COALFIRE CONTROLS

Report on InterSystems Corporation's Managed Services US Solution Relevant to Security, Availability, and Confidentiality Throughout the Period January 1, 2024 to December 31, 2024

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' Managed Services US Solution (system) were effective throughout the period January 1, 2024 to December 31, 2024, 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 data center colocation 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 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' Managed Services US Solution were effective throughout the period January 1, 2024 to December 31, 2024, 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

Greenwood Village, Colorado
February 12, 2025

Section 2

Assertion of InterSystems Corporation Management

InterSystems
Creative data technology

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' Managed Services US Solution (system) throughout the period January 1, 2024 to December 31, 2024, 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 for data center colocation 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 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, 2024 to December 31, 2024, 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, 2024 to December 31, 2024, 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 Managed Services US 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 Cambridge, Massachusetts, InterSystems employs more than 2,000 personnel in over 100 countries. The managed services department supports customers globally, including in the United States and the United Kingdom.

InterSystems, through the Managed Services US operations, provides managed services of InterSystems technology, including InterSystems IRIS® and HealthShare, to the customer either on-premises (managing the operation of the solution utilizing InterSystems technology) or through hosting services provided by InterSystems supporting the customer solution. For example, the InterSystems HealthShare platform implements a “connected health” strategy that links all data, applications, and processes to provide access to comprehensive patient records and real-time analytics. In addition to licensing the InterSystems HealthShare platform for customers to operate in their own environment, InterSystems provides a managed solution that may include the hosting of the environment for the managed solution. This managed service is provided by managed services teams within the Technical Services Department and the Managed Services US Solution (or “the system”) is overseen by the Managed Services US team (Managed Services). For customers who choose to host the HealthShare platform within their own environment, Managed Services still provides relevant services in order to maintain that environment; however, the technical boundary of the client’s managed services environment and the controls related to the security, availability, and confidentiality of that environment are not within the scope of this report.

The boundaries of the system in this section details the Managed Services US Solution. Any other Company services, including managed services for other regions, are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of the Managed Services US 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 Managed Services US Solution.

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

Infrastructure

For customers using the Managed Services US Solution within the InterSystems-hosted environment, the Managed Services US Solution provides a set of services for a complete development and deployment environment, including any required infrastructure (e.g., servers, storage, and networking) to deliver various InterSystems technology solutions based on InterSystems products, as well as HealthShare to customers as a platform-as-a-service (PaaS) offering. The Managed Services US Solution encompasses the hosting, management, and operations of a customer environment used for the delivery of the Managed Services US Solution, which InterSystems maintains and provides for its customers to utilize and to interact with its customers’ own instance of the Managed Services US Solution. The service delivery includes the standup, configuration, backup, and ongoing operation and monitoring of the underlying parts of the environment.

The HealthShare platform operated by Managed Services in the United States is located at [redacted] data centers. The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure			
Production Tool	**Business Function**	**Operating System**	**Hosted Location**
Servers	Information and data processing	Linux	[redacted]
Computers and networking equipment	Information transfer and communication	Linux	[redacted]
Databases	Data storage	InterSystems IRIS® Data Platform	[redacted]

Software

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

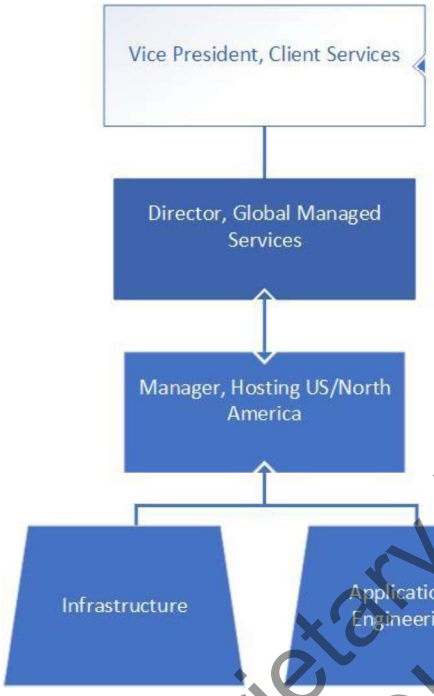
Software	
Production Application	**Business Function**
Veeam	Backup and replication
Splunk	Log aggregation system
Nagios	Infrastructure monitoring
Netbox	Asset management
Puppet and Red Hat Satellite	Configuration management of Linux OS changes
ClamAV and Cortex XDR	Antivirus

People

Managed Services, which reports to the Director of Managed Services, is responsible for the operation and support of the system. On occasion, resolution of Managed Services US Solution issues may require assistance from the InterSystems customer support group, development, or product management. On those occasions, temporary access to the Managed Services US Solution may be authorized on a strictly limited basis. All such access is logged and managed through the internal ticketing system.

The InterSystems Data Protection Officer is responsible for ensuring compliance with data protection laws and regulators.

The following organization chart reflects the Company's internal structure related to the groups discussed above:



Procedures

Procedures include the automated and manual procedures involved in the operation of the Managed Services US 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 human resources (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 Managed Services US 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 backup scheduling, network monitoring, and overall data handling.
Change Management	InterSystems utilizes procedures developed for the management of the system's infrastructure and modifications, including OS and network appliance upgrades and patching.
Incident Management	InterSystems continuously monitors for incidents and security vulnerabilities.

Procedures	
Procedure	**Description**
Policy Management and Communication	InterSystems communicates organizational values and behavioral standards to all personnel through policy statements and training.
Backups and Off-site Storage	InterSystems performs daily backups to the off-site backup location in Virginia, with backup completion notifications sent to InterSystems. Failed backups are either re-run the following day or are investigated for recurring issues and resolved. Off-site replication of data is also performed daily. Stored backup media is maintained in an encrypted state.
Network and Servers	InterSystems keeps the networking equipment and servers in its network perimeter secure against known vulnerabilities by installing vendor-supported OSs and patches. Internal vulnerability assessments of the network that contains the system are performed weekly. An external vulnerability assessment is performed annually by a third-party provider.

Data

Client data is defined as customer health information that is transacted through the HealthShare platform, which acts as an information exchange. Clients do not have direct access to the InterSystems network environment, nor does InterSystems have direct access to customer environments.

The Company has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks.

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 should 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.
- Controls to provide reasonable assurance that the Company is notified of changes in:
  - User entity vendor security requirements
  - The authorized users list
- 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 used and stored by the Company.
  - Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
- User entities should only grant access to the Company's system to authorized and trained personnel.
- Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.

- User entities should 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 [redacted] as a subservice organization for data center colocation services. InterSystems' controls related to the Managed Services US Solution cover only a portion of the overall internal control for each user entity of the Managed Services US 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 [redacted] related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. [redacted] physical security controls should mitigate the risk of unauthorized access to the hosting facilities. [redacted] environmental security controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the [redacted] SOC 2 report annually. In addition, through its operational activities, InterSystems management monitors the services performed by [redacted] 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 [redacted] management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Managed Services US Solution to be achieved solely by InterSystems. The CSOCs that are expected to be implemented at [redacted] are described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	• [redacted] is responsible for restricting data center access to authorized personnel via access control systems. • [redacted] is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2 A1.2	• [redacted] is responsible for ensuring that smoke detection and fire suppression equipment is in place at each location and that these are monitored both within the network operations center (NOC) and by a third party. • [redacted] is responsible for the maintenance of fire suppression systems in place for all locations by the NOC and third party. • [redacted] is responsible for the maintenance and monitoring of the cooling and humidity systems by the NOC and a third party. • [redacted] is responsible for facility walkthroughs that are performed routinely for all [redacted] facilities and data centers. During the facility walkthroughs, environmental aspects are observed, and any noted issues are escalated according to data center procedures. • [redacted] is responsible for redundant electrical and telecommunication systems. • [redacted] is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS).

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 Managed Services US Solution. Commitments are communicated in written hosting or solution service agreements with customers, as well as in service-level availability (SLA) specifications.

System requirements are specifications regarding how the Managed Services US 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 Managed Services US 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 three business days, upon discovery of a security incident.	• 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 • Data center security and environmental controls

Trust Services Category	Service Commitments	System Requirements
Availability	• InterSystems will have data updates for environments with disaster recovery services replicated from the primary data center to a secondary data center. Disaster recovery services will be delivered using a recovery point objective (RPO) and a recovery time objective (RTO) as specified in the relevant SLA. • InterSystems will maintain a system uptime percentage of at least 99.9% during any given calendar month. • InterSystems will provide external users with guidelines and technical support resources relating to system operations on the InterSystems website. The Company will notify customers of critical changes that may affect their processing.	• Redundant systems that ensure availability • Secondary data center for recovery • 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