System and Organization Controls (SOC) 3 Report

Applied Epic, EZLynx, Applied TAM, Doris, Vision

Management's Report of Its Assertions on Applied Systems, Inc's Broker Management Systems Based on the Trust Services Criteria for Security, Availability, and Confidentiality

For the Period October 1, 2024 to March 31, 2025

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of Applied Systems, Inc

Scope

We have examined Applied Systems, Inc ("Applied") accompanying assertion titled "Assertion of Applied Systems, Inc Management" (assertion) that the controls within Applied's Broker Management Systems (system) were effective throughout the period October 1, 2024 to March 31, 2025, to provide reasonable assurance that Applied'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*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.*

Applied use subservice organizations to provide functions performed by the subservices organizations' system. The description of the boundaries of the system presented in Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Applied, to achieve Applied'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 Applied's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. 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

Applied 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 Applied's service commitments and system requirements were achieved. Applied has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Applied 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 Applied'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 Applied'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 Applied's Broker Management Systems were effective throughout the period October 1, 2024 to March 31, 2025, to provide reasonable assurance that Applied's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP

June 30, 2025
Las Vegas, Nevada

SECTION TWO: MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER APPLIED SYSTEMS, INC'S BROKER MANAGEMENT SYSTEMSBASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY, AND CONFIDENTIALITY

June 30, 2025

Scope

We are responsible for designing, implementing, operating, and maintaining effective controls within Applied Systems, Inc's (Applied) Broker Management Systems (system) throughout the period October 1, 2024 to March 31, 2025, to provide reasonable assurance that Applied'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*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.* Our description of the boundaries of the system is presented in Attachment A (description) 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 October 1, 2024 to March 31, 2025, to provide reasonable assurance that Applied's service commitments and system requirements were achieved based on the applicable trust services criteria. Applied'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.

Applied uses subservice organizations to supplement its services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Applied, to achieve Applied's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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 October 1, 2024 to March 31, 2025, to provide reasonable assurance that Applied's service commitments and system requirements were achieved based on the applicable trust services criteria.

Applied Systems, Inc

ATTACHMENT A: APPLIED SYSTEMS, INC'S DESCRIPTION OF THE BOUNDARIES OF ITS BROKER MANAGEMENT SYSTEMS

Company Background

Since 1983, Applied Systems, Inc. ("Applied") has led an industry Applied helped to create with a mission to continuously improve the business of insurance. Insurance agencies and brokerages have faced new challenges and demands on their businesses over time, and Applied has been there to guide them. Applied has been at the forefront of insurance technology, leading the way through innovation. As the insurance industry becomes increasingly global, Applied is delivering new technology and expanded multinational capabilities for this changing marketplace.

Headquartered in Chicago, Illinois, Applied serves over 339,000 users worldwide. Applied is a leading provider of hosted software solutions, providing applications for agencies, brokers, and insurers. These software solutions are available from a combination of Applied public, private and third-party cloud services through Applied Cloud Services ("Applied Cloud") product offerings, depending on the needs of Applied's customers. The Broker Management Systems and their related controls, including system redundancy, are key differentiators in providing and maintaining high availability, 24/7 access for customers. The scope of this report covers the services which house data within Applied's colocation environments and third-party cloud services located within the United States, Canada, and the United Kingdom.

Additional data center differentiators include:

- **High Availability Platform**
  - Purpose-built data centers classified as Tier 3+ as defined by the Uptime Institute;
  - Multiple Internet connections to provide redundant Internet access for Applied's clients business;
  - Excess capacity within each data center to act as the disaster recovery destination for an opposing site;
  - High availability and redundancy within each site, including uninterruptable power supply and climate control;
  - Redundant firewalls and networking infrastructure; and
  - Resource pool of servers operating in a highly available cluster to allow immediate recovery for any localized failure.
- **Data Protection and Integrity**
  - All backups performed to disk targets then replicated to the data centers., and
  - 24/7/365 operation, with constant monitoring and performance of first level problem resolution against the Applied Cloud.

- **Advanced Security**
  - All databases stored in the Applied Cloud leverage AES-256 data-at-rest-encryption (DARE) which is FIPS 140-2 certified;
  - Network, application, and asset monitoring and testing protect data classified as personal information (also referred to as personally identifiable information or personal data);
  - Internet traffic protected by a minimum of 256-bit, bi-directional, packet-level encryption; and
  - Advanced building design protects the data center floor from exterior penetration, maintains complex video surveillance, strict access control policies and utilizes mantraps, biometric systems and on-site security guards.

Use of Applied software deployed within the Applied Cloud provides clients' business with flexibility, security, and business continuity to drive business growth and profitability. By hosting the Applied solutions in the Applied Cloud, clients gain best in class technology to support online product needs. Applied is committed to continually investing in the Applied Cloud to support business growth.

Applied Broker Management Systems Overview

Applied provides various market leading software applications designed to enhance Applied's core product capabilities, including Applied Epic, Applied TAM, EZLynx, DORIS, Vision, and other products to Applied's customers from the Applied Cloud. The Broker Management Systems are hosted in the Applied Cloud and provided through a Software-as-a-Service (SaaS) model, with customers purchasing software access rights for the number of users required.

System Overview

The System is comprised of the following components:

- ***Infrastructure*** **-** The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software*** **-** The programs and operating software of a system (systems, applications, and utilities)
- ***Data*** **-** The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People*** **-** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- ***Procedures*** **-** The automated and manual procedures involved in the operation of a system

Infrastructure

For each Applied Cloud environment built in Applied's data centers, Applied consistently use like technologies utilizing manufacturers including Cisco, Pure Storage, Dell, F5 Networks,

VMware, Microsoft, and others. Applied owns and maintains all operating equipment within the contracted (colocation) space of the data center. At a minimum, all sites contain the following infrastructure:

- Redundant power feeds from separate UPS systems to each rack;
- Multiple Internet providers using BGP and diverse paths for redundancy in Internet connectivity;
- Redundant network infrastructure including firewalls, IDS/IPS, Domain & Geolocation shunning, DDoS protection, load balancers, switches, VPN devices and routers;
- 10 GB network connectivity support for all core devices;
- Fully virtualized server platform with servers in resource clusters based on load type;
- Physical hosts redundantly connected to SAN, network, and power components
- Virtual network segmentation for products and server purpose; and
- Remote control technologies including managed PDU's, secure console devices and remote server out-of-band management.

Production Environment

Applied utilizes Google Cloud Platform to provide infrastructure management services. Services operate within a shared security responsibility model, where GCP is responsible for the security of the underlying cloud infrastructure, and Applied is responsible for the systems deployed in GCP.

Applied uses many technologies and protocol in order to better secure Applied's infrastructure.

Production instances at GCP are logically and physically separated from Applied Systems, Inc's internal corporate network. Orca Software is leveraged to test for vulnerabilities and offers context, prioritization, and remediation for the identified vulnerabilities. Orca delivers industry-leading Cloud Security that identifies, prioritizes, and remediates security risks and compliance issues across Applied's GCP infrastructure

At Applied, Cloudflare is leveraged for the Web Application Firewall. This focuses on evaluating incoming application requests for known vulnerabilities based on a set of rules.
GCP's VCP Firewall is utilized to control network traffic.

We also use the following tools in addition to those identified above:

- Kubernetes- Automated deployment, scaling, and container management
- Envoy- Network traffic management
- Apigee- API management solution
- Terraform- IaC platform, RBAC within cloud environment
- Cloudflare- Web Application Firewall (WAF), DDos Mitigation, Content Delivery Network (CDN) Services, and DNS Services

Applied Data Centers
Applied deploys the Broker Management Systems through the Applied Cloud, which operates from within purpose-built colocation data centers geographically distributed to support its global customer base. Facilities are selected using a risk assessment process to identify locations that have a low risk of natural disaster from earthquake, flood, fire, windstorm or other severe weather conditions. Site selection also includes consideration for local civil disruptions, power capacity and stability, proximity to other high risks such as railways, airports, and selective manufacturing environments. Each data center has a SOC or country equivalent assessment conducted annually.

Each colocation facility is sited at, and managed by, a subservice organization with skilled and experienced employees to provide core facility components to Applied. These include physical security and access controls; power systems including utility power, N+1 generator power, redundant UPS systems, redundant power distribution and switching components, and redundant circuits delivered to each rack; redundant heating, ventilation, and air conditioning (HVAC) systems; dry pipe and multi-zone fire detection devices with early smoke detection capabilities; video surveillance with 24-hour monitoring; and diverse telecommunications paths into the facility.
Specific features provided by the data centers include:

- **Highly Secure Environment**
  - Multiple layers of hardened physical security;
  - 24x7x365 on-site security presence;
  - Closed-circuit television surveillance with digital storage;
  - Multiple layers of electronically controlled card access;
  - Keyed access to physical Applied space;
  - Electronic key card readers; and
  - Facility verification of government issued photo IDs against approved access list.
- **Power Distribution**
  - Commercial grade high-capacity UPS system with complete isolation for redundancy;
  - Multiple 1,500+ KW generators for backup power with N+1 redundancy;
  - Minimum of five days of on-site fuel supply and extended refuel contracts;
  - Each circuit breaker backed by diverse power distribution units and diverse UPS infrastructures for the ultimate in uptime;
  - Isolated redundant UPS configuration providing industry's highest MTBF; and
  - Individual circuit load monitoring to ensure the best power management.
- **Environmental Control**
  - Temperature above floor maintained between 64 and 78 degrees; humidity maintained between 40 and 60 percent;
  - Redundant HVAC with minimum of 30 percent reserved capacity installed;
  - Sufficient air handling units for N+1 redundancy; and

- Multiple glycol cooling units for N+1 redundancy.
- **Fire Detection/Prevention**
  - Zoned dry-piped, pre-action sprinkler system; and
  - Zoned VESDA (Very Early Warning Smoke Detection) system throughout the data center.
- **Private/Point-to-point network connectivity**
  - Applied provides connectivity options for VPN solutions between Applied data center and some clients' facilities, as required; and
  - Applied supports the use of MPLS connectivity into the Applied Cloud environment for customers who prefer to use network connectivity with carrier provided service level agreements.
- **Connectivity (Availability and selection of carriers varies by location)**
  - Diverse entry paths into each facility;
    - Lumen;
    - Comcast;
    - Bell CA:
    - Zayo;
    - 365 Data Centers;
    - Equinix;
    - eStruxture Data Centers;
    - Aptum;
    - Megaport

Software

Applied leverages Microsoft® technologies for nearly all its virtual machine operating systems. Authentication services are provided through Microsoft Active Directory, database services are provided through Microsoft SQL Server, and web services mostly provided through Microsoft IIS. Other operating systems may be found on specialty devices, custom hosting environments built to customer specifications, and limited infrastructure management toolsets.

Application products in this scope developed by Applied and operating from the data center include:

- **Agency and Brokerage Management Systems**
  - Applied Epic - Applied Epic is the insurance industry's fastest-growing agency and brokerage management system. Epic's modern, flexible and secure architecture provides agencies and brokerages with a single platform that scales as the Company grows. It allows you to manage and maintain a clear picture of your entire agency across all roles, locations and lines of business, including both P&C and benefits. Applied's Epic software is browser-native so your team is able to easily access data, minimize software management and more quickly realize the

value of new capabilities. Build your agency on a system that automates back office operations, keeps your front office sales team connected, and integrates with customer service and insurer connectivity technologies.

- EZLynx - EZLynx's integrated agency management technologies provide comparative rating, agency management and automation, commercial submissions, retention tools, consumer quoting, email marketing, text messaging, online client self-servicing, and so much more. The system maximizes agencies' potential by increasing their ability to retain current customers while acquiring new business. By providing a central location, EZLynx enables agents to generate and store quotes, policies and documents, as well as easily re-market with up-to-date information that is synced from agents' daily policy downloads. Through advanced automation and the ability to seamlessly connect to insurers and insureds, agents using EZLynx improve productivity, simplify management, optimize serviceability and increase profitability.
- Applied TAM - Applied TAM was the most-widely used agency management software in the insurance industry for business automation. For nearly 40 years, Applied TAM has provided insurance agencies and brokerages with the leading software to manage day-to-day operations across their business.
- Applied Doris - Applied DORIS is a cloud-based agency management system that automates business operations of growing insurance agencies specializing in personal lines property and casualty insurance.

Data

Applied acts as the data processor for agency, broker and carrier information stored or transmitted through the Broker Management Systems deployed within the Applied Cloud. Specifics include:

- Customer data stored within the Applied Cloud environment is classified as CONFIDENTIAL to all Applied staff;
- Applied stores data in one of the aforementioned data centers, which is backed-up daily and replicated to its paired site for disaster recovery;
- In addition to stored/hosted data being encrypted at rest, Applied uses secure communications channels for data transmitted through the application or Web services between the end-user and the data center; and
- Applied destroys data from storage in the Applied Cloud no later than 180 days after the cancellation of a contract, and data expires from backup media in accordance with its backup retention policy.

Data Minimization & Security: Applied requires that proper security protocols are put in place to protect data from breaches or unauthorized access. AI features and use may not be deployed unless and until such security protocols are in place. Applied minimizes data that may be used for AI development and only collects and uses information for legitimate purposes. AI models are developed in-house and live in their own independent environment

which Applied owns or controls. While Applied may use an external AI model to power certain layers, Applied does not leverage public AI offerings and limits data points to pass as inputs into such models. Applied further restricts such models from learning from data and wherever possible, remove identifying information and sanitize the data which is being used.

Training Safely: Applied takes appropriate steps so that identifying information is not used to train a model. Applied prohibits the use of any information at all to train a third-party AI model.

AI is Clear: Applied leverages a mix of AI models such as large language models (LLM) and large events models (LEM). Applied provides transparency by clearly labeling any interaction with or content generated by AI to enable users to determine the impact they want AI to have on the work humans do and decisions humans make. For example, Applied includes notices indicating where a summary was created by AI, and where a second paragraph of text was edited by a human.

Humans in Control: Humans retain ultimate control over any AI-driven actions. Users drive the workflow, control which decisions are made, and are responsible for the outcomes. Delivering experiences that keeps the human in the driver's seat allows users to quickly evaluate and decide which AI suggestions to accept, so that users have confidence in the information and resulting actions.

Applied Epic Email Summarization

Applied Epic Email Summarization is a tool that does exactly what it sounds like– it summarizes email content using the power of AI. This tool must be enabled by the user before it can be used, reinforcing Applied's "Humans in Control" key principle. Next, Email Summarization only gains access to the emails the user wishes to summarize. It does not read all emails and does not access document storage. This is another opt-in situation. The user must select an email and attach it to Epic (bring it out of their inbox into the Epic UI). From there the user must click a button before the summary is generated. Nothing is passed to any AI service until that button is pressed. The AI used to summarize the email has been developed by Applied. During the process of summarizing the email, Applied sends the selected email to an internal service and extract just the text out of it (any attachments are dropped). From there the text is summarized using an enterprise AI model which is invoked via secured API. The email text and the summary that's generated from there is stored in an Applied managed database, in an Applied managed environment within the Applied network, similar to how each agency has its own Epic instance.

EZLynx Virtual Assistant

EZLynx Virtual Assistant, or EVA as she's more commonly known, is an RPA tool that interacts with a human to guide their workflow and steps within the EZLynx platform. EVA answers questions on workflows or other functionality as a type of guide. EVA will help you spend less time on manual tasks and more time on customer relationship management. A feature within Communication Center, when enabled by a user EVA will monitor your assigned number for text messages from your customers and will respond to them accordingly. Eva has the ability to assist insureds with requests for their Coverage, Vehicle, or Driver information. More information about EVA can be found here or by contacting your EZLynx sales representative.

People

The competence of employees is a key element of the system. Applied is committed to the development of its employees and the recruitment of qualified professionals to support the growth of Applied's business.

A dedicated team of technology professionals are responsible for the design, deployment, management, administration, and monitoring of the Applied Cloud and in turn the software solutions deployed via the Applied Cloud. The Cloud Services team consists of staff specializing in storage, server, network, application, virtualization, security, monitoring, and SQL technologies. This includes but is not limited to engineers, application administrators, a 24x7x365 operations team, and DevOps resources. All teams report up through the Senior Vice President of Cloud Services.

It is the responsibility of these team members to maintain the data center and the related software applications in a working state for the Applied Cloud customer base. This includes managing resources against capacity requirements, provisioning new orders, monitoring for system and application health, performing routine application updates and patch management at the OS and application layers, and monitoring for and assisting with the remediation of security threats. The Senior Vice President of Cloud Services works closely with Applied's Chief Information Security Officer (CISO) and the Information Security team to meet such requirements.

Key positions are as follows:

Chief Customer Officer (CCO) is responsible for Applied's customer delivery strategy and operational execution for Applied's Professional Services, Support and Cloud-based solutions.

Chief Technical Officer (CTO) directs the technology, architecture, and application development of Applied's products.

Chief Information Officer & Chief Information Security Officer (CISO) heads the Office of Information Security for Applied and related Corporate IT services. Leads all information security related initiatives, including management of the information security program, which includes formalizing a cyber-risk management strategy, continuous governance and compliance exercises, as well as vulnerability management practices and incident response procedures.

Senior Vice President of Cloud Services, heads global IT operations for Applied's Cloud hosting services and oversees the operations of Applied's four global data centers.

Vice President of Product Operations is responsible for developing the product roadmap for Applied Cloud administration and management applications, and consulting with the Applied application development teams to represent the unique requirements that come with hosting and updating Applied applications in the data center.

Director of Internal Application Development directs the technology, architecture, and application development of internal and data center information systems and integrations.

Director of Data Center Engineering leads the team responsible for the architecture, deployment, and support of technology within the Applied Cloud data centers.

Procedures

Applied provides multiple technology platform services to its customers through a subscription of services. These include agency and brokerage management systems, carrier interface, reporting services, and consumer-focused products.

Applied has a series of procedures to provision new subscriptions for services provided by the Applied Cloud, including Broker Management Systems. These steps include:

- Set up new client entities based on applicable signed contracts;
- Modify backup and monitoring policies to include new resources;
- Verify product access is customer ready; and
- Setup initial authorized application administration account and provide information to the customer in a secure manner.

Once new system subscriptions are created and administrative users for the client account have been established within the system, the following activities occur to ensure that services are available for client use:

- Resources actively monitored for available and capacity management;
- System performance metrics reviewed;
- Backup and restore procedures performed;

- Application updates managed;
- Customer communications distributed to advise of maintenance schedules, product updates, and other relevant information;
- Ongoing security management, assessments, and remediation; and
- Termination of access when customer cancels service, including the removal of data in accordance with the defined policy after a designated holding period.

The Leadership Committee operates independently and provides oversight of the system of internal control.

Complementary Subservice Organization Controls

Certain principal service commitments and system requirements can be met only if complementary subservice organization controls (CSOC) assumed in the design of Applied's controls are suitably designed and operating effectively at the subservice organizations, along with related controls at Applied.

Equinix

Applied uses Equinix as the co-location data center for the Applied Cloud environment. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at Equinix, alone or in combination with the controls at Applied, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
6.4	Equinix is responsible for restricting physical access to facilities and protected information assets to authorized personnel.
A 1.2	Equinix is responsible for maintaining and monitoring environmental protections and recovery infrastructure.

365 Data Centers

Applied uses 365 Data Centers as the co-location data center for the Applied Cloud environment. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at 365 Data Centers, alone or in combination with the controls at Applied, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
6.4	365 Data Centers is responsible for restricting physical access to facilities and protected information assets to authorized personnel.
6.7	365 Data Centers is responsible for implementing security measures to protect information against threats during transmission, movement, or removal.
A 1.2	365 Data Centers is responsible for maintaining and monitoring environmental protections and recovery infrastructure.

Aptum

Applied uses Aptum as the co-location data center for the Applied cloud environment. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at Aptum, alone or in combination with the controls at Applied, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
6.4	Aptum is responsible for restricting physical access to facilities and protected information assets to authorized personnel.
6.7	Aptum is responsible for implementing security measures to protect information against threats during transmission, movement, or removal.
A 1.2	Aptum is responsible for maintaining and monitoring environmental protections and recovery infrastructure.

eStruxture

Applied uses eStruxture as the co-location data center for the Applied cloud environment. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at eStruxture, alone or in combination with the controls at Applied, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
6.4	eStruxture is responsible for restricting physical access to facilities and protected information assets to authorized personnel.
6.7	eStruxture is responsible for implementing security measures to protect information against threats during transmission, movement, or removal.
A 1.2	eStruxture is responsible for maintaining and monitoring environmental protections and recovery infrastructure.

Google Cloud Platform (GCP)

Applied uses GCP provide infrastructure management services for the Applied Cloud environment. The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at GCP, alone or in combination with the controls at Applied, to provide assurance that the required trust services criteria in this report are met.

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
6.4	GCP is responsible for restricting physical access to facilities and protected information assets to authorized personnel.
A 1.2	GCP is responsible for maintaining and monitoring environmental protections and recovery infrastructure.

Applied Management receives and reviews the Equinix, 365 Data Centers, Aptum, eStruxture's, and GCP SOC 2 Type 2 report on an annual basis. Any deficiencies identified in a subservice organization's SOC 2 report are analyzed for relevance to and effect on Applied's organization and its users. As part of the review:

- Management confirms that the CSOCs listed above are covered within the scope of Equinix, 365 Data Centers, Aptum, eStruxture's, and GCP SOC 2 Type 2 reports and are found to be operating effectively during the audit period.
- Management determines that the Complementary User Entity Controls (CUECs) identified in Equinix, 365 Data Centers, Aptum, eStruxture's, and GCP SOC 2 Type 2 reports are included in the scope of this SOC 2 report as controls that are tested by the service auditor.

In addition, through its daily operational activities, management monitors the services performed by Equinix, 365 Data Centers, Aptum, eStruxture, and GCP to ensure that operations and controls expected to be implemented are functioning effectively.

Complementary User Entity Responsibilities

User Entity Responsibilities

Applied's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

However, in order for user entities to benefit from Applied's system and its controls, the following responsibilities should be considered by user entities:

#	User Entity Responsibilities	Related Applicable Trust Services Criteria
1	Users are responsible for restricting authority of provisioning new user accounts within any Applied Software-as-a-Service model application.	6.2
2	Users are responsible for disabling access in a timely manner to ensure the terminated employee account access is removed.	6.2
3	Users are responsible for ensuring user owned or managed applications, platforms, databases, and network devices that may process or store data derived from Applied are logically secured. Users are also responsible for Internet access to the Applied Cloud environment.	6.1
4	Users are responsible for ensuring user access to reports and other information transmitted to, or generated from, Applied is restricted based on business need.	6.4, 6.7
5	Users of Applied hosted applications are responsible for maintaining appropriate IT General Computer Controls and Application Controls.	6.2, 6.3
6	Users of Applied hosted applications are responsible for maintaining appropriate password management controls including complexity, periodic change, and minimum length.	6.1, 6.3

#	User Entity Responsibilities	Related Applicable Trust Services Criteria
7	Users are responsible for adhering to all regulatory compliance issues when they are associated with Applied in a service agreement.	2.3, C1.1
8	Users are responsible for reviewing and approving the terms and conditions stated in service agreements with Applied.	2.3, 7.2

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Description of Services Provided

Applied's leading global cloud software automates the exchange of information and data throughout the insurance lifecycle among agents, brokers, insurers, and consumers throughout the United States, Canada, the Republic of Ireland, and the United Kingdom. By enabling greater access to information and streamlining workflows, Applied's customers can capitalize on new opportunities, increase the efficiency and profitability of their business, and continuously deliver the high-level service that customers expect.

The Applied Broker Management Systems portfolio consists of some of the following components:

- Applied Epic is the world's most widely used management platform. It allows agencies to manage and maintain a clear picture of their entire agency across all roles, locations and lines of business, including both P&C and benefits.
- EZLynx is a cloud-based, all-in-one agency management system, complete with intuitive tools for agency management and automation, retention, commercial submissions, eSignature, email marketing, text messaging, online client self-servicing, and so much more.
- Applied TAM provides brokers the ability to automate daily operational processes, effectively manage customer policy information and seamlessly connect with insurers and policyholders.
- Applied DORIS is an agency management system that helps agents manage customer and business operations.

Principal Service Commitments and System Requirements

Applied describes the products, services, and scope of work provided to its clients through software and services agreements, orders, and Applied's public website. Obligations, responsibilities, and deliverables are documented and agreed upon by both parties in the Applied Master Agreement and related paperwork, and contracts must be established before software or services are provided. Applied designs its software solutions to meet contractual commitments and periodically reviews contracts to verify that the commitments therein reflect the ongoing updates to the software and services Applied provides.

Security, availability, and confidentiality commitments are documented and communicated to customers within these agreements, which include, but are not limited to, the following:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of the Applied Cloud and customer data therein in accordance with Applied's security requirements;
- Reporting on Controls at a Service Organization Relevant to Security, Availability, and Confidentiality (SOC 2) examinations;
- Use formal employee management processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews;
- Use of encryption technologies to protect customer data both at rest and in transit over untrusted networks;
- Use of firewalls, IP shunning devices, and network segmentation to restrict data flow.
- Infrastructure security monitoring including intrusion detection & prevention systems, centralized log management and alerting;
- Prevent malware from being introduced to production systems;
- Vulnerability management program designed to identify and correct vulnerabilities within the Applied Cloud in a timely manner;
- Incident Response program designed to minimize and remediate the impact of cyberattacks and protect resources; and
- Geographically separated data centers with multi-layered physical security controls.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

Applied establishes system and operational requirements that support the achievement of the principal service commitments, compliance with applicable laws and regulations, and other system requirements. These requirements are communicated in Applied's policies and procedures, system design documentation, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided that any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

Applied regularly reviews the security, availability, confidentiality, and performance metrics to ensure these commitments are met.