A-LIGN
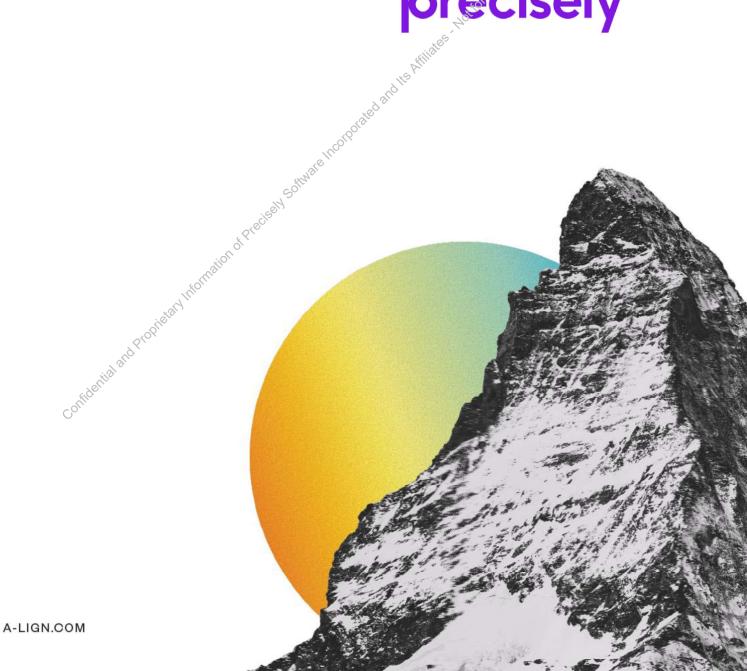
Precisely Software
Incorporated

Type 2 SOC 3

2023

precisely

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2023 to December 31, 2023

Table of Contents

SECTION 1

ASSERTION OF PRECISELY SOFTWARE INCORPORATED MANAGEMENT

ASSERTION OF PRECISELY SOFTWARE INCORPORATED MANAGEMENT

March 15, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Precisely Software Incorporated's ('Precisely' or 'the Company') Data Integrity and Analysis Software as a Service (SaaS) System throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Precisely'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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Precisely Software Incorporated's Description of Its Data Integrity and Analysis SaaS System throughout the period January 1, 2023 to December 31, 2023" 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 January 1, 2023 to December 31, 2023, to provide reasonable assurance that Precisely's service commitments and system requirements were achieved based on the trust services criteria. Precisely'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 "Precisely Software Incorporated's Description of Its Data Integrity and Analysis SaaS System throughout the period January 1, 2023 to December 31, 2023".

Precisely uses Amazon Web Services ('AWS') and Microsoft Azure ('Azure') to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Precisely, to achieve Precisely's service commitments and system requirements based on the applicable trust services criteria. The description presents Precisely's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Precisely's controls. The description does not disclose the actual controls at the subservice organizations.

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

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 January 1, 2023 to December 31, 2023 to provide reasonable assurance that Precisely's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Precisely's controls operated effectively throughout that period.

Diane Ferguson

_____

Diane Ferguson
VP, Deputy General Counsel
Precisely Software Incorporated

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Precisely Software Incorporated

Scope

We have examined Precisely's accompanying assertion titled "Assertion of Precisely Software Incorporated Management" (assertion) that the controls within Precisely's Data Integrity and Analysis SaaS System were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Precisely'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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Precisely uses AWS and Azure 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 Precisely, to achieve Precisely's service commitments and system requirements based on the applicable trust services criteria. The description presents Precisely's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Precisely'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 organization controls.

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

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

Our examination included:
- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

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

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 Precisely's Data Integrity and Analysis SaaS System were suitably designed and operating effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Precisely's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Precisely's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Precisely's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Precisely, user entities of Precisely's Data Integrity and Analysis SaaS System during some or all of the period January 1, 2023 to December 31, 2023, business partners of Precisely subject to risks arising from interactions with the Data Integrity and Analysis SaaS System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE
_____
Tampa, Florida
March 15, 2024

SECTION 3

PRECISELY SOFTWARE INCORPORATED'S DESCRIPTION OF ITS DATA INTEGRITY AND ANALYSIS SAAS SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2023 TO DECEMBER 31, 2023

OVERVIEW OF OPERATIONS

Company Background

Precisely is a global leader in data integrity, providing accuracy, consistency, and context in data. The company empowers organizations worldwide, including 99 of the Fortune 100, to deliver trusted data to drive more confident business decisions.

With decades of deep domain expertise and a unique combination of software, data, and data strategy services, Precisely addresses today's data challenges and enables over 12,000 global organizations to maximize strategic opportunities. Precisely's comprehensive solutions for data integration, data quality, data governance, location intelligence, and data enrichment enable customers to trust their data for business decision making, analytics, and AI.

Businesses across many industries use Precisely's data integrity capabilities, including financial services, telecommunications, healthcare, media and communications, retail, public utilities, government and insurance. Precisely's product and services revenue base has grown significantly in the last several years. However, Precisely is a privately held company and does not disclose specific financial information. Precisely has approximately 2500 team members globally and is headquartered out of Burlington, MA, with offices in the United States, United Kingdom, France, Germany, Poland, India, Japan, and Australia.

The company was founded in the state of New Jersey in 1968 under the name, Whitlow Computer Systems. The company changed its name in 1981 to Syncsort to align its identity with its flagship mainframe product. In 2013, Syncsort acquired Circle Computer Group. They subsequently acquired William Data Systems in 2015. In 2017, Centerbridge Partners acquired Syncsort along with Vision Solutions and combined the two companies. In 2019, Syncsort acquired the software and data business of Pitney Bowes backed by Centerbridge Partners and Clearlake Capital Group. In May 2020, Syncsort rebranded itself as Precisely to improve brand identity. In March 2021, Clearlake Capital Group, in affiliation with TA Associates, re-acquired Precisely and Centerbridge Partners retained a minority stake. In 2021, Precisely acquired leading data quality and data governance companies, Infogix and WinShuttle, as well as data vendor, AnchorPoint. In 2022, Precisely acquired SaaS CCM vendor, CedarCX, and data vendor, PlaceIQ. Also in 2022, Insight Partners and Partners Group joined existing ownership as institutional investors in Precisely. In 2023, Precisely acquired Transerve, a location intelligence and data provider with expertise in spatial data handling, processing, and analysis.

Description of Services Provided

Precisely provides software (on-premises & SaaS), support, data products, professional / managed services and strategic services that allows businesses to make more confident decisions based on data that is trusted to have maximum accuracy, consistency, and context.

Twelve main product groups comprise the breadth of Precisely SaaS offerings: Precisely Data Integrity Suite, Trillium Cloud Platform, Spectrum OnDemand (SPOD), Spectrum Spatial Analyst / Insights (SSA/SSI), Precisely Application Programming Interface (API)s / Developer Hub, Precisely Data Experience (PDX), Precisely Automate (Evolve, Studio & Studio Manager), Precisely EnterWorks, GeoTax, MapMarker Online, Data360, and advanced controls products.

Data Integrity Suite

The Precisely Data Integrity Suite connects a comprehensive set of flexible, interoperable data integrity cloud services through its shared data catalog, machine learning-powered intelligence, and agents that enable workloads to run where their data resides. The Suite's cloud services span the data integrity management lifecycle, including Data Integration, Data Governance, Data Observability, Data Quality, Geo Addressing, Spatial Analysis, and Data Enrichment.

The Data Integrity Suite's cloud services can be deployed independently or in combination. They are built on proven Precisely technology, integrate with the Precisely portfolio of products, and work seamlessly with both traditional and modern tech stacks.

- The Data Integration service allows customers to break down data silos by quickly building modern data pipelines that drive innovation.
- The Data Observability service allows customers to proactively uncover data anomalies and act before they become costly downstream issues.
- The Geo Addressing service allows customers to verify, standardize, cleanse, and geocode addresses to unlock valuable context for more informed decision-making.
- The Data Quality service allows customers to deliver data that's accurate, consistent, and fit for purpose across operational and analytical systems.
- The Data Governance service allows customers to manage data policy and processes with greater insight into their data's meaning, lineage, and impact.
- The Data Enrichment service allows customers to enrich their business data with expertly curated datasets containing thousands of attributes, enabling faster, more confident decisions.
- The Spatial Analytics service allows customers to derive and visualize spatial relationships hidden in their data to reveal critical context for better decisions.

The Suite's Data Integrity Foundation enables the combination of capabilities in ways that were not previously possible. The foundation allows for the sum of the cloud services to be much greater than its parts. The Data Integrity Foundation connects the cloud services through the following components:

- A shared data catalog enables the metadata gathered by one service to be shared and built upon by other services
- Intelligence that uses observations, AI/ML-derived insights, and data integrity process automation to streamline and accelerate user workflows
- Agents that allow the user to design data integrity workloads in the cloud and run them in the cloud, on-premises, or in hybrid environments

The Data Integrity Suite is delivered through a modern SaaS-based delivery model. The Data Integrity Suite's innovative hybrid SaaS architecture is underpinned by 5 common platform services: Encryption Service, Key Service, Notification Service. Audit Service, and SaaS Agent.

Trillium Cloud Platform

Trillium is a versatile, powerful data quality solution that supports rapidly changing business needs, data sources and enterprise infrastructures - including big data and cloud. Its data cleansing and standardization features automatically understand global data, such as customer, product, and financial data, in any context making preformatting and pre-processing unnecessary.

Trillium services deploy in batch or in real-time, using the same rule sets and standards across an unlimited number of applications and systems. Open APIs let users connect to custom and third-party applications, while controlling and managing data quality services centrally from one location. In addition, users can apply global verification rules built from local, country-by-country databases, and apply the appropriate country's postal rules to clean and correct name and address data.

Trillium has been designed to run natively in cloud or on-premises big data environments, ensuring business information is integrated, fit-for-purpose and accessible across the enterprise, regardless of volume. It features optimized native processing that leverages the high-performance computing power of distributed big data frameworks including Hadoop MapReduce and Spark to process high volumes within targeted time windows to meet critical Service Level Agreements.

Users can visually build and locally test rule-based data quality projects and deploy them to run automatically anywhere in data pipelines and real-time applications. Using Intelligent Execution technology, data quality processing is dynamically optimized at run-time, based on the chosen computer framework and available resources. No design changes or tuning are required, even if frameworks change.

Users access the platform through real time web services via APIs, including Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). Batch files uploaded to the Simple File Transfer Protocol (SFTP) server are processed by Precisely and the results downloaded by users from the SFTP server. Trillium Platform client software is utilized to manage the scheduled job processing. Users can also access the system via web browser and access Trillium Admin and Discovery Center.

Spectrum OnDemand (SPOD)

Spectrum OnDemand is a SaaS platform that enhances data management and enrichment through agile, customizable services focused on location intelligence and customer information. Its features include:
- Address verification to ensure accuracy and eliminate duplicates
- Address enrichment with e-mail and phone validations; household, purchase, and other demographics; and social media insights into interests, education, employment
- Enhancement of applications and workflows with location-based data

The platform offers flexible integration with existing applications via APIs, including SOAP, REST, and SDKs, facilitating both real-time and batch processing for various data sources. Users can interact with the services through web services, an SFTP server for batch processing, and an online portal for easy access and management.

Spectrum Spatial Analyst (SSA) / Spectrum Spatial Insights (SSI)

Spectrum Spatial is a powerful Location Intelligence solution. Integrate Location Intelligence into any workflow and customize experiences to drive more efficient, enlightened decisions. With its open data standards, interoperability and scalable, omnichannel visualization, Spectrum Spatial makes it easy to operationalize geospatial data. Integrate, access, manage and enrich data and benefit from the flexibility of an SOA-compliant solution architecture for geoprocessing. With Spectrum Spatial, a user can move from restrictive software and data challenges to sharing data and empowering users to create insights.

Spectrum Spatial makes it easy to embed geospatial rules, logic and visualization into existing operational systems and workflows. It brings industrial-strength Location Intelligence to straight-through processing and enables self-service applications, all uniquely aligned to business needs. Senior management, data scientists, business analysts and customers will all find Spectrum Spatial simple to use. Intuitive functionality brings advanced analysis to any desktop, website, tablet or mobile need. Users can easily access, update and visualize, anywhere, anytime; fulfill mapping requests; and share data with co-workers, citizens, customers and partners.

Spectrum Spatial Insights, a web-based extension, enables users to easily create, manage, and share analyses, maps, and reports, leveraging internal and external data sources without requiring extensive training. This robust platform simplifies data management and enhances enterprise-wide insight. It is particularly useful for site performance analysis / sales forecasting.

Precisely APIs / Developer Hub

Precisely APIs empower users to build innovative verification and location-based applications for multiple platforms (including both web and mobile). Developers can use location data to develop innovative apps for commercial and consumer markets or incorporate the data into everyday applications, business processes, and workflows. Key capabilities and features allow the user to:
- Add millions of global commercial and retail businesses, and landmark points-of-interest to business processes and workflows.
- Add lifestyle and demographic insights to location data.
- Add autocomplete address search into applications and websites.
- Enrich address with points of interest and place names.
- Integrate local tax rates into billing, commerce, payments as well as payroll applications, business processes and workflows.

- Base maps for visualization.
- Create smart drive-time and drive distance.
- Capture detailed property information for analysis, planning, and decisions.
- Routing directions for single or multiple origin & destination inputs.
- Examine local crime, earthquake, flood, and fire risks.
- Locate IP addresses, landline devices, and Wi-Fi Access Points.
- Standardize and validate mailing addresses, return city and state or province name for a given input postal code, and conversely also look up the postal code for a particular city.
- Validate e-mail addresses and identify problematic e-mail addresses.

The SDKs can help the user get started quickly and easily. Code for generating OAuth token for authentication using accounts' API Keys and Secrets is also included in all the following SDKs: Node.js SDK, Android SDK, iOS SDK, Java SDK,.Net (C#) SDK, and JavaScript SDK (Only for Maps API).

Precisely Data Experience (PDX)

PDX (formerly the Software Data Marketplace or SDM) is where end-users may access and download Precisely datasets and software. For convenience, this may be accessed through the "Precisely Data Experience" link on the support homepage.

Choosing precise and accurate data to fulfill client business requirements can be overwhelming, time-consuming, and ultimately costly. Registration to the Precisely Data Experience grants access to the largest single repository of global location data in the cloud providing hundreds of accessible and format-specific data set. Software delivery of available licensed packaged product can also be affected through the PDX.

Precisely Automate (Evolve, Studio and Studio Manager)

Precisely Automate Evolve is the only process automation platform specifically designed to digitize strategic SAP data processes like product launches, customer and vendor onboarding, GL account setup, plant maintenance, and more. Automate Evolve brings together enterprise-grade process automation, robust data stewardship, and deep SAP integration capabilities, with a no-code, low-code approach to solution design. This unique combination enables organizations to digitize strategic data processes faster and at scale-directly supporting critical digital transformation initiatives.

Key Features include:
- Enterprise-grade workflow and automation
- Robust data stewardship
- Deep SAP integration
- No-code, low-code solution design

Precisely Automate Studio simplifies data extracts and reporting from SAP to avoid cumbersome, and error-prone manual methods. With Automate Studio, the user can create and manage SAP records, develop ad-hoc reports from real time SAP data and has the flexibility to select data from multiple SAP tables, infosets or logical databases in order to get the exact data needed for the client's task. For even greater flexibility, Automate Studio has the ability to schedule queries and map data to multiple file types, including Excel and Access, giving the user the freedom to create the reports needed to build a report, or complete their data management task.

The Direct functionality in Automate Studio is designed to leverage built-in SAP APIs, or remote function modules to improve automation performance. In addition, Automate Studio can also use BAPIs for SAP data creation, extraction, and updates. These direct capabilities deliver superior performance for dedicated SAP business and IT teams where the automated process is less dependent on business users and requires faster, more consistent performance.

Key features fall into four categories:

- Data Creation: Creating new master data (materials, vendors, customers, etc.) or transactional data (journal vouchers, invoices, etc.) in SAP systems.
- Data Maintenance and Transformation: Mass changes to SAP data throughout the customers ERP system for activities ranging from vendor updates to pricing changes and more.
- Data Migration: Loading legacy systems data into SAP applications during initial SAP implementation or for M&A activity and migrating data from SAP ECC to SAP S/4HANA.
- Data Integration: Loading Excel data from other sources into the SAP ERP system or from SAP to other systems. Data such as vendor invoices or bank statements.

Automate Studio Manager is a powerful administration and governance platform for Automate Studio licenses. It enables granular control over who can do what with Automate Studio software, share content, assign licenses, execute jobs from the server, and much more.

Schedule and execute jobs from the server:

- Set policies like the number of records and transactions allowed and monitor job progress from within Automate Studio Manager
- See at a glance who did what and when with Automate Studio and quickly get to the underlying data files exchanged with SAP
- Report on KPIs using Automate Studio Manager
- Use out-of-the-box and custom reporting to view:
  - Time and cost savings
  - Records processed by transaction
  - Process status
  - Active users
  - Data errors and more
  - Key Benefits
  - Store and manage content centrally
  - Approve scripts prior to use
  - Assign and manage WinShuttle licenses
  - Enforce governance through roles management
  - Get ROI, SLA, and usage reports
  - Enable approval step before data is posted
  - Run audit reports to compliance requirements
  - Set granular policies for data exchanges with SAP
  - Manage SAP and other data connections
  - Schedule server-side SAP data exchanges

Connect is an online licensing component service that supports the platform.

EnterWorks

Precisely EnterWorks is an enterprise-grade multi-domain master data management solution that can be adapted to any domain including specific capabilities to address Product Information Management (PIM) and Digital Asset Management (DAM)use cases. Precisely EnterWorks integrates enterprise databases and applications to create a "golden record" for strategic data assets across systems to enable timely and accurate decision-making.

Acting as the single source of truth for master data, Precisely EnterWorks allows the user to synchronize and syndicate trusted data and content to systems and channels all from a single platform. More than traditional master data management, Precisely EnterWorks provides the information and tools needed to drive incremental revenue, reduce costs, and transform digital initiatives into a competitive advantage. And its no-code, low-code design empowers business and data teams to accelerate processes and improve data quality across multiple domains, including product, customer, vendor, material, and location, without sacrificing functionality.

Product Information Management (PIM)

Precisely EnterWorks can be used to aggregate and manage product content across all business applications, creating seamless and differentiated experiences that drive business. A hub for more than just product content, EnterWorks empowers business teams to glean product intelligence from their customer, location, sales, and other data. With this insight, they can craft compelling, contextual product offers and content that drive better customer experiences and incremental revenue. EnterWorks' core automation, syndication, and data quality, combined with state-of-the-art AI/ML, print automation, and portal technologies, enable business teams to work both smarter and faster. With this edge, they can make products easier to find and deliver tailored, on-brand content that turns shoppers into customers directly or through channel partners.

Multi-domain Master Data Management (MDM)

Precisely EnterWorks can also integrate enterprise databases and applications to create a "golden record" for strategic data assets across systems to enable timely and accurate decision-making. Acting as the single source of truth for master data, EnterWorks allows the user to get trusted data and content to the systems and channels all from a single platform. More than traditional master data management, EnterWorks provides the information and tools needed to drive incremental revenue, reduce costs, and transform digital initiatives into a competitive advantage. And its no-code, low-code design empowers business and data teams to accelerate processes and improve data quality across multiple domains, including product, customer, vendor, material, and location, without sacrificing functionality.

Digital Asset Management (DAM)

Automatically generate versions of content across multiple applications with Precisely EnterWorks to maintain cross-channel consistency, both in print and online. By integrating full-featured DAM capabilities, EnterWorks makes it easy to manage any unstructured content, including images, videos, audio, documents, and templates. With a central repository for enterprise-wide digital assets and data, the user can streamline storing, categorizing, and managing product-related files and information. Teams can import metadata from images, configure custom fields for cross-selling and up-selling, and automatically generate multiple image formats and resolutions for print and online use. As an all-in-one DAM and data hub, EnterWorks allows the user to link products, items, brands, assets, and other criteria. These data relationships are bi-directional, meaning users can quickly determine which products are associated with a specific document or file to make agile business decisions.

Workflow and Collaboration

Deploy a robust set of workflow management tools with Precisely EnterWorks to enable, automate, and enforce best practices in data and content integration and flow across multiple sources, applications, and enterprises. EnterWorks allows the user to set data governance rules, create multiple routings and alerts, and audit data and user activity to ensure accountability and compliance with established policies. Combine profiling and attribute management tools to monitor, analyze, and improve master data. With EnterWorks, the user can standardize and validate data and gain continuous insight into its completeness and quality. The user can utilize a drag-and-drop interface to manage complex business processes and streamline collaboration between business and technical users, both internal and external, as well as view the activity flow graphically and create alerts and workflows for proactive management and intervention.

GeoTax

GeoTax supports any consumer or business in the United States of America (USA) to determine local tax jurisdictions and tax rates based on address inputs. This product also corrects and standardizes the provided address rapidly. For the system to return the proper information the user must at least enter an Address and either the City and State or the ZIP Code. The tax rate report provides the address found and the sales tax rate listed by jurisdiction. Addresses that do not geocode at a high level of confidence are identified and flagged for further research.

MapMarker Online

MapMarker is an online batch geocoding service that assigns geographic coordinates to address records or returns an Address for a given X, Y(longitude and latitude) coordinates. MapMarker features and capabilities include:
- Multiple subscription plans to choose from including a free trial.
- Support of multiple input and output file formats.
- File templates to help create an input address record file.
- Support of an input address record file that contains addresses or Latitude/Longitude from multiple countries.
- Options to customize input fields for matching.
- Worldwide geocoding coverage.
- Return of the most accurate geocode available for every address.
- Supplied streets and points global reference data.
- Address cleansing and standardized address output.
- E-mail notification when geocoding job completes.
- Administrator and user account management functions.

Precisely Data360

At the core of Precisely Data360 are data ingestion, preparation, analysis, visualization, workflow, and collaboration capabilities enabling business users to quickly visualize and intuitively drill down into data sets. Precisely Data360 also enables users to remediate and track issues with intelligent workflows. Users can easily collaborate across communication silos to answer questions and expedite resolutions. Business users will rejoice in being able to use simple drop-down menus to perform many tasks that often require Structured Query Language (SQL)/R/Python scripting.

Precisely Data360 DQ+

Improve analytical outcomes and big data adoption with high volume data quality checks such as data profiling, consistency, conformity, completeness, timeliness, reconciliations, visual data prep, and machine learning to foster end-user trust by verifying the quality big data. Eliminate the need for multiple tools by aggregating data from disparate sources; pinpointing data of interest to perform data quality checks, aggregations, and transformations; evaluate and review data quality; and combine and correlate data from different sources using a visual data prep process.

Apply machine learning algorithms with intuitive drag-and drop functionality to conduct ad-hoc analysis - segmentation, classification, regression, recommendation, and forecasting across many nodes for faster execution. The power of Data360 DQ+ capabilities enhances data quality checks by applying analytical analysis based on machine learning algorithms to continuously improve data quality automation not possible with other tools.

Precisely Data360 Govern

Data 360 Govern allows customers to manage data policy and processes with greater insight into their data's meaning, lineage, and impact. Define and collaborate on business and technical data assets with clearly defined data definitions, rolling up quality metrics from Precisely data quality products and other third-party data quality tools, extracting technical data lineage to transform it into business lineage with the enhanced capability to perform impact analysis across the data supply chain.

Precisely Data360 Analyze

Through its intuitive drag and drop interface, Data360 Analyze allows users to access virtually any data source from legacy systems to NoSQL platforms and easily acquire and parse that data in a fraction of the time. All users can visually collaborate as they extract, prepare, and analyze data from unrelated sources and create a comprehensive source for analysis without incurring the infrastructure costs and time required by traditional warehouses and extract, transform, load (ETL). Data360 Analyze automates data blending and cleansing, as native functions allow users to profile, aggregate, correlate and transform selected data. The solution also features collaborative feedback loops between IT and business users to promote cooperation, fast communication, and ensure that changes don't derail the entire analysis process.

Advanced Controls Products

Precisely advanced controls products combine with the platform to offer increased functionality, visibility, and options for Precisely customers. Precisely advanced controls products provide enhanced functionality for more advanced use cases, such as monitoring data with highly complex formats and analyzing high volumes of data for fraudulent behavior.

Precisely Assure DQ

Precisely Assure verifies, balances, reconciles, and tracks data within highly complex, data intensive business environments.

Precisely ACR

Precisely ACR provides an organization with accurate, consistent, and reliable data integrity in high volume, mainframe, or host-based environments.

Precisely ER

Precisely ER provides reconciliation and case management to streamline workflows.

Precisely Insight

Precisely Insight provides the dashboards that roll up a series of business rules into logical groups to monitor the performance of a process.

Precisely Perceive

Precisely Perceive provides real-time enterprise data management and reporting.

Precisely NetMind

Precisely NetMind is an enterprise class risk and fraud management solution for traditional wireline, wireless (pre- and post-paid), voice over internet protocol (VoIP), data, cable, and next generation networks, protecting any mix of voice, data, messaging, internet protocol television (IPTV) and M-Commerce services.

Precisely provides its enterprise software either on-premises or via cloud deployments. For cloud deployments, Precisely offer SaaS that can be fully accessed and configured by the customer. This offering reduces the total cost of ownership for customers because there is no additional hardware to purchase, the solution is scalable, upgrades and patches are conducted by Precisely, and it leverages industry leading security controls. Precisely Professional Services provides organizations access to trained and certified Precisely resources, operational stability, best practices, standards, processes and more. Precisely offers technical and functional support of its software through its dedicated Support function. Through Precisely Managed Services, customers are able to have a completely proactively managed solution operated by Precisely professionals.

The Precisely Strategic Services team can partner with the customer to define the strategy, business case, and metrics that will deliver defined outcomes. With a focus on the customer's unique objectives, they will leverage Precisely's technology capabilities, but also look at people, processes, and performance metrics:

Data Integrity Suite	Trillium	Spectrum	Precisely API / Developer Hub	Precisely Data	WinShuttle	Infogix
Data Integrity Suite	Trillium Cloud Platform	SPOD	Precisely APIs	PDX	Automate (Evolve, Studio, and Studio Manager)	Data360 (Govern, Analyze, and DQ+)
		SSA / SSI	GeoTax		EnterWorks	Advanced Controls (Assure, ACR, ER, Perceive, NetMind and Insight)
			Mapmaker Online			

Principal Service Commitments and System Requirements

Precisely designs its processes and procedures related to its Data Integrity and Analysis SaaS Services to meet its objectives for its Data Integrity and Analysis SaaS Services. Those objectives are based on the service commitments that Precisely makes to user entities, the laws and regulations that govern the provision of its Data Integrity and Analysis SaaS Services, and the financial, operational, and compliance requirements that Precisely has established for the services. The Data Integrity and Analysis SaaS Services of Precisely are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as supranational, national, and state privacy security laws and regulations in the jurisdictions in which Precisely operates.

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 offered provided online. Security commitments are standardized and include, but are not limited to, the following:
- Security principles within the fundamental designs of the Data Integrity and Analysis SaaS 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.

Precisely establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Precisely's system policies and procedures, system design documentation, and contracts 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 Data Integrity and Analysis SaaS Services.

Components of the System

Infrastructure

Primary infrastructure used to provide Precisely's Data Integrity and Analysis SaaS System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Virtual Network Services	AWS Virtual Private Cloud (VPC) Azure VPC	Provides secure segmented network architecture including Virtual Private Network (VPN) termination and proxy access to other AWS/Provider services. Forwards data based on multi-layer rules
Kubernetes Services	Amazon EKS	Provides K8S node instances
Application Servers	Amazon AWS EC2 Microsoft Azure Virtual Machines	Provides virtualized server instances
Compute Clusters	Amazon AWS Elastic Map Reduce (EMR) Microsoft Azure Databricks	Provides scalable compute clusters for job processing
Database Servers	Amazon AWS Relational Database Service (RDS) Microsoft Azure Database for PostgreSQL Microsoft Azure Database for SQL	Provides virtual Oracle, SQL, and Postgres database server platforms
Database Service	Amazon AWS DynamoDB Microsoft Azure SQL Database as a Service (DBaaS) Microsoft Azure CosmosDB MongoDB Atlas	Provides virtual DBaaS NoSQL database platform Provides SQL database as a service

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Data Warehouse	Amazon AWS Redshift Microsoft Azure SQL Data Warehouse	Provides data warehouse services
Scaling Engine	Amazon AWS Elastic Beanstalk Microsoft Azure Processor App Service	Provides automatic deployment scaling of web workloads
Search Service	Microsoft Azure ElasticSearch	Dynamic search function
Directory Federation Service	Microsoft Azure Active Directory (AD) Microsoft Azure Client Federation Service Okta	Internal directory and Security Assertion Markup Language (SAML) integration services including Multi-Factor Authentication (MFA)
Load Balancer	Amazon AWS Application Load Balancer (ALB) Amazon AWS Elastic Load Balancing (ELB) Microsoft Azure Load Balancer	Provides application-sensitive automatic application traffic balancing and automatic network traffic balancing
Application Firewall	Amazon AWS Web Application Firewall (WAF) Microsoft Azure WAF Signal Science WAF	Provides web application vulnerability detection and filtering
Storage System	Amazon AWS S3 Microsoft Azure Blob Storage Microsoft Azure Data Lake Storage	Provides encrypted storage volumes and backup targets
Communication	Microsoft Azure Service Bus	Provides encrypted communication between stack components
Logging	AWS CloudTrail AWS CloudWatch	Log Aggregation and Correlation
Hypervisor and System / Network Manager	Amazon AWS Console Microsoft Azure Console	Provides management interface for all AWS and Azure services
Common Application Core Services	Precisely CAS	Provides access authorization and other core services to some applications
Onboarding	Precisely Embark	Provides onboarding services for PDX
Management UI	Precisely PDT	Management Platform

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Security	AWS GuardDuty AWS ControlTower AWS Inspector AWS SecurityHub	Security configuration and posture management
Feature Management	LaunchDarkly	Provides feature and version management services
API Management	Google Apigee	API Gateway
Address Data Source	Precisely Verimove Access	Provides Postal Address Change Data
Licensing	Precisely Connect	Provides licensing and entitlement services
File System Services	Amazon EFS	Provides scalable file system services

Software and Services

Primary software and services used to provide Precisely's Data Integrity and Analysis SaaS System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Precisely Data Integrity Suite	Linux, Kubernetes	Data Integrity Software
Precisely Trillium	Linux	Data Quality Software
Precisely Spectrum	Linux	Data Enrichment Software
Precisely APIs	Linux	Developer APIs and SDKs
Precisely Data Experience	Linux	Data and Software Fulfillment Portal
Precisely Automate Evolve and Automate Studio	Windows	Data Processing and Extraction Automation Software
Precisely EnterWorks	Windows	Product Information, Master Data, and Digital Asset Management Software
Precisely GeoTax	Linux	Geocoded Tax Rate Lookup Service
Precisely MapMarker	Linux	Batch Geocoding Software
Precisely Data360 DQ+, Govern and Analyze	Linux	Data Quality, Data Governance and Analytics Software
Precisely Assure, ER, Insight, NetMind, ACR and Perceive	Linux, Mainframe	Advanced Controls and Analytics Software

Primary Software		
Software	**Operating System**	**Purpose**
TrendMicro Deep Security; Palo Alto PrismaCloud; CrowdStrike	Linux	Centrally managed endpoint security tool with SPI Firewall, IPS, File Integrity Monitoring, Anti-Malware, Web filtering, and Log Inspection
Manage Engine Applications Manager; DataDog	Linux	Centrally Managed Application and System Availability Monitoring and Alerting Tool
Amazon Linux	Linux	Pre-hardened server platform OS
RedHat Linux	Linux	Pre-hardened server platform OS
Microsoft Windows Server	Windows	Pre-hardened server platform OS
OpenSSH	Linux	Encryption-based file transfer and console server
goofys	Linux	Linux-based S3 volume mounting tool
Microsoft Application Insights	Linux	Log and Azure Resource Monitoring tool
Microsoft Operational Insights	Linux	Log and Azure Resource Monitoring tool
Microsoft.NET Server	Windows	.NET Application Server
Apache Tomcat	Linux	Java Application server
Apache Web Server	Linux	Reverse Proxy Server
ElasticSearch	Linux	Search Service
Google Auth / Microsoft Auth / Azure AD	Linux	MFA Token Generator
Chef / TerraForm / Ansible	Linux	Scripted IaC System Deployment Tool
Slack	SaaS	Communications and Workflow Tool
Heap.io	SaaS	Usage Insight Platform
Intercom	SaaS	Interaction Platform
LaunchDarkly	SaaS	Feature and Change Management
BottleRocket / K3S	SaaS	K8S Host
ChainGuard	SaaS	K8S Container Hardening and Signing
PrismaCloud	SaaS	K8S Container Object and Operational Scanning
SQL Server	Windows	Database Server
PostgreSQL	Linux	Database Server
MySQL	Linux	Database Server
Oracle Database	Linux	Database Server

Primary Software		
Software	**Operating System**	**Purpose**
SumoLogic	SaaS	Centrally Managed Application and System Availability Monitoring and Alerting Tool
Workato	SaaS	Backoffice workflow and data integration
DataDog	SaaS	Centrally Managed Application and System Availability Monitoring, CSPM and Alerting Tool
Tenable.io	SaaS	Vulnerability Scanning Platform
PagerDuty	SaaS	Escalation and notification workflow service
Slack	SaaS	Communication and workflow integration platform
AWS Vulnerability Manager / CrowdStrike	SaaS	Vulnerability Management
Rapid7 / Fortra Frontline	SaaS	Vulnerability Management
Mandiant ASM	SaaS	Attack Surface Management
ProofPoint	SaaS	Mail Security and Security Training
Microsoft Sentinel	SaaS	SIEM
Microsoft Defender	SaaS	EDR platform
CrowdStrike	SaaS	EDR platform
Atlassian StatusPage	SaaS	Service status platform
GitLab / GitHub	SaaS	Code repository and management platform
CheckMarx / BurpSuite	SaaS	SAST and DAST Code Scanning
BlackDuck	SaaS	OpenSource and Composition Scanning
Cloudability	Linux	Billing allocation and analysis tool
AWS GuardDuty	SaaS	CSPM Monitoring Service
AWS CloudWatch	SaaS	Log and AWS Resource Monitoring tool
Aviatrix	SaaS	Secure Network and Permissions Configuration Utility
Salesforce ServiceCloud	SaaS	Support Ticketing System and Community
Twilio SendGrid / Mandrill	SaaS	SMTP Mail Service
Microsoft Azure Sentinal / Defender	SaaS	SIEM / CSPM / XDR
Atlassian Confluence	Linux	Documentation and workbook management
Atlassian Jira	Linux	Ticketing and operations platform

People

The Precisely staff provides support for the above services in the following functional, but not limited to, areas:
- Executive Management - provides general oversight and strategic planning of operations.
- Development Team - responsible for delivering a responsive system that fully complies with the functional specification.
- Quality Assurance Team - verifies that the system complies with the functional specification through functional testing procedures.
- System Administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system.
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues.
- Operations Team Managers - collaborate with the Information Security Function on new projects and initiatives to ensure that information security risks are appropriately treated.
- Product Security - provide a centralized service for the deployment maintenance and tracking of security tooling across the business. Provide product security support and training and maintain a group of security champions across the business.
- Cloud Security - implementation, maintenance, and oversight of the security controls within the cloud environments.
- Cloud Operations - responsible for the creation, operation, and maintenance of the cloud infrastructure and application.
- Site Reliability Engineering - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system.

Data

Precisely has implemented both automated and manual procedures to capture and address significant events and conditions. These procedures protect against events that could impact hardware, software, and any operational activities.

The following are examples of security-related activities that will be monitored and logged:
- Malware detection and monitoring
- System Login Events, including failed attempts
- Object Access, including integrity monitoring
- System Events that pertain to security
- Code modification and/or product-level updates

Automated alerts are set in the system to alert key stakeholders of significant events. Alarm conditions will be defined based upon suspicious or security-related activities. Alarm events will be messaged directly to the review team to investigate. Incidents that require investigation will be logged within the ticketing system.

The following is a list of some of the events that will trigger a systemic alert:
- Authentication failures (executing 'su' command with bad password).
- Antivirus agent has timed out and is not operating.

Precisely has also implemented policies and procedures to protect customer environments and data in the event of a disaster. These procedures include policies for a business contingency plan, disaster recovery, backup, and emergency operation. Applications and data are categorized in order to provide priority to level of criticality for recovery or significant event remediation.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to Precisely's policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Precisely team member.

<u>Physical Access</u>

Cloud hosting services are provided by AWS and Azure. AWS and Azure are responsible for the physical and environmental security used to protect the data stored at their facilities. See "Subservice Organizations" section below for additional information.

<u>Logical Access</u>

Precisely uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Employees sign on to the Precisely network via a user account and password. Users are also required to separately sign on to any infrastructure components and applications. Passwords must conform to defined password standards and are enforced through the required parameter settings. These settings are part of the configuration standards and force users to change passwords at a defined interval; disable the user account's ability to access the system and components after a specified number of unsuccessful access attempts; and mask workstation screens, requiring re-entry of the user account and password after a period of inactivity.

As a component of the termination process or a change in employee roles, access permissions are reviewed and updated (or revoked) as necessary. In addition, IT privileged access to the Precisely production environment is reviewed on a monthly basis.

Customers access Precisely SaaS services through the Internet using encrypted Web sessions. Customers must supply a valid user account and password to gain access to the customer cloud resources. Passwords must conform to password configuration configured within the Precisely application.

<u>Computer Operations - Backups</u>

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel at the third-party data center perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on private networks logically secured from other networks. In addition, the third-party hosting services provider replicates data to a secure offsite location that is physically separate from the production location.

<u>Computer Operations - Availability</u>

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Precisely monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches SLAs. Precisely evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:
- Data center space, power, and cooling
- Disk storage

- Network bandwidth

Change Control

Precisely maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted annually to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from outside (external testing) the network.

Vulnerability scanning is performed on a weekly basis in accordance with Precisely policy. The third-party solution uses industry standard scanning technologies and a formal methodology specified by Precisely. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Scanning is performed with approved scanning templates.

Authorized employees may access the system through the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Data Integrity and Analysis SaaS System performed in the Burlington, Massachusetts facility.

This report does not include the cloud hosting services provided by AWS and Azure.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common/Security, Availability and Confidentiality criterion were applicable to the Precisely's Data Integrity and Analysis SaaS System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS and Azure.

Subservice Description of Services

AWS and Azure provide cloud hosting services to Precisely to assist in supporting the in-scope infrastructure.

Complementary Subservice Organization Controls

Precisely's services are designed with the assumption that certain controls will be implemented by the subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Precisely's services to be solely achieved by Precisely control procedures. Accordingly, the subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Precisely.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server location are managed by electronic access control devices.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
		When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		Objects are stored redundantly across multiple fault-isolated facilities.
		The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.4	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.
Availability	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

Precisely management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, Precisely performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and the subservice organizations.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations.

COMPLEMENTARY USER ENTITY CONTROLS

Precisely'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 of the Trust Services Criteria related to Precisely's services to be solely achieved by Precisely control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Precisely's.

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. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for notifying Precisely of changes made to technical or administrative contact information.
2. User entities are responsible for maintaining their own system(s) of record.
3. User entities are responsible for ensuring the supervision, management, and control of the use of Precisely services by their personnel.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Precisely services.
5. User entities are responsible for providing Precisely with a list of approvers for security and system configuration changes for data transmission.
6. User entities are responsible for immediately notifying Precisely of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
7. User entities are responsible for understanding and complying with their contractual obligations to Precisely Software.