

System and Organization Controls (SOC 3) Report

Independent Assurance Report on Controls at Service Organization

Picsart, Inc.



Contents

Independent Assurance Report on the Description of Controls, their Design and Operating Effectiveness	2
Picsart, Inc. Management Statement	5
Picsart, Inc.'s System Description	7

Independent Assurance Report on the Description of Controls, their Design and Operating Effectiveness

Գրանթ Թորնթոն Քոնսլթինգ ՓԲԸ

Երևան Պլազա բիզնես կենտրոն

ՀՀ, ք. Երևան 0015

Գրիգոր Լուսավորչի 9

Հ. + 374 10 500 964

+ 374 10 500 961

Grant Thornton Consulting CJSC

Yerevan Plaza Business Center

9 Grigor Lusavorich Street,

Yerevan 0015, Republic of Armenia

T + 374 10 500 964

+ 374 10 500 961

To the Management of Picsart, Inc.

Scope

We have performed an independent reasonable assurance engagement on Picsart, Inc.'s description of its system entitled "Picsart Creative Platform" on pages 7-12, for the period from 1 March 2023 to 29 February 2024 (the "System Description"), and on the design and operation of controls related to control objectives stated in the System Description, based on the criteria for the security, availability, processing integrity, confidentiality and privacy (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

Management's Responsibilities

In "Picsart, Inc. Management Statement", Picsart, Inc. has provided a statement about the fairness of the presentation of the System Description and the design and operating effectiveness of the controls to achieve the related control objectives. Management of Picsart, Inc. is responsible for preparing the Description and the accompanying Statement on pages 5-6, including the completeness, accuracy, and method of presentation of the System Description and the Statement, providing the services covered by the System Description, specifying the control objectives and stating them in the System Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Statement, and designing, implementing, documenting and effectively operating controls to achieve the stated System-related control objectives.

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

The firm applies International Standard on Quality Management 1 and accordingly maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on Picsart, Inc.'s System Description and on the design and operating effectiveness of the controls to achieve the related control objectives stated in the System Description, based on our procedures.

We conducted our engagement in accordance with the "*International Standard on Assurance Engagements 3000 (Revised): Assurance Engagements other than Audits or Reviews of Historical Financial Information*" issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, based on the criteria stated in management's Statement, the System Description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the System Description.

An assurance engagement to report on the service organization's system and the suitability of the design and operating effectiveness of controls involves performing procedures to obtain evidence about the fairness of the System Description presentation and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives, based on the criteria in management's Statement. The procedures selected depend on the service auditor's judgment, including the assessment of risks that the System Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the System Description. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the System Description were achieved. An assurance service of this type also includes evaluating the overall presentation of the System Description, suitability of the control objectives and suitability of the criteria specified by the service organization in its assertion.

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

Inherent Limitations of Controls

The System Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' environments and systems and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or failures, including the possibility of human error and circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy will be achieved.

Examples of inherent limitations in an entity's security controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer;
- Ineffective controls at a vendor or business partner;
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.



Also, the projection to the future of any evaluation of the fairness of the presentation of the System Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are described on pages 7-10.

In our opinion, in all material respects:

- the System Description fairly presents Picsart, Inc.'s System as designed and implemented throughout the period from 1 March 2023 to 29 February 2024, in accordance with the description criteria;
- the controls related to the control objectives stated in the System Description were suitably designed throughout the period from 1 March 2023 to 29 February 2024 to provide reasonable assurance that Picsart, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Picsart, Inc.'s controls throughout the period from 1 March 2023 to 29 February 2024;
- the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the System Description were achieved, operated effectively throughout the period from 1 March 2023 to 29 February 2024 to provide reasonable assurance that Picsart, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria and if the subservice organizations and user entities applied the complementary controls assumed in the design of Picsart, Inc.'s controls throughout the period from 1 March 2023 to 29 February 2024.

Grant Thornton Consulting CJSC

03 April 2024



Picsart, Inc. Management Statement

Picsart, Inc. Management's Statement Regarding the Effectiveness of its Controls, Based on the Trust Services Principles and Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy

We have prepared the accompanying description of Picsart, Inc.'s System entitled "Picsart Creative Platform" (including Picsart Applications and "Picsart for Developers" platform), throughout the period from 1 March 2023 to 29 February 2024, for user entities of the services and their auditors who audit and report on such user entities' in the areas of security, availability, confidentiality, processing integrity and privacy and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks related to internal control related to security, availability, confidentiality, processing integrity and privacy.

Picsart, Inc. uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Picsart, Inc., to achieve Picsart, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Picsart, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Picsart, Inc.'s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Picsart, Inc., to achieve Picsart, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Picsart, Inc.'s controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of Picsart, Inc.'s controls.

The System description does not extend to the controls of the user entities as set out in "Terms of Use" at [Terms of Use - Picsart](#).

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

- System description fairly presents Picsart, Inc.'s System during the period from 1 March 2023 to 29 February 2024 as it relates to controls of security, availability, confidentiality, processing integrity and privacy. The criteria we used in making this statement were that the System description:
 - presents how the System was designed and implemented to process relevant user entity data, including, if applicable:
 - types of services provided, including, as appropriate, the types of data processed;
 - the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities;
 - how the system captures and addresses significant events and conditions;
 - relevant control objectives and controls designed to achieve those objectives;
 - other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
 - includes relevant details of changes to Picsart, Inc.'s system during the period covered by the System Description;
 - does not omit or distort information relevant to Picsart, Inc.'s system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Picsart, Inc.'s

System that each individual user entity and its auditor may consider important in its own particular environment.

- controls related to the control objectives stated in the System Description were suitably designed and operating effectively throughout the period from 1 March 2023 to 29 February 2024 to achieve those control objectives, if the subservice organizations and user entities applied the complementary controls assumed in the design of Picsart, Inc.'s controls throughout the period from 1 March 2023 to 29 February 2024. The criteria we used in making this assertion are the following:
 - Risks that threaten the achievement of the control objectives stated in the System Description have been identified by the management of Picsart, Inc.;
 - Controls identified in the System Description would, if operated as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the System Description from being achieved;
 - Controls were consistently applied as designed, including manual controls were applied by individuals who have the appropriate competence and authority.
- System was protected against unauthorized access, use, or modification to achieve Picsart, Inc.'s commitments and system requirements;
- System was available for operation and use, to achieve Picsart, Inc.'s commitments and system requirements;
- System information is collected, used, disclosed, and retained to achieve Picsart, Inc.'s commitments and system requirements;
- System processing is complete, valid, accurate, timely, and authorized to meet Picsart, Inc.'s commitments and system requirements;
- Personal information is collected, used, retained, disclosed, and disposed to meet Picsart, Inc.'s commitments and system requirements, based on the Control Criteria.

Picsart, Inc. Management

29 March 2024

Picsart, Inc.'s System Description

Picsart, Inc. Background

Picsart, Inc. is an information technology company based in multiple locations that develops the Picsart suite of online photo and video editing applications, with a social creative community, also the “Picsart for Developers” platform for Enterprise customers. The platform allows users to take and edit pictures and videos, draw with layers, and share the images on Picsart, Inc.'s and other social networks. It is one of the world's most popular apps, with reportedly more than 1 billion downloads across 180 countries.

Control Environment

Picsart, Inc. management has identified the controls over the system throughout the period from 1 March 2023 to 29 February 2024 to achieve its commitments and system requirements related to the operation using the criteria for security, availability, processing integrity, confidentiality and privacy (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this, the management has selected a set of controls to provide reasonable assurance that:

- System is protected against unauthorized access, use, or modification to achieve Picsart, Inc.'s commitments and system requirements;
- System is available for operation and use, to achieve Picsart, Inc.'s commitments and system requirements;
- System information is collected, used, disclosed, and retained to achieve Picsart, Inc.'s commitments and system requirements;
- System processing is complete, valid, accurate, timely, and authorized to meet Picsart, Inc.'s commitments and system requirements;
- Personal information is collected, used, retained, disclosed, and disposed to meet Picsart, Inc.'s commitments and system requirements, based on the Control Criteria.

Scope

The scope of the systems covered in this report includes:

The key products of the Company are:

- Picsart Photo Editors
- Picsart Video Editors
- Picsart Mobile Apps
- Picsart Quicktools
- Picsart for Developers
- Picsart Business Solutions
- Admaker tool

The Key organizational units (teams) of the Company are:

- Infrastructure department
- Engineering department
- Product department
- Finance department

- Legal department
- Android platform unit
- IOS platform unit
- Windows platform unit
- System Monitoring and Control unit
- QA unit
- Monetization unit
- Web-Growth unit
- Distribution (CI/CD) unit
- Administrative unit
- Trust and Safety unit
- Talent growth unit
- Recruitment unit
- Information security unit

The key tools of the Company used for product development:

- AWS
- Google workspace
- Google Cloud Platform
- GitLab
- GitHub
- Kubernetes
- MongoDB
- Kibana
- Elastic Search
- Datadog
- Testrails
- Testflight
- Jenkins
- BugSnag
- Figma
- JIRA
- Confluence
- Asana
- SonarCloud
- G-Suite

- Slack

Infrastructure

Picsart, Inc.'s infrastructure includes the facilities, network, and hardware, as well as some operational software (e.g., host operating system, virtualization software, etc.) that support the provisioning and use of these resources. Picsart, Inc.'s infrastructure is designed and managed in accordance with security compliance standards and Picsart, Inc.'s security policies.

Picsart, Inc.'s servers are hosted mainly at DEFT Data Centers, some of the components are stored at Google Cloud Platform and AWS. Only switch room is located in the Yerevan office, which serves the internal network and enterprise Wi-Fi access points.

Locations

The locations covered in this report include:

- 16, Halabyan street, Yerevan, 0038, Armenia
- Optima Onyx Tower, Suite 1103, 1010 South Federal Highway, Hallandale Beach, FL 33009

People

Picsart, Inc.'s organizational structure provides a framework for planning, executing, and controlling business operations. Executive and senior leadership play important roles in establishing Picsart's tone and core values. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations, and segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel.

The Company follows a structured on-boarding process to familiarize new employees with dedicated information systems, tools, processes, systems, security practices, policies and procedures. Employees are provided with the set of the Picsart, Inc.'s policies and pass induction training to educate them as to their responsibilities concerning information security.

Customer Data

Picsart, Inc. provides solutions for processing videos and pictures.

Picsart, Inc. stores the following customer data in the data centers and cloud platforms:

- Email address of the customer account,
- Customer username/account data,
- Customer's videos and pictures, that are created/edited by Picsart, Inc.'s applications and tools,
- Analytics data.

Availability

Picsart, Inc.'s solutions are architected in a manner to maintain availability of its services through defined programs, processes, and procedures. The Business Continuity Program encompasses the processes and procedures by which Picsart, Inc. identifies, responds to, and recovers from a major event or incident within the environment. This program builds upon the traditional approach of addressing contingency management, incorporating elements of business continuity and disaster recovery plans while expanding to consider critical elements of proactive risk mitigation strategies. These strategies include continuous infrastructure capacity planning.

Contingency plans and incident response playbooks are maintained to reflect emerging continuity risks and lessons learned. Plans are tested and updated through the course of business, and the Picsart, Inc.'s Business Continuity Program is regularly reviewed and approved by senior leadership.

Picsart, Inc. has identified critical system components required to maintain the availability of the system and recover services in the event of an outage. These components are replicated across multiple availability zones; authoritative backups are maintained and monitored to ensure successful replication.

Picsart, Inc.'s solutions operate on DEFT Data Centers and cloud platforms (AWS and GCP). Sensitive user data is kept in the MongoDB in an encrypted manner. All data storages used in Picsart, Inc.'s environment are encrypted based on industry best practices (AES256 for data-at-rest).

All connections to the frontend and backend are encrypted with strong encryption protocols while in transit (at least TLS 1.2). It is fully automated and monitored by continuous functional tests to detect any sort of downtime, protect infrastructure needs and support availability commitments and requirements. Additionally, Picsart, Inc. maintains a capacity planning model to assess infrastructure usage and demands.

Security

Picsart, Inc. has established information security policies and there is an executive-level commitment to implement and follow the policies throughout the organization. Picsart, Inc. communicates its security commitment to customers in "Security Policy" at [Security policy – Picsart](#).

Information Security program is led by the CTO of Picsart.

Confidentiality

Picsart is committed to protecting the security and confidentiality of its customers' content, defined "Privacy Policy" at [Privacy Policy - Picsart](#). Picsart, Inc. communicates its confidentiality commitment to customers in "Community Guidelines" at [Community Guidelines - Picsart](#).

Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend security awareness training, which includes information, policies, and procedures related to protecting customers' content. Picsart, Inc. monitors the performance of third parties through periodic reviews, which evaluate performance against contractual obligations, including confidentiality commitments.

Privacy

Picsart, Inc. is committed to protecting the personal data of its customers' content, defined as "Privacy Policy" at [Privacy Policy - Picsart](#). Picsart, Inc. communicates its privacy commitment to customers in "Terms of Use" at [Terms of Use - Picsart](#).

Complementary user entity controls

Picsart, Inc.'s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Picsart, Inc.'s services to be solely achieved by Picsart, Inc.'s control procedures. Accordingly, user entities should establish their own internal controls or procedures to complement those of Picsart, Inc.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. These controls should not be regarded as a comprehensive list of all controls that might be pertinent at the user entities' locations. User entities' management is responsible for selecting and implementing these complementary user entity controls:

1. Ensuring the compliance with Picsart, Inc.'s Privacy Policy by their personnel and their clients;
2. Understanding and complying with their contractual obligations to Picsart, Inc.;
3. Notifying Picsart, Inc. of changes made to technical administrative contact information;
4. Notifying Picsart, Inc. regarding new, terminated user accounts and changes necessary thereto;
5. Immediately notifying Picsart, Inc. of any actual or suspected information security breaches involving the system, including compromised user accounts;
6. Grant access only to authorized and trained personnel and removing access when no longer necessary or appropriate;
7. Ensuring the supervision, management, and control of the use of the System by their personnel and their clients;
8. Developing internal policies for disaster recovery and business continuity, that address the inability to access or utilize the System;
9. Preventing the loss, malfunctioning, or damage to the System.

Complementary subservice organization controls

When controls at a vendor are necessary in combination with Picsart, Inc.'s controls to provide reasonable assurance that Picsart, Inc.'s service commitments and system requirements are achieved, based on the applicable trust services criteria, the vendor is considered a subservice organization. Picsart, Inc.'s services are designed with the assumption that certain controls will be implemented by subservice organizations (complementary subservice organization controls). It is not feasible for all the Trust Services Criteria related to Picsart, Inc.'s services to be solely achieved by Picsart, Inc.'s control procedures. Accordingly, subservice organizations should establish their own internal controls or procedures to complement those of Picsart, Inc.

Management has identified the following subservice organizations and has elected the carve-out method for the purpose of System Description and management assertion.

Subservice organization	Description
AWS	Cloud hosting services
Google Workspace	Cloud hosting services

The following are the applicable trust services criteria and controls that subservice organizations should establish to complement those of Picsart, Inc., provide additional assurance that the Trust Services Criteria described within this report are met.

Criteria	Control
CC6 Series Logical and Physical Access	<ul style="list-style-type: none"> - Physical access to the datacenter facilities is restricted to authorized personnel. - Physical access to data centers is approved by an authorized individual.

Criteria	Control
	<ul style="list-style-type: none"> - Procedures are implemented to authenticate authorized users, restrict access and detect unauthorized access attempts. - Security measures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization. - Encryption has been implemented, by default or as configured by the subservice organization, to secure the transmission and storage of information. - Procedures are implemented to securely decommission and physically destroy production assets.
CC7 Series System Operations	<ul style="list-style-type: none"> - Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems. - Incident response procedures are established and implemented to identify, analyze and remediate events and/or incidents. - Environmental protections, monitoring and procedures for regular maintenance are implemented at the datacenter facilities.
CC9 Series Risk Mitigation	<ul style="list-style-type: none"> - Procedures are established and implemented to ensure risk mitigation activities are identified, selected, and developed for risks arising from potential business disruptions.
A Series Availability	<ul style="list-style-type: none"> - Monitoring tools are implemented to monitor and manage the capacity and availability of hosting infrastructure. - Environmental protections, data backup processes and recovery mechanisms have been implemented and are appropriately tested to adequately address availability requirements.

Picsart, Inc.'s management, along with the subservice organizations, defines the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as SLAs. In addition, Picsart performs monitoring of the subservice organization controls, including the following:

- Holding periodic discussions with vendors and subservice organizations,

Reviewing attestation reports over services provided by vendors and subservice organizations, if applicable.



Grant Thornton

www.grantthornton.am

© 2024 Grant Thornton Armenia. All rights reserved.

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton Armenia is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms.

GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.