Insight Assurance

Trusted Risk Advisory Professionals

System and Organization Controls 3 (SOC 3) Report

Report on Pigment's Description of Its Business Planning Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period April 1, 2022, to September 30, 2022

Pigment

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Pigment SAS

Scope

We have examined Pigment's' ('Pigment') accompanying assertion titled "Pigment's Management Assertion" (assertion) that the controls within Pigment's Business Planning Platform were effective throughout the period April 1, 2022, to September 30, 2022, to provide reasonable assurance that Pigment's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

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

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

Service Organization's Responsibilities

Pigment is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Pigment's service commitments and system requirements were achieved. Pigment has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Pigment is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion, that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were

achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Pigment's service commitments and system requirements based on the applicable trust service criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Pigment's service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion, that the controls within Pigment's Business Planning Platform were effective throughout the period April 1, 2022, to September 30, 2022, if complementary subservice organization controls and complementary user entities controls were effective, to provide reasonable assurance that Pigment's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Insight Assurance LLC

Tampa, Florida
December 23, 2022

PIGMENT'S MANAGEMENT ASSERTION

Pigment

PIGMENT'S MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Pigment's ('Pigment') Business Planning Platform throughout the period April 1, 2022, to September 30, 2022, to provide reasonable assurance that Pigment's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Attachment A, titled, "Pigment's Management Description of the Boundaries of its Business Planning Platform", and identifies the aspects of the system covered by our assertion.

Pigment uses a subservice organization to provide hosting services. Attachment A indicates that effective complementary subservice organization controls are necessary, along with controls at Pigment, to achieve Pigment's service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the types of complementary subservice organization controls assumed in the design of Pigment's controls. Attachment A does not disclose the actual controls at the subservice organization.

Attachment A indicates that complementary user entity controls are necessary, along with controls at Pigment, to achieve Pigment's service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the complementary user entity controls assumed in the design of Pigment 's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2022, to September 30, 2022, to provide reasonable assurance that Pigment's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Pigment's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B titled "Pigment's Principal Service Commitments and System Requirements."

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2022, to September 30, 2022, if complementary subservice organization controls and complementary user entity controls were effective, to provide reasonable assurance that Pigment's service commitments and system requirements were achieved based on the applicable trust services criteria.

Pigment SAS

December 23, 2022

ATTACHMENT A

PIGMENT'S DESCRIPTION OF BUSINESS PLANNING PLATFORM

Pigment SAS ("Pigment") is a privately held company established in June 2020 offers Education and Training Technology Services. Pigment is a corporation headquartered in Dover, Delaware.

SERVICES OVERVIEW

PIGMENT BUSINESS PLANNING PLATFORM

Pigment is a SaaS software product that is primarily used to help finance staff to perform business planning by processing financial numbers such as margin, cost and revenues, and model their business processes to inform their decision-making process.

Although this is the primary use for this product, it's a versatile data analysis and modeling platform and users may be using it in different use cases.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of infrastructure, software, people, data, and procedures.

Infrastructure

Pigment maintains a system inventory that includes virtual machines (Google Compute instances), employee computers (desktops and laptops), and networking devices (virtual switches and routers). The inventory documents device name, device type, vendor function, OS, location, and notes

The Pigment application infrastructure is located at Google's data centers. Google acts as a hosting subservice organization (SSO) for the company through the use the Google Cloud Platform. The subservice organization provides the physical security and environmental protection controls, as well as managed services for Pigment's infrastructure.

The SSO's network security uses hardware and software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules. In addition to the firewall, Pigment uses anti-virus and anti-spyware applications to protect systems from viruses.

Pigment's Information Security Policy and security procedures ensure that all computer devices (including servers and desktops) connected to the Pigment network have proper virus protection software (for applicable operating systems), current virus definition libraries, and a vendor-supported version of the operating system with security patches installed. The IT department verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the anti-virus system will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and corporate data. E-mail is scanned and filtered by Google Workspace's e-mail solution. Server operating systems utilize anti-virus and anti-spyware programs when applicable. All employee computers have a minimum standard hardware and software configuration. IT staff maintains several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

Software

Pigment maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. Critical software in use includes the following:

- Google Cloud Platform
- Google Workspace
- Okta
- Slack
- Zendesk

People

The Pigment staff provides support to the above services. Pigment employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the Pigment and its data secure.

Pigment's corporate structure includes the following roles:

Co-Chief Executive Officer (CEO) – Handles the strategic direction of the organization. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments. This role is equally distributed between two individuals acting as a single entity.

Chief of Staff – Acting as a right arm to the co-CEOs, the Chief of Staff coordinates efforts between all teams and provides a buffer between the CEOs and the rest of the team.

Sales - Primary role for outbound reach to prospects and completing sales. They are also responsible for the maintenance and renewals of existing customer contracts.

Technology and Engineering – This role is responsible for the operations of the day-to-day items to maintain the integrity of the environment. This role is also responsible for the provisioning and research and development of new and upcoming services within the company.

Chief Information Security Officer - Reporting to the CEO, this role is responsible for the design, maintenance and implementation an information security governance framework to measure, evaluate and manage organizational risks related to information security

Customer Experience – This role includes the support team and crosses over to the engineering team. It is primarily responsible for daily support aspects of the business. This includes but is not limited to the support of end-users with day-to-day issues, as well as assisting in the onboarding, implementation, and migrations of new and existing customers as part of their ongoing maintenance.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured which is utilized by Pigment in delivering its Business planning Services.

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. All employees and contractors of Pigment are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to Pigment's business and finances are, as a matter of Pigment policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the Client Services and IT Departments. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

Pigment has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. Client data is deleted upon termination of the contract. A ticket is created and assigned to the product team and system engineering team to coordinate the deletion of the data. First, all files received or generated from the client are identified and deleted by the system engineering team then the product team deletes all user-related data.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Passwords protection with assigned user rights is required for access to the network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards in order to obtain the stated objectives for network and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and located within the organization's intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

Human Resources Policies and Procedures

Pigment has formal hiring procedures that are designed to ensure that new team members are able to meet or exceed the job requirements and responsibilities. All candidates go through interviews and assessments of their education, professional experience, and certifications. Background checks are

performed for all newly hired employees before the start date and include a review of their education and past experience references.

During the onboarding process, the new employees review the Employee Handbook, Code of Conduct, and any other relevant policies and procedures relevant to their role. Newly hired employees are required to sign an acknowledgment of receipt and understanding of the Employee Handbook and Code of Conduct. These policies and procedures are also available to employees through the internal policies repository. Security awareness training is also completed at least annually by all employees that include the areas of security and confidentiality to communicate the security implications around their roles and how their actions could affect the organization.

Ongoing performance feedback is provided to all employees and contractors. Formal performance reviews are completed annually by management to discuss expectations, goals, and the employee's performance for the last fiscal year.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Pigment uses a subservice organization to provide hosting services. Management of Pigment receives and reviews the SOC 2 report of GCP on an annual basis. In addition, through its daily operational activities, the management of Pigment monitors the services performed by GCP to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively to meet Pigment's service commitments and system requirements based upon the security, availability and confidentiality trust services criteria.

The assertion indicates that certain applicable trust services criteria can be met only if the Subservice Organizations controls, assumed in the design of Pigment controls, are suitably designed and operating effectively along with related controls at the service organization.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Pigment controls related to the Education and Technology Training Services System only cover a portion of the overall internal controls for each user entity. It is not feasible for the applicable trust service criteria related to the system to be achieved solely by Pigment control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Pigment.

User auditors should determine whether the following controls have been in place in operation at the user organization:

- Controls to provide reasonable assurance that user access including the provisioning and deprovisioning are designed appropriately and operating effectively.
- User entities are responsible for understanding and complying with their contractual obligations to Pigment.
- User entities are responsible for notifying Pigment of changes made to the administrative contact information.

ATTACHMENT B

PIGMENT'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Pigment designs its processes and procedures related to the Pigment's Business planning Services system ("System") to meet its objectives. Those objectives are based on the service commitments that Pigment makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Pigment has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal

Pigment establishes operational requirements that support the achievement of security relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.