during the risk assessment process.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design. The Company has a formalized IT risk management methodology that defines a risk identification and assessment procedure to identify threats that may affect system security.	No exceptions noted.
C_RSK_03	CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management conducts a periodic fraud risk assessment to identify the various ways that fraud and misconduct can occur, including how management might engage in inappropriate actions, and maintains documentation of this assessment.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design. The Company has a formalized IT risk management methodology that defines a risk identification and assessment procedure to identify threats that may affect system security.	No exceptions noted.
C_RSK_04			The Company has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design. The Company has a formalized IT risk management methodology that defines a risk identification and assessment procedure to identify threats that may affect system security.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
RISK ASSESSMENT					
C_RSK_05	CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly affect the system of internal control.	<p>The Company, through its ongoing an annual risk assessment process, evaluates changes in</p> <p>a. the regulatory, economic, and physical environment in which The Company operates.</p> <p>B. the business environment, including industry, competitors, regulatory environment, and consumers.</p> <p>C. the potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.</p> <p>D. the management and respective attitudes and philosophies on the system of internal control.</p> <p>E. The Company's systems and changes in the technology environment.</p> <p>F. vendor and business collaborate relationships.</p>	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
MONITORING ACTIVITIES					
C_MON_01	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.	The internal audit department performs periodic audits to include information security assessments.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_MON_02			The Company provides training, as well as annual performance reviews, for internal audit personnel.	We conducted an interview with Sevil Huseynova, Head of Human Resource Department, and discussed the control design.	No exceptions noted.
C_MON_03			Internal audit personnel perform IT audit procedures using a formal methodology, document their procedures and results in working papers, and prepare an audit report summarizing the procedures performed and the findings from those procedures.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_MON_04	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.	Internal audit performs control assessments on an annual basis and communicates results to the executive management for monitoring of corrective actions.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
MONITORING ACTIVITIES					
C_MON_05			Reporting protocols for identified deficiencies documented and made available to personnel.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
CONTROL ACTIVITIES					
C_CONTR_01	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.	As part of its annual risk assessment, management linked the identified risks to controls that designed and operated to address them. When the need for new controls identified, management develops the requirements for the new controls and uses the change management process to implement them.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_CONTR_02			As part of the risk assessment, management assessed the environment, complexity, nature and scope of its operations when developing control activities to mitigate the risks.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_CONTR_03			A business continuity and disaster recovery plan documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_CONTR_04			The disaster recovery plan tested on an annual basis.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
CONTROL ACTIVITIES					
C_CONTR_05	CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	As part of the IT strategic plan, strategic IT risks affecting the organization and recommended courses of action identified and discussed.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design. We obtained IT investment plan prepared annually that determines strategic IT risks affecting the organization and recommended courses of action identified and discussed.	No exceptions noted.
C_CONTR_06			Management developed a list of control activities to manage the technology infrastructure risks identified during the annual risk assessment process.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_CONTR_07			Management developed a list of control activities to manage the security access management risks identified during the annual risk assessment process.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
CONTROL ACTIVITIES					
C_CONTR_08	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.	The Company's policy and procedure manuals address controls over significant aspects of operations. Policy sections include: a. security requirements for authorized users; b. data classification and associated protection, access rights, retention, and destruction requirements; c. risk assessment; d. access protection requirements; e. user provisioning and de-provisioning; f. responsibility and accountability for security; g. responsibility and accountability for system changes and maintenance; h. change management; j. security and other incidents identification, response and mitigation; l. handling of exceptions and situations not specifically addressed in policies; m. commitment and requirement identification and compliance measurement; and n. information sharing and disclosure.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design. We inspected information security policy, access management policy and procedure, risk management methodology and change management policy developed by the Company.	No exceptions noted.
C_CONTR_09			IT security policies are reviewed and updated annually by senior management for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design. We inspected information security policy and risk management methodology developed by the Company.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
C_LPAC_01	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.	Documented policies and procedures are in place regarding systems authentication, access.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_LPAC_02			Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets created to remove access as necessary in a timely manner.	1. We conducted an interview with Ferkhad Yunisov, Head of Infrastructure department, and discussed the control design. 2. We conducted an interview with Perviz Guliyev, Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation" on 04/12/2019 and discussed the control design.	No exceptions noted.
APP.01			Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and segregation of duties.	We conducted an interview with Perviz Guliyev, Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation" and discussed the control design.	No exceptions noted.
APP.02			Access for terminated and/or transferred users removed or modified in a timely manner.	1. We conducted an interview with Perviz Guliyev, Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation" and discussed the control design. 2. We inspected user lists, including user account statuses, within the application database.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
				3. We inspected the lists of resigned employees and extracted list of users to test that resigned users' accounts are terminated in a timely manner.	
APP.03			Access authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users authorized to gain access to the system. Password parameters meet company and/or industry standards (e.g., password minimum length and complexity, expiration, account lockout).	1. We conducted an interview with Perviz Guliyev, Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation" and discussed the control design. 2. We inspected the application password configurations.	No exceptions noted.
APP.04			Privileged-level access (e.g., security administrators) is authorized and appropriately restricted.	1. We conducted an interview with Tehmin Babayev, Developer of "Information Technology department, Programming division", developer of the target application and discussed the control design. 2. We extracted the list of users to identify that privileged-level accounts are authorized and appropriate for user's assigned duties.	No exceptions noted.
UNIX.05			Access authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users authorized to gain access to the system. Password parameters meet company and/or industry standards (e.g., password minimum length and complexity, expiration, account lockout).	1. We conducted the interview with Rashad Huseynov, Lead Network Engineer, and discussed the control design. 2. We requested, but did not obtained the Company's password policy. 3. We inspected the password settings on OS level.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
UNIX.06			Privileged-level access (e.g., security administrators) is authorized and appropriately restricted.	<ol style="list-style-type: none"> 1. We conducted the interview with Rashad Huseynov, Lead Network Engineer, and discussed the control design. 2. We determined that privileged access to OS layer was provided only to appropriate specialists of Programming Unit according job function. 	No exceptions noted
SQL.01			Access authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users authorized to gain access to the system. Password parameters meet company and/or industry standards (e.g., password minimum length and complexity, expiration, account lockout).	<ol style="list-style-type: none"> 1. We conducted an interview with Tehmin Babayev, developer of Information Technology department, Programming division and discussed the control design. 2. We were informed that "MySQL server and phpmyadmin GUI" is used. 3. We were informed that only Tehmin Babayev has access to the database. 4. Tehmin Babayev uses randomly generated password by "phpmyadmin" 5. Passwords that are in use meet industry standards. 	No exceptions noted
SQL.02			Privileged-level access (e.g., security administrators) is authorized and appropriately restricted.	<ol style="list-style-type: none"> 1. We conducted an interview with Tehmin Babayev, developer of Information Technology department, Programming division and discussed the control design. 2. We were informed that privileged access on Database Level (MySQL Server) is restricted and only Tehmin Babayev has privileged access. 3. We were informed that there are no active generic accounts on MySQL Server. 	No exceptions noted

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
NTW.01			<p>Network administrative access is restricted to user accounts accessible by authorized by the following personnel:</p> <ul style="list-style-type: none"> • Senior Network and System Administrator 	<ol style="list-style-type: none"> 1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design. 2. According to the interview with Rashad Huseynov, administrative access to the IPS (Palo Alto) is provided only to him based on assigned duties. Rashad Huseynov has full permissions within Palo Alto system. 3. We inspected the list of administrative users in the Palo Alto system. 	No exceptions noted
NTW.02			<p>Network users authenticated via individually assigned user accounts and passwords. Networks are configured to enforce:</p> <ul style="list-style-type: none"> • History • Maximum age • Minimum age • Length • Complexity 	We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted.
NTW.03			<p>Network audit policy configurations are in place that include:</p> <ul style="list-style-type: none"> • Object access • System events • Change events 	<ol style="list-style-type: none"> 1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design. 2. According to the interview with Rashad Huseynov, objects for service, application are defined, system and events are displayed in IPS logs. 3. We inspected system and configuration logs and screenshots of object access configurations. 	No exceptions noted
NTW.04			Alerts generated to notify network administrators of suspicious activity.	1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
				<p>2. According to the interview with Rashad Huseynov, Palo Alto IPS generates the list of logs with alerts containing the severity indicator.</p> <p>3. The system automatically takes an action if needed and network administrators can take actions by observing threat logs.</p> <p>4. We inspected the screenshots of threat logs.</p>	
NTW.05			<p>Management utilizes intrusion detection systems (IDS) to detect unauthorized intrusion into the production environment. The IDS functionality has configurations to prevent against DDOS (Distributed Denial of Service) attacks.</p>	<p>1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.</p> <p>2. According to the interview with Rashad Huseynov, Palo Alto IPS is utilized to detect unauthorized intrusions and activities, the system automatically takes action according to the configurations. All suspicious activities are listed in the Threat Logs.</p> <p>3. We were informed that Palo Alto system is properly configured to protect against DDOS attacks.</p> <p>4. We inspected the screenshots of threat logs and DoS protection configurations.</p>	No exceptions noted
C_LPAC_03	CC6.2	<p>Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access administered by the entity. For those users whose access administered by the entity, user system</p>	<p>Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.</p>	<p>We conducted an interview with Galib Hamidov, Head of IT department and discussed the control design.</p>	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
C_LPAC_04		credentials removed when user access is no longer authorized.	Human Resources management utilizes a termination checklist to ensure that specific elements of the termination process consistently executed. This includes but is not limited to the terminated employee's physical and logical access to IT facilities and computer systems. The checklist retained in the employee files.	We conducted an interview with Ferkhad Yusinov, Head of Infrastructure department, and discussed the control design.	No exceptions noted.
C_LPAC_05			Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately.	We conducted an interview with Ferkhad Yunisov, Head of Infrastructure department, and discussed the control design.	No exceptions noted.
C_LPAC_06	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.	A termination checklist completed and access revoked for employees within 24 hours as part of the termination process.	We conducted an interview with Ferkhad Yusinov, Head of Infrastructure department, and discussed the control design.	No exceptions noted.
C_LPAC_07			Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
C_LPAC_08	CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Policies and procedures are in place to guide personnel in physical security activities.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_LPAC_09			Visitors to the facility and server room required should be escorted by an employee.	1. We conducted an interview with Rashad Huseynov, Lead Network engineer, and discussed the control design. 2. We were informed that currently the Company performs modification of server room.	No exceptions noted.
C_LPAC_10			Visitors to the facility and server room are required sign a visitor's log.	1. We conducted an interview with Rashad Huseynov, Lead Network engineer, and discussed the control design. 2. According to the interview with Rashad Huseynov access to server room is regulated by fingerprint scan, and notifications of each entrance sent by SMS to Rashad Huseynov.	No exceptions noted.
C_LPAC_11			Access to the server room is provided by fingerprint and assigned to the following positions: • Senior Network and System Administrator	We conducted an interview with Rashad Huseynov, Lead Network engineer, and discussed the control design.	No exceptions noted.
C_LPAC_12			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 that has	Policies and procedures are in place to guide personnel on the destruction of data.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
		been diminished and is no longer required to meet the entity's objectives.			
FRW.01	CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	System firewalls configured to limit unnecessary ports, protocols and services. The only ports open into the environment defined.	<ol style="list-style-type: none"> 1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design. 2. According to the interview with Rashad Huseynov, permitted and denied services, protocols and ports are configured in firewall's access rules. Unknown and restricted connections are dropped by the firewall system. 3. We inspected the screenshot of 'permit' and 'deny' rules, configured on the firewall. 	No exceptions noted
FRW.02			The ability to modify the firewall system software, configurations or rule sets is restricted to authorized IT firewall admin personnel.	<ol style="list-style-type: none"> 1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design. 2. We inspected screenshot of privileged-level users within firewall system. 	No exceptions noted
NTW.09			Intrusion detection systems are used to provide continuous monitoring of the Company's network and prevention of potential security breaches.	<ol style="list-style-type: none"> 1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department). 2. According to the interview with Rashad Huseynov, Palo Alto IPS is used for monitoring and prevention of potential security breaches, the system automatically takes action according to the configurations. All suspicious activities are highlighted in the Threat Logs. 3. We inspected screenshots of system configurations and threat logs. 	No exceptions noted

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
	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.	Removable media to be used for customer or system data is encrypted and sanitized prior to connecting such devices to the information system.	We conducted an interview with Ferkhad Yunisov, Head of Infrastructure department, and discussed the control design. The Company has implemented antivirus software on domain level for all endpoints and periodic scans are performed.	No exceptions noted.
NTW.06			VPN, SSL, secure file transfer program (SFTP), and other encryption technologies used for defined points of connectivity.	<ol style="list-style-type: none"> 1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design. 2. According to the interview with Rashad Huseynov, users have access to the company's network via encrypted VPN channel and connections with other companies are maintained via encrypted channels. 3. We inspected the screenshots of encryption settings for VPN and connections with other companies. 	No exceptions noted
C_LPAC_14	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.	Only authorized system administrators are able to install software on system devices. Unauthorized use or installation of software explicitly covered in the employee handbook and Rules of Behavior.	We conducted an interview with Ferkhad Yunisov, Head of Infrastructure department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Logical and Physical Access Controls					
NTW.07			Content filter and virus prevention system is utilized to analyze network events and report possible or actual network security breaches.	<ol style="list-style-type: none"> 1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department), and discussed the control design. 2. According to the interview with Rashad Huseynov, Palo Alto IPS is utilized to filter the URLs and protect against viruses and vulnerabilities on the network level, the system automatically takes action according to the configurations. Symantec Endpoint Protection is installed on employee's workstations. 3. We inspected the screenshots of Security Profiles configurations in the Palo Alto system. 	No exceptions noted
C_LPAC_15			Vulnerability scans performed on an annual basis and remedial actions taken.	We conducted an interview with Rashad Huseynov, (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
System Operations					
NTW.08	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.	The monitoring software is configured to alert when thresholds have been exceeded.	1. We conducted an interview with Rashad Huseynov, Lead Network engineer, and discussed the control design. 2. We inspected the monitoring system configurations, notification configurations and an example alert and determined that the monitoring software is configured to alert the Senior Network and System Administrator when thresholds had been exceeded.	No exceptions noted
C_SysOP_01			Internal audits are performed and reviewed by management on an annual basis.	We conducted an interview with Galib Hamidov, Head of IT department, on 21/11/2019 and discussed the control design.	No exceptions noted.
C_SysOP_02			Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	We conducted an interview with Rashad Huseynov, (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted.
C_SysOP_03	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	Security incidents are reported to the help desk and tracked through to resolution. Incidents that may affect security compliance are reported to the security compliance officer.	We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
System Operations					
NTW.09		its objectives; anomalies are analyzed to determine whether they represent security events.	Intrusion detection systems are used to provide continuous monitoring of the Company's network and prevention of potential security breaches.	<p>1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.</p> <p>2. According to the interview with Rashad Huseynov, Palo Alto IPS is used for monitoring and prevention of potential security breaches, the system automatically takes action according to the configurations. All suspicious activities are highlighted in the Threat Logs.</p> <p>3. We inspected the screenshots of system configurations and threat logs.</p>	No exceptions noted
NTW.10			All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted.
FRW.03			The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	<p>1. We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.</p> <p>2. According to the interview with Rashad Huseynov, unknown or restricted connections are not allowed by the firewall system.</p> <p>3. We inspected the screenshot of 'permit' and 'deny' rules, configured on the firewall.</p>	No exceptions noted
C_SysOP_04	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.	The Company has developed security incident response policies and procedures that are communicated to authorized users. A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
System Operations					
C_SysOP_05			A ticket tracking application is utilized to track and respond to incidents. All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_SysOP_06	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.	Management has established defined roles and responsibilities to oversee implementation of information security policies including incident response.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
BCP.01	Daily incremental and weekly full backups are configured for the databases.		1. We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design. 2. We inspected the backup policy within the system.	No exceptions noted.	
NTW.10	All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.		We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted.	
C_SysOP_07	Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.		We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted.	
NTW.10	CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
System Operations					
C_SysOP_08			Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	We conducted an interview with Rashad Huseynov (Lead Network Engineer of Information Technology department) and discussed the control design.	No exceptions noted.
C_SysOP_09			Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_SysOP_10			A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Change Management					
C_CHM_01	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.	The Company has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	We conducted an interview with Perviz Guliyev (Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation") and discussed the control design. We were informed that development of the system is outsourced.	No exceptions noted.
C_CHM_02			System change requests are documented and tracked in a ticketing system.	We conducted an interview with Perviz Guliyev (Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation") and discussed the control design.	No exceptions noted.
C_CHM_03			The Company's software and infrastructure change management process requires that change requests are: <ul style="list-style-type: none"> • Authorized • Formally documented • Tested prior to migration to production • Reviewed and approved by management The Company requires all changes, including maintenance activities, to be documented in the help desk application and tracked from initiation through deployment and validation.	We conducted an interview with Perviz Guliyev (Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation") and discussed the control design.	No exceptions noted.
C_CHM_04			Baseline configurations are retained within the configuration manager tool for roll back capability anytime an approved configuration change is made. Baseline configurations are reviewed and updated annually, when required due to reviews and system changes, and anytime integral system components are added.	We conducted an interview with Perviz Guliyev (Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation") and discussed the control design. We were informed that development of the system is outsourced.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Change Management					
C_CHM_05			The Company maintains a documented change management and patch management process.	We conducted an interview with Perviz Guliyev (Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation") and discussed the control design.	No exceptions noted.
C_CHM_06			The Company contracts with third parties to conduct monthly security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management. Management develops a plan of action for each recommendation and follows up on open recommendations monthly.	We conducted an interview with Perviz Guliyev (Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation") and discussed the control design.	No exceptions noted.
C_CHM_07			Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.	We conducted an interview with Perviz Guliyev (Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation") and discussed the control design. We were informed that development of the system is outsourced.	No exceptions noted.
C_CHM_08			Prior code is held in the repository for rollback capability in the event that a system change does not function as designed.	We conducted an interview with Perviz Guliyev (Manager of "Department of Perspective Development and ASAN Service of the Board of Technical Assistance and Electrical Installation") and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Risk Mitigation					
C_RSKM_01	CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel when performing the risk assessment process.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_RSKM_02			A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_RSKM_03			Management develops risk mitigation strategies to address risks identified during the risk assessment process.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_RSKM_04	CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The risk management program includes the use of insurance to minimize the financial impact of any loss events.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Control ID	TSC Ref. #	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Results of Tests Performed by Deloitte
Risk Mitigation					
C_RSKM_05			A vendor risk assessment is performed for all vendors on an annual basis that have access to confidential data or affect the security of the system.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.
C_RSKM_06			Defined Service Level Agreements (SLA) are in place to outline and communicate the terms, conditions and responsibilities for third-party providers.	We conducted an interview with Galib Hamidov, Head of IT department, and discussed the control design.	No exceptions noted.

Deloitte.

Deloitte adı Deloitte Touche Tohmatsu Limited şəbəkəsinə daxil olan üzv şirkətlərdən birinə və ya bir neçəsinə və əlaqədar müəssisələrinə aid ola bilər. DTTL ("Deloitte Qlobal") və bu şəbəkəyə daxil olan hər bir üzv şirkət ayrı-ayrılıqda hüquqi şəxslər və müstəqil müəssisələrdir. DTTL müştərilərə xidmətlər göstərmir. Ətraflı məlumat üçün www.deloitte.com/about səhifəsinə daxil olun.

Deloitte qlobal səviyyədə audit və əminlik, konsaltinq, maliyyə, risk, vergi üzrə məsləhət xidməti və digər əlaqədar xidmətlər göstərən aparıcı markalardandır. 150-dən çox ölkədə və ərazidə xidmətlər göstərən üzv şirkətlər şəbəkəsi Fortune Global 500® üzrə beş şirkətdən dördünə öz xidmətlərini göstərir. Deloitte-un təxminən 312,000 peşəkar mütəxəssisinin təklif etdiyi fərq yaradan həllər haqqında ətraflı məlumat üçün www.deloitte.com səhifəsinə daxil olun.

Bu məlumatda yalnız ümumi informasiya əks olunur və Deloitte Touche Tohmatsu Limited şirkətlərindən, onun üzv şirkətlərindən və ya əlaqədar müəssisələrdən (birlikdə "Deloitte Şəbəkəsi") hər hansı biri bu məlumat vasitəsilə peşəkar məsləhətləşmə və ya xidmətlər təmin etmir. Maliyyə fəaliyyətinizə və ya müəssisənizə təsir göstərə biləcək hər hansı qərarlar qəbul etməzdən və ya tədbirlər görməzdən əvvəl peşəkar mütəxəssis ilə məsləhətləşmək daha məqsəduyğundur. Deloitte Şəbəkəsinə daxil olan heç bir müəssisə bu məlumata istinad edən hər hansı şəxsin məruz qaldığı zərərə görə məsuliyyət daşımır.