Report on InterSystems Corporation's Cloud Services Solution Relevant to Security, Availability, and Confidentiality Throughout the Period January 1, 2025 to December 31, 2025

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To: InterSystems Corporation ("InterSystems")

Scope

We have examined InterSystems' accompanying assertion titled "Assertion of InterSystems Corporation Management" (assertion) that the controls within InterSystems' Cloud Services Solution (system) were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that InterSystems' 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*.

InterSystems uses a subservice organization to provide hosting services for its IT infrastructure. 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 InterSystems, to achieve InterSystems' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of InterSystems' controls. 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

InterSystems 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 InterSystems' service commitments and system requirements were achieved. InterSystems has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, InterSystems 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 American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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 InterSystems' 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 InterSystems' 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 InterSystems' Cloud Services Solution were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that InterSystems' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of InterSystems' controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Louisville, Colorado
April 6, 2026

Section 2

Assertion of InterSystems Corporation Management

InterSystems Corporation
One Congress Street
Boston, MA 02114-2010

Main: +1 617 621 0600
Support: +1 617 621 0700
InterSystems.com

Assertion of InterSystems Corporation ("InterSystems") Management

We are responsible for designing, implementing, operating and maintaining effective controls within InterSystems' Cloud Services Solution (system) throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that InterSystems' 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 and identifies the aspects of the system covered by our assertion.

InterSystems uses a subservice organization to provide hosting services for its IT infrastructure. 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 InterSystems, to achieve InterSystems' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of InterSystems' controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that InterSystems' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of InterSystems' controls operated effectively throughout that period. InterSystems' 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.

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, 2025 to December 31, 2025, to provide reasonable assurance that InterSystems' service commitments and system requirements were achieved based on the applicable trust services criteria.

InterSystems Corporation

Attachment A

InterSystems Corporation's Description of the Boundaries of Its Cloud Services Solution

Type of Services Provided

InterSystems Corporation (“InterSystems” or “the Company”) was founded in 1978 and develops advanced data management, connectivity, and analytics technologies to assist its clients in healthcare, financial services, government, utilities, and other industries. Headquartered in Boston, Massachusetts, InterSystems employs more than 2,000 personnel in over 100 countries.

InterSystems Cloud Services operations provide managed services delivered and operated by InterSystems. The solution is built on a dedicated InterSystems IRIS instance, InterSystems IRIS for Health, also known as InterSystems Health Connect, hosted within a cloud service provider environment. Oversight and operational responsibility for the Cloud Services Solution resides with the InterSystems Cloud Delivery Team (CDT).

The boundaries of the system in this section details the Cloud Services Solution. Any other Company services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of the Cloud Services Solution are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Cloud Services Solution.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes Amazon Web Services (AWS) to provide the resources to host the Cloud Services Solution. Although the Company leverages the experience and resources of AWS to scale quickly and securely as necessary to meet current and future demand, the Company is responsible for designing and configuring the Cloud Services Solution architecture within AWS to ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure		
Production Tool	**Business Function**	**Hosted Location**
Databases	Customer data storage	AWS
Amazon Elastic Compute Cloud (Amazon EC2) instances	Compute	AWS
Virtual Private Cloud (VPC)	Isolation	AWS
AWS Elastic Load Balancing (ELB)	Resilience	AWS

Infrastructure		
Production Tool	**Business Function**	**Hosted Location**
AWS CloudTrail	Audit	AWS
Amazon CloudWatch	Observability	AWS
AWS Config	Compliance	AWS
Transfer Family	Data transfer	AWS
Amazon Elastic File System (Amazon EFS)	Customer data storage	AWS
Amazon Elastic Container Service (Amazon ECS)	Compute	AWS
AWS Secrets Manager	Security	AWS
AWS Lambda	Compute	AWS
Amazon GuardDuty	Security	AWS
Amazon Simple Storage Service (Amazon S3)	Customer data storage	AWS
Amazon EC2 Container Registry	Resilience	AWS
AWS Backup	Resilience	AWS
AWS Key Management Service (KMS)	Encryption	AWS
Lacework	Security	AWS
Amazon Route 53	Resilience	AWS
Amazon Simple Queue Service (Amazon SQS)	Resilience	AWS
Coralogix	Observability	AWS
Amazon Cognito	Security	AWS
Amazon Simple Notification Service (Amazon SNS)	Observability	AWS

Software

Software consists of the programs and software that support the Cloud Services Solution (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the Cloud Services Solution include the following business functions, as shown below:

- OS
- Security event monitoring and alerting
- System monitoring and observability
- Alerting
- Configuration management
- Code repository and software development platform
- Project tracking

People

The Company develops, manages, and secures the Cloud Services Solution via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing Company-wide activities, establishing and accomplishing goals, and managing objectives.
Managed Services	Responsible for the operation, security, and support of the Cloud Services Solution through the CDT.
Human Resources (HR)	Responsible for onboarding new personnel and facilitating the employee termination process.
Recruiting	Responsible for defining the roles and positions of new hires and performing background checks and other screening.
Cybersecurity	Responsible for overseeing and monitoring of cybersecurity and data protection operations and governance.

Procedures

Procedures include the automated and manual procedures involved in the operation of the Cloud Services Solution. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the Cloud Services Solution:

Procedures	
Procedure	**Description**
Logical and Physical Access	InterSystems has developed policies and procedures, including a Password Policy, Confidentiality Policy, Confidential Information Controls Policy, and Privileged Management Policy, which are designed to prevent or mitigate unauthorized application access and data loss.
System Operations	InterSystems has developed procedures related to configuration management, network monitoring, and overall data handling.
Change Management	InterSystems utilizes procedures developed for the secure management of changes within the cloud environment.
Risk Mitigation	InterSystems maintains a risk assessment program to identify and address risks that may impact the Cloud Services Solution.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API) and Transmission Control Protocol (TCP) sockets, the customer or end-user defines and controls the data they load into and store in the Cloud Services Solution production network. Once stored in the environment, the data is accessed remotely from customer systems via a secure internet connection. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for the transmission of confidential or sensitive information over private and public networks. Encryption is enabled for databases housing sensitive customer data.

User Entity Responsibilities

Management of user entities is responsible for the following, which should not be regarded as a comprehensive list of all controls that should be employed by user entities:

- User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.
- User entities have controls to provide reasonable assurance that the Company is notified of changes in user entity vendor security requirements.
- It is the responsibility of the user entity to have policies and procedures to:
  - Inform their employees and users that their information or data is being processed and stored by the Company.
  - Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
  - Ensure compliance with relevant laws and regulations governing the user entity's processing of information through services provided by the Company.

- User entities grant access to the Company's system only to authorized and trained personnel.
- User entities maintain controls regarding the creation, use, and monitoring of credentials for access to services provided by the Company.
- User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization to provide hosting services for its IT infrastructure. The Company's controls related to the Cloud Services Solution cover only a portion of the overall internal control for each user entity of the Cloud Services Solution.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Cloud Services Solution to be achieved solely by the Company. Therefore, each user entity's internal control much be evaluated in conjunction with the Company's controls, taking into account the related CSOCs expected to be implemented at AWS are described below.

Criteria	Complementary Subservice Organization Controls
CC6.1 C1.1	• AWS should encrypt databases in its control.
CC6.4	• AWS should restrict data center access to authorized personnel. • AWS should monitor data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 C1.2	• AWS should securely decommission and physically destroy production assets in its control.
CC6.8	• AWS is responsible for ensuring that physical infrastructure and virtual servers supporting the service are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

Criteria	Complementary Subservice Organization Controls
CC7.2 A1.2	• AWS should install fire suppression and detection and environmental monitoring systems at the data centers. • AWS should protect data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS should oversee the regular maintenance of environmental protections at its data centers.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Cloud Services Solution. Commitments are communicated in written service agreements with customers, as well as in service-level availability (SLA) specifications.

System requirements are specifications regarding how the Cloud Services Solution should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Cloud Services Solution include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• InterSystems will provide a security program that carefully considers data protection matters across the Company's suite of services, including data submitted by customers to its services. • InterSystems will maintain administrative, physical, and technical safeguards for protection of the security (including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage), confidentiality, and integrity of customer information. InterSystems will regularly monitor compliance with these safeguards. • InterSystems will store and access all customer information in a manner that complies with the requirements of applicable data protection and security laws. • InterSystems will ensure that its compliance with confidentiality, security, and data protection obligations, as well as the technical and organizational information security measures implemented by InterSystems and its subcontractors, are subject to regular audits occurring at least once per year. • InterSystems will notify the customer without unreasonable delay, but within no more than 3 business days, upon the discovery of a security incident. • InterSystems will notify the customer without unreasonable delay, but within no more than 3 business days, upon the discovery of a breach.	• Logical access standards • Employee provisioning and deprovisioning standards • Risk assessment standards • Change management standards • Firewalls • System hardening standards • Logging and monitoring standards • Incident handling standards • Encryption standards • Test environments

Trust Services Category	Service Commitments	System Requirements
Availability	• InterSystems will maintain an SLA commitment of 99.9% availability for cloud infrastructure and customer production environments. • InterSystems will offer replication of data to a secondary cloud region for disaster recovery purposes (optional). • InterSystems will provide maintenance to customer environments in the form of patches or updates with the least disruption to delivery of customer services during a weekly maintenance window. Customers will receive notification of an adequate window of time during which to perform testing in each environment before upgrades are promoted to the next environment.	• Redundant systems that ensure availability • Backup and restore capabilities • Network configuration management • Network capacity and health monitoring
Confidentiality	• InterSystems will protect customer confidential information in the same manner that it protects its own confidential information of like kind, but in no event using less than a reasonable standard of care. • InterSystems will ensure that the solution support personnel engaged in the processing of customer information are informed of the confidential nature of the customer information, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. InterSystems will ensure that such confidentiality obligations survive the termination of their engagement.	• Data protection and security program • Employee training program