bakertilly

Proprietary & Confidential

ADDEPAR

Analytics & Reporting and Navigator Platforms

SOC 3

Relevant to Security, Confidentiality, and Privacy

JULY 1, 2024 TO AUGUST 31, 2025

Table of Contents

I. Independent Service Auditor's Report

Addepar, Inc.
335 Madison Ave, Suite 1430
New York, NY 10017

To the Management of Addepar, Inc.:

Scope

We have examined Addepar, Inc.'s accompanying assertion in Section II titled "Addepar, Inc.'s Assertion" (assertion) that the controls within Addepar, Inc.'s Analytics & Reporting and Navigator Platforms (system) were effective throughout the period July 1, 2024 to August 31, 2025, to provide reasonable assurance that Addepar, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022),* in AICPA *Trust Services Criteria*.

Addepar, Inc. uses Amazon Web Services for data center and network infrastructure services (subservice organization). Addepar, Inc.'s description of the boundaries of its system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Addepar, Inc., to achieve Addepar, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Addepar, Inc.'s controls. The description 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.

Service Organization's Responsibilities

Addepar, Inc. 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 Addepar, Inc.'s service commitments and system requirements were achieved. Addepar, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Addepar, Inc. 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 engagement.

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 Addepar, Inc.'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 Addepar, Inc.'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 policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Addepar, Inc.'s Analytics & Reporting and Navigator Platforms were effective throughout the period July 1, 2024 to August 31, 2025, to provide reasonable assurance that Addepar, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Seattle, Washington
September 30, 2025

ADDEPAR

II. Addepar, Inc.’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Addepar, Inc.’s Analytics & Reporting and Navigator Platforms (system) throughout the period July 1, 2024 to August 31, 2025, to provide reasonable assurance that Addepar, Inc.’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 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, 2024 to August 31, 2025, to provide reasonable assurance that Addepar, Inc.’s service commitments and system requirements were achieved based on the trust services criteria. Addepar, Inc.’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.

Addepar, Inc. uses Amazon Web Services for data center and network infrastructure services (subservice organization). The description of the boundaries of our system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Addepar, Inc., to achieve Addepar, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Addepar, Inc.’s controls. The description does not disclose the actual controls at the subservice organization.

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, 2024 to August 31, 2025, to provide reasonable assurance that Addepar, Inc.’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A - Addepar, Inc.’s Description of the Boundaries of Its Analytics & Reporting and Navigator Platforms

A. System Overview

1. Services Provided

OVERVIEW OF THE OPERATIONS

COMPANY BACKGROUND

Addepar, Inc. (Addepar) is a privately held company, founded in 2009, with more than 1,000 employees and two offices in the United States: New York, New York; Salt Lake City, Utah, along with global offices in London, UK; Edinburgh, UK; Dublin, Ireland; Geneva, Switzerland, São Paolo, Brazil, Dubai, UAE, and Pune, India. Addepar's wealth management platform provides data aggregation, analytics, and performance reporting to enable investors and financial advisors to manage and report financial portfolios. Addepar serves thousands of clients, including leading financial advisors, family offices, and large financial institutions that collectively manage over $7 trillion in assets.

ANALYTICS & REPORTING PLATFORM

Addepar’s Analytics & Reporting Platform assimilates online data from multiple custodial banks into a single format. With Addepar, investment-management professionals at any level—from registered investment advisors to advisors at major private banks—have the power to see precisely where their portfolio stands at any given moment. The platform has the flexibility to cope with the ever-changing landscape of financial data, while remaining intuitive to users across the spectrum of investment management.

NAVIGATOR PLATFORM

Addepar’s Navigator product is a forward-looking portfolio projection tool that allows investors to understand key metrics on a portfolio out into the future. Navigator enables users to simulate different economic scenarios and forecast cash flows across the entire portfolio. These forecasts help investors to determine the level of capital commitment and pacing to apply over time helping to minimize cash drag, meet investment goals and maximize portfolio returns.

SERVICES PROVIDED BY A SUBSERVICE ORGANIZATION

Addepar's Analytics & Reporting and Navigator offerings are hosted in Amazon Web Services' (AWS) cloud infrastructure where all data is access-controlled and encrypted. Amazon provides the data center and networking infrastructure, which Addepar requires, including Amazon's virtual Elastic Compute Cloud (EC2) servers and Amazon's Simple Storage Service (S3) storage capabilities. Other leveraged services include those supporting operational availability, scalability, redundancy, security, and monitoring.

Addepar management has processes to review Amazon's System and Organization Control (SOC) report for security and environmental controls as they impact the Addepar environment. This subservice organization is excluded from the scope of this report.

CORE COMPONENTS

Addepar offers a complete web-based hosted Software-as-a-Service with all clients leveraging the same instance of the software. Through the Addepar and Navigator platforms, companies can leverage Addepar's software for multi-custodian and multi-asset data aggregation, portfolio analysis, and end-client reporting. Addepar's open Rest APIs are used to connect to companies' broader technology stack.

Addepar's Analytics & Reporting Platform has two main technical components: Addepar Data Platform and Addepar Management Platform. These components provide the following functions:

- *Addepar Data Platform (ADP)* – Accepts external data, such as custodian data, third-party market data, and proprietary data sets to conduct extract, transform, and load (ETL) data transformation and data verification checks. ADP utilizes a multi-tier, service-oriented architecture to extract, transform, and load many data sources into a standard format that can then be input into the user-facing portion of the application known as the Addepar Management Platform (AMP). ADP is not in-scope for this SOC 2 report.
- *Addepar Management Platform (AMP)* – Provides the user interface, manages data on the Addepar platform, and facilitates reporting and analysis. AMP uses a multi-tier architecture, including load balancers and front-end web servers. On the back end, Addepar has developed a multi-tier, service-oriented architecture, including services for data processing, on-demand calculations, and API servers for external integrations.

Through the Navigator platform, companies can leverage Addepar's software to optimize investment planning by modeling and projecting portfolio spending, commitments, and distributions over an entire investment cycle.

Navigator has several technical components:

- *Ingestion* – Ingest processing which retrieves ownerships and valuations from Addepar and provides transformations and aggregations into data formats ready for modeling.
- *Modeling* – Provides the user interface for entering assumptions, scenarios, cash flows and other model inputs used in modeling the assets retrieved from the ingestion step.
- *Projections* – Generate forward looking projections, reports, dashboards and downloads. These show cash flows, net asset values, liquidity, allocations and other projected financial markers.

REPORTING

Addepar offer portfolio analysis, risk reporting, data verification, and scalable, customized end-client reporting with capabilities to support multi-currency, across asset classes (marketable securities, alternatives, real assets), and complex ownership and householding structures. This functionality provides advisors and end-clients access to customizable, comprehensive, and scalable client reporting and portal/mobile access. The Analytics & Reporting Platform provides drag-and-drop functionality throughout the native report writer to change charts, fonts, branding, color schema, and asset tables. While the Addepar team will support the users, the platform provides numerous self-service options. The analysis dashboard and reporting function require little user training.

Actions on the platform are logged. Data is on-demand, and a complex multi-page report can be created in a matter of seconds. The user has the flexibility to leverage Addepar's Rest API to send reports downstream to the white-labeled, end-client portal to be rendered to PDF and accessed in Addepar's native mobile application.

2. Infrastructure

Addepar uses the AWS Infrastructure as a Service (IaaS) cloud infrastructure to host Analytics & Reporting and Navigator systems. Amazon provides the data center facilities, servers, and network used for development, staging, and production. Addepar controls the cloud network configuration. Physical and environmental controls for these facilities are described in the Amazon SOC report and reviewed annually by Addepar's Information Security team. Within AWS, Addepar uses the following services for Analytics & Reporting and Navigator services:

- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Kubernetes Service (EKS)
- Amazon Relational Database Service (RDS)
- Amazon ElastiCache
- Amazon Virtual Private Cloud (VPC)
- Amazon Load Balancing (ELB/ALB)
- Amazon Identity and Access Management (IAM)
- Amazon Key Management Service (KMS)
- Amazon Simple Storage Service (S3)
- Amazon Redshift
- AWS Secrets Manager (ASM)

Addepar provisions servers using hardened configurations built by Addepar's Infrastructure Platform team.

Addepar logically separates its production, testing, development, and corporate environments onto dedicated AWS servers. Addepar's production environments are highly secured, and access to it is strictly limited. Other environments are separated from production, with unique access models built around the principle of least privilege; no employee has access to any system or data for which they do not have an approved business need. Client data is completely segmented in a secure way per entity/Addepar client on the same scalable database infrastructure.

3. Software

The Analytics & Reporting and Navigator Platforms are comprised of cloud-hosted server clusters and databases, with a client-facing web portal. Administration tools are used by internal personnel to administer this infrastructure.

Code changes for Addepar are checked into a source code control system in a private repository. Addepar's automated build system is responsible for pulling source code from the source code control system, compiling and building the project, and uploading the build package to Addepar's test and staging environments. Changes are subjected to rigorous security and functionality testing before being advanced to the production environment. Authentication and authorization security checks are enforced throughout the deployment process.

Addepar's software development process delivers updates at semi-monthly intervals. Clients receive notification of new releases within the platform. Addepar software rollouts do not require any local software updates on the end-client part and are performed outside of clients' normal usage hours. There is a regular release schedule.

Patches or updates deemed critical follow an emergency release management process, wherein an update may be made outside of the semi-monthly release cycle. When this occurs, clients are notified as soon as possible, depending on the update's scope and importance.

4. People

The key teams that support the delivery of the Addepar Analytics & Reporting and Navigator Platforms include:

- *Software Engineering* – The Software Engineering team develops the platform and implements new features. Development and testing efforts are performed using discrete environments with anonymized data.
- *Product Engineering* – The Product Engineering team develops the platform and implements new features. Development and testing efforts are performed using discrete environments with anonymized data. The Product Engineering team is also responsible for deploying and maintaining the production, staging, and development environments.
- *Quality Engineering (QE)* – The QE team performs comprehensive automated and manual testing of product features and changes to the Addepar and Navigator codebase, including functional, regression, performance, and stress testing.
- *Engineering Productivity* – The Engineering Productivity team is responsible for deploying and maintaining the Addepar production, staging, development, and testing environments.
- *Core Platform Engineering* – The Core Platform Engineering team is responsible for deploying and maintaining the Addepar production, staging, development, and testing environments.
- *Core Platform Operations* – The Core Platform Operations team is responsible for provisioning and managing infrastructure with a service level agreement (SLA) and numerous tools to permit infrastructure and service management by various Engineering teams.
- *Information Security (InfoSec)* – The Information Security team works across the organization to ensure the confidentiality and integrity of clients' assets. It is responsible for automated and manual security testing, including vulnerability scans, penetration testing, source code reviews, and design reviews. The team provides secure development training for engineers and annual security training for all employees.
- *Services* – The Services team guides clients through the platform onboarding and implementation process, from contract signing to software customization. They assist with data migration and verification and facilitate software training. Services also include the Support team, which addresses active clients' requests and routes them to the appropriate representative.

5. Data

Addepar manages data on its AWS-hosted environment as follows:

- *Addepar Database* – Addepar's central production database uses a MySQL Database Management System (DBMS) to store accounts information and application settings. This database resides in the United States. Access to this system is restricted. Fields within the MySQL database known to contain Personally Identifiable Information (PII) or other data deemed sensitive, are encrypted using 256-bit AES encryption.
- *AMP Servers* – The AMP Server infrastructure is a cloud hosted service with direct access to the AMP database that encapsulates various layers of business logic and exposes Application Programming Interfaces (APIs) via a representational state transfer (REST) API Interface. A set of load-balancers are used for resiliency and redundancy to be fault tolerant. Amazon S3 backed storage with Server-Side Encryption is used for Addepar's document management feature. Data stored in AWS is encrypted at rest using AWS full-disk encryption.
- *Data Ingestion Servers* – A subset of servers is used to process custodian feeds and perform data aggregation. The Addepar Data Operations team performs data verification when necessary, and then data provided by financial custodians is parsed and normalized into a standard format readable by AMP Servers.
- *Addepar Website* – Addepar's corporate website and support portal is hosted on Netlify. It contains an overview of the Company and products, in addition to software packages and a knowledge base site for registered clients.
- *Customer Web Portal* – Part of Addepar's product is a web-based portal, designed to allow Addepar clients, as well as their clients, to access and understand their data.
- *Custodian SFTP* – A Secure File Transfer Protocol (SFTP) service is used by custodians, prime brokers, and fund administrators to upload financial feeds. Addepar requires that all transmitted files are stored in an encrypted format, so that in the event of a system compromise no sensitive data is revealed. Access to this external service is restricted to authorized parties.
- *Navigator Database* – Navigator's central production database uses Amazon RDS managed database services to store accounts information and application data such as ownership information, modeling assumptions and results of projection runs. This database resides in the United States. Access to this system is restricted. RDS DB instances are encrypted at rest using industry standard AES-256 encryption. Connectivity is via encrypted connections. Full backup snapshots are stored nightly and point-in-time restores are kept.
- *Navigator Application Servers* – These servers provide the user interface via web services. Provides the APIs which are used by the front-end browser based React application to update. Resilience is provided by Amazon AWS application load balancers.
- *Navigator Simulation Servers* – These servers provide background processing such as ingest processing, simulation run pipelines and scheduled services.

COLLECTIONS OF PERSONAL INFORMATION

Addepar collects personal information that users provide in various ways through the Addepar website and platform services. These include the following:

- *Login Credentials* – Login credentials are required to access Addepar services.
- *Communications* – If you contact Addepar by email, using the inquiry contact form on the Addepar website or by postal mail or other means, personal information is collected and associated with the communication.

Addepar collects personal information uploaded to the Analytics & Reporting and Navigator Platforms by users who are paid subscribers of the Services for processing on their behalf. This is "Customer Data." This information may include information about a client's customers, such as name, email address, and financial account data, to perform wealth management services for those customers via the Services. Addepar users may electronically submit customer data to the services or instruct third parties (including custodians) to do so. Addepar may access customer data in accordance with the license agreement between Addepar and the user and subject to applicable law.

AUTOMATED INFORMATION COLLECTION

When a client uses Addepar's services, some information is collected automatically. This includes automatically collecting the client's browser Internet Protocol (IP) address, the browser type, the nature and identification of the device being used to access the Addepar service, the website that was visited immediately before accessing any web-based Services, and the actions and content taken on Addepar's Services.

Addepar may collect this information automatically using technologies such as standard server logs, cookies, and web beacons. A "cookie" is a text file that websites send to a visitor's computer or other Internet-connected devices to uniquely identify the visitor's browser or to store information or settings in the browser. A "web beacon," also known as an Internet tag, pixel tag, or clear GIF, links web pages to web servers and their cookies and may be used to transmit information collected through cookies back to a web server. Addepar uses automatically collected information to administer, operate, and improve services and to improve marketing effectiveness.

Further information may be referenced in Addepar's Privacy Policy located on Addepar's website.

6. Processes and Procedures

Addepar policies that apply to Company personnel are published internally. Engineering procedures are also posted. Access to the entire knowledge base is restricted to logged-in employees using their corporate credentials via Single Sign-On (SSO). During the onboarding at Addepar, personnel must review and acknowledge the Addepar Business Conduct and Ethics Policy, Employee Handbook, and Security Training materials.

INFORMATION SECURITY

Information Security Policies and their supporting processes are developed to manage cybersecurity risk to systems, people, assets, data, and capabilities. Addepar's policies and controls focus on five activities:

- *Identify* – Develop organizational activities to support cybersecurity identification and risk mitigation efforts.
- *Protect* – Develop and implement adequate safeguards to ensure the delivery of critical services. This includes supporting the ability to limit or contain the impact of a potential cybersecurity event.
- *Detect* – Develop and implement adequate activities to identify the occurrence of a cybersecurity event.

- *Respond* – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- *Recover* – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

B. Complementary Subservice Organization Controls

Addepar, Inc.'s controls related to the Analytics & Reporting and Navigator Platforms cover only a portion of overall internal control for each user entity of Addepar, Inc. It is not feasible for the criteria related to the Analytics & Reporting and Navigator Platforms to be achieved solely by Addepar, Inc. Therefore, each user entity's internal controls must be evaluated in conjunction with Addepar, Inc.'s controls, taking into account the types of controls expected to be implemented by the subservice organization as described below.

Complementary Subservice Organization Controls	
Amazon Web Services	
1	Access to the physical facilities housing hosted systems is restricted to authorized users.
2	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
3	Environmental mechanisms provide protection over fire, water, power outages, temperature changes and natural disasters.

C. User Entity Responsibilities

There are no controls at the user entity that are necessary, in combination with Addepar, Inc.'s controls, to provide reasonable assurance that Addepar, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria (complementary user entity controls).

There are, however, certain responsibilities that users of the system must fulfill for the user entity to derive the intended benefits of the services of the Analytics & Reporting and Navigator Platforms. The user entity responsibilities presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities are responsible for their own control environments and their operational effectiveness.

User Entity Responsibilities	
1	Ensuring that financial feeds are accurate, complete and uploaded in a timely manner, and ensuring timely notification to custodians and data providers to cease sending financial data that are no longer needed for the Addepar service.
2	Immediately notifying Addepar of any actual or suspected information security breaches, including compromised user accounts.
3	Enforcing a strong password policy and two-factor authentication, where available. Each Addepar platform account is required to have a password of at least eight characters. The password must contain at least three of the four following character classes: • Lower case characters • Upper case characters • Numbers • Punctuation and special characters During the first login, users are forced to change their temporary password. Optionally, clients can enforce password aging.
4	Determining which users should be granted access to the system, for verifying permissions periodically, as well as the timely removal of users who no longer require access to the system.
5	Ensuring that changes to authorized personnel are communicated to Addepar in a timely manner.
6	Ensuring the secure transmittal of data to Addepar.
7	Ensuring that any reports or data output from the system are maintained in accordance with their internal or client requirements and applicable law.

Attachment B – Principal Service Commitments and System Requirements

Addepar's principal service commitments are based on the services described in this document. The service commitment is to provide and secure Addepar's cloud-based enterprise software supporting the Analytics & Reporting and Navigator Platforms for investment management professionals.

Addepar's service commitments are documented in its contracts with users. Among other items, they include protecting user data by maintaining a security program designed to maintain data security and integrity and prevent unauthorized access.

These commitments are reflected in Addepar's internal policies and processes and affect how Addepar's system is designed, developed, and operated.

.