AlignOps

SOC 3 Report

July 1, 2023 through June 30, 2024

HANCOCK/DANA

Table of Contents

Section 1 – Independent Service Auditors' Report

HANCOCK/DANA

Independent Service Auditors' Report

To: Management of AlignOps

Scope

We have examined AlignOps' (or Align), formerly known as Align Technologies and Toolwatch Corporation, accompanying assertion titled "Management's Assertion" (assertion) that the controls within the Construction Operations and Safety Reporting Management System (system) were effective throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that Align's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria.*

Service Organization's Responsibilities

Align 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 Align's service commitments and system requirements were achieved. Align has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Align is responsible for selecting, and identifying in its assertion, the applicable trust services 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 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 AICPA. 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the controls were not effective to achieve Align's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Align'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 the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were 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 polices or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Align's Construction Operations and Safety Reporting Management System were effective throughout the period July 1, 2023 to June, 30 2024, to provide reasonable assurance that Align's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

HANCOCK & DANA PC

Hancock & Dana PC

Omaha, NE
November 13, 2024

Section 2 – Management's Assertion

Assertion of the Management of AlignOps

We are responsible for designing, implementing, operating, and maintaining effective controls within AlignOps' (or Align), formerly known as Align Technologies and Toolwatch Corporation, Construction Operations and Safety Reporting Management System throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that Align's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria.* Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that Align's service commitments and system requirements were achieved based on the applicable trust services criteria. Align'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.

Complementary subservice organization controls, along with controls at Align, are used to provide reasonable assurance that Align's service commitments and system requirements were achieved based on the applicable trust services criteria.

Complementary user entity controls, along with controls at Align, are used to provide reasonable assurance that Align's service commitments and system requirements were achieved based on the applicable trust services criteria.

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 July 1, 2023 to June 30, 2024, to provide reasonable assurance that Align's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A – Description of the Boundaries of the Construction Operations and Safety Reporting Management System

Attachment A

Description of the Boundaries of the Construction Operations and Safety Reporting Management System

Services Provided

AlignOps (or Align), formerly known as Align Technologies and Toolwatch Corporation, is a Software as a Service (SaaS) provider delivering an operations management platform, which with a pair of product sets, offers solutions to the construction and non-construction industries. Align unites field, warehouse, and back-office teams on a single platform that drives job site productivity by streamlining operations. Align's platform consists of Construction Enterprise Asset Management (EAM) products in the operations product line, and Safety Reports products, and Align Environmental Health and Safety (EHS), in the safety reporting product line.

The EAM product in the Align System is operated as Software as a Service (SaaS) system deployed on computer desktop, mobile devices, and the third-party hosted cloud environment. Networks are subject to vulnerability management and web application scanning. The primary aim of the system is to enable asset management and operations management through user roles.

Safety Reports products in the Align System are operated as Software as a Service (SaaS) solution deployed in two parts, on mobile devices and the production environment, which is a third-party hosted cloud environment. Networks are subject to vulnerability management and web application scanning. The primary aim of the system is to use elements within any or all seven applications of the product suite, to help manage applicable components of an environmental health and safety program.

Align EHS is an extension of the Safety Reports products, where account and user management are housed within the Align product, and all other functions are managed in the Safety Reports products with Align branding. A single mobile application is used to access products under the Safety Reports umbrella which the Align client has subscribed to. The Align administrative layer provides Align EHS-branded administrative access to the Safety Reports products under the same subscription.

System Architecture and Infrastructure

Align EAM and Align EHS product systems utilize a third-party hosted, cloud-based environment, which function as subservice organizations. The carve-out method has been elected with respect to subservice organizations. Align employs modern, modular architecture. This modular architecture logically breaks apart the platform into smaller pieces that are easier to reason about and change. Each module encapsulates business rules and data, and other modules access or interact with data in a module through limited exposed contact.

The platform is hosted in three separate geographic regions. Managing three separate regions helps to minimize the 'blast zone' in case of issues, helping to avoid a situation where all clusters go down. Customers on the platform may have several Align orgs, but an individual org exists in a single cluster.

The Safety Mobile and Web Applications interact with the Backend Services via web services and form posts over secure HTTPS protocol. The web services are authenticated using a combination of service keys, account and user credentials and carry payloads in JSON format. Safety Backend Services store data in Azure platform services for durable, persistent storage.

All of the Safety Reports apps utilize cross-platform mobile technology that allows a single mobile code base to be compiled to specific platforms. Each of the apps uses a device's internet connection to communicate back to Safety Report's servers via a secure web service architecture. All the apps are paired with an online web portal that provides a dashboard and extensive reporting for the data collected in each app.

Software - Product

The Align product includes three types of software which are part of the system's SaaS offerings.

- Desktop client – allows asset management from an internet-connected PC or Mac computer using a secure web connection.
- Two Mobile applications
    a. Align EAM – allows asset management from mobile devices, using a secure web connection.
    b. Align EHS – provides access to select Safety Reports apps based on account settings, using a secure web connection.
- Cloud-based client – allows asset management from any device, using a secure web connection.

The platform allows access to where data is housed. Based on user role, the person accessing the system can fulfill different functions related to asset management. The third-party complementary services are used to support these applications.

Safety Reports product suite systems utilize remote servers, and Microsoft Azure, a third-party hosted, cloud-based environment.

Safety Reports products include seven software applications:

- Safety Inspection – allows the end-user to perform an inspection based on ad-hoc or checklist-based means, including file attachments, and creates a report which is submitted via email. Application has limited 'offline' capabilities, utilizing temporary local storage.
- Safety Training – allows the end user to perform small group training events using pre-loaded material, track attendance and creates a report submitted via email. Application has limited 'offline' capabilities, utilizing temporary local storage.
- Safety Job Safety Analysis (JSA) – allows the end user to perform task-based job hazard analysis with the industry standard 'Task, Hazard, Control' format created as a report submitted via email; this application also has an audience component. Application has limited 'offline' capabilities, utilizing temporary local storage.
- Safety Observation (Obs) – allows the end user to quickly report negative, positive, or agnostic observations and creates an email, if applicable, based on administrative settings. Application has no 'offline' capabilities.
- Safety Incident – allows the end user to create and send a formalized incident report on one of six incident types via email, including diagrams and file attachments. Application has no 'offline' capabilities.
- Safety Scan – allows the end user to both manage asset attributes through an edit function, and perform an inspection based on 'scanning' of a QR code; this creates an email, if applicable, based on administrative settings. Application has no 'offline' capabilities.
- Safety Forms – allows the end user to fill out a form using content set up by the administrator. Application has no 'offline' capabilities.

People

Align employs a hybrid workforce of full-time US-based staff. Offices are located in Denver, CO and St. George, UT, and some offshore application and system developers on contract. Remote Align employees

are able to ‘work from anywhere’ due to the utilization of browser and/or cloud-based solutions available to respective teams which allow them to perform any task either in, or out of the office.

- Employees managing support of the system fall under the DevOps/Engineering team. The Information Security (InfoSec) team which manages the majority of the controls stated in this report are among this group of staff members.
- Employees managing product support and development fall under the Product team.
- Employees managing client training, product support and implementation fall under the Professional Services team.
- Employees managing outreach, client relationships, sales and marketing fall under the Sales/Client Success and Marketing teams.
- Employees managing Human Resources and/or Finance-related tasks fall under the combination HR/Finance team.
- Executive employees oversee these teams as direct business unit managers or serve as subject matter experts and members of the board of directors.

Data

Data managed in the Align products is mostly entered by either Align staff or the end-user as part of client onboarding, with assets provided with attributes that allow different parts of their management within the system. Data can be edited by the end-users depending on the role they operate out of. Some data in the system comes from third-party integration with outside systems, if so set up by the client account.

Data managed in the Safety Reports product allows data entry through either a mobile or browser-based application. The system has two user roles, application, and administrative user. Data is either entered through use of template uploads by staff, or by the end-user role through use of any of the applications. Data management within the system is managed by the administrator user role. As of the time of this report’s writing, no external system data is imported through integration into the back end managing the Safety Reports products.

Processes and Procedures

Align adheres to its own stated security policies which are owned and managed by the InfoSec team. Policies define accountability and responsibility for evaluating control effectiveness and managing changes based on the needs of the environment. Items addressed include:

- Human Resources
- Asset Management
- Access Control
- Physical Security
- Web Environment/Cyber Security
- Communications Security
- Systems acquisition, development, maintenance, and management
- Supplier and Customer relationships
    - Confidentiality and privacy commitments that are consistent with Align’s commitments are part of written agreements. Vendors and business partners who have access to confidential information have committed to either a Non-Disclosure Agreement (NDA) or similar as deemed appropriate by Management and/or Human Resources. Compliance with such is evaluated through either the risk assessment on a periodic basis, or as needed as part of incident management.
- Incident Management
- Compliance

Attachment B – Principal Service Commitments and System Requirements

Attachment B

Principal Service Commitments and System Requirements

Align designs its processes and procedures related to meeting its objectives for the Construction Operations and Safety Reporting Management System. Those objectives are based on the service commitments that Align makes to user entities, the laws and regulations that govern the provision of the System and the financial, operational and compliance requirements that Align has established for its services.

Security, availability, and confidentiality commitments to user entities are documented and communicated in customer agreements, as well as in the description of the offerings provided on the Align website. Security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

- Security: Align employs a combination of policies and procedures to ensure defensive measures are in place to mitigate the threats of physical security, cyber security, and data/financial security to protect the Company and its customers.

- Availability: Align uses process monitoring to track availability of systems. Data from monitoring is used for executive decision making to gauge sufficiency of staffing and infrastructure, as well as product improvement opportunities.

- Confidentiality: Align utilizes encryption and other relevant security controls and policies to ensure the confidentiality of customer data.

Align establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Align's 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 to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Align System.