Consensus Assessment Initiative Questionnaire (CAIQ) for InterSystems HealthShare on AWS

May 2021

Introduction

The Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire provides a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions which can then be used for a wide range of uses, including cloud provider selection and security evaluation. Additional information about the CAIQ process can be found on the Cloud Security Alliance site https://cloudsecurityalliance.org/.

InterSystems has completed this questionnaire with the answers below. The questionnaire has been completed using the current CSA CAIQ standard, v3.1.
If you have specific questions about this document, please engage with your InterSystems account representative.

The answers contained in this CAIQ version 3.1 are related to specific InterSystems Cloud Services on AWS as listed here:

HealthShare Unified Care Record (UCR)
Intended Use: HealthShare Unified Care Record is a data aggregation and sharing platform for patient-centric clinical data. It is intended to consolidate data from multiple clinical and non-clinical systems in a wide range of formats into a single integrated record. It is also intended to allow controlled access to the records based on configurable consent rules.

Limitations: The UCR is a secondary repository of health information for a patient. It is not intended to serve as the primary or fully complete repository of health information for a patient.

Data in the UCR must not be used as the sole basis for medical decision making.
The UCR must not be used as a lossless, unaltered archive of medical information. The UCR processes data prior to storage in the UCR storage format (Summary Document Architecture, or SDA). This processing may modify the data, such as transforming invalid or nonstandard data to valid standard values, adding default values for missing data, and omitting unsupported data. Customers may also apply custom data transformations to incoming data prior to storage in the UCR.

HealthShare Health Connect
Intended Use: Health Connect is communication middleware intended to facilitate interoperability and connection among disparate data systems. It is intended to provide health information managers the ability to translate, normalize, and reconcile data from disparate sources.

HealthShare Clinical Viewer (foundation)
Intended Use: HealthShare Clinical Viewer is intended to allow healthcare professionals to view clinical and administrative information about a patient and thereby help with clinical decision-making as a secondary repository of health information. Patient data from HealthShare Foundation Products populates the Clinical Viewer allowing it to span all care settings supported by the HealthShare Unified Care Record. As a single longitudinal record of a patient within an organization, the Clinical Viewer provides accurate and up-to-date information about services and care provided to the patient and makes it possible to discern how the information relates across the patient's healthcare journey.

Limitations: The Clinical Viewer is a secondary repository of health information for a patient. It is not intended to serve as the primary or fully complete repository of health information for a patient.

Data in the Clinical Viewer must not be used as the sole basis for medical decision making.

The Clinical Viewer must not be used as a lossless, unaltered archive of medical information. The UCR, on which the Clinical Viewer relies, processes data prior to storage in the UCR storage format (Summary Document Architecture, or SDA). This processing may modify the data, such as transforming invalid or nonstandard data to valid standard values, adding default values for missing data, and omitting unsupported data. Customers may also apply custom data transformations to incoming data prior to storage in the UCR.

Pre-requisites: Requires HealthShare Unified Care Record.

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

CAIQv3.1

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
AIS-01.1	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			InterSystems	InterSystems uses industry standards (see the related official document: https://www.intersystems.com/isc-resources/wp-content/uploads/sites/24/Secure_Coding_Practices_WP.pdf) in association with the development of product. The Solution Offering is provided through AWS, which also uses such standards and is the accredited by AGID as a Cloud Service Provider (CSP). In addition, according to the CAIQ for AWS the requirement is also guaranteed by AWS itself (See https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf)
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			InterSystems	All code used to deliver the relevant offering is analyzed by an automated tool.
AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	X			InterSystems	All code, used to deliver the relevant offerings, goes through a peer-review process before release to manufacturing.
AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			InterSystems	The InterSystems Third Party Risk Management process requires contractually any third party developing code for use in or with InterSystems products to adher to code development processes compliant with the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS).
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			InterSystems	All solution implementation deployed by InterSystems have penetration and vulnerability testing performed before any go-live process.
AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			Shared	Security requirements for deployment and operation of cloud-based solutions for customer are provided in the Global Privacy & Security Requirements addendum under the managed services agreement. See, https://www.intersystems.com/MSGPSS.
AIS- 02.2	Are all requirements and trust levels for customers access defined and documented?	X			InterSystems	A component of the implementation of the customer solution includes the definition and documentation of the role-based access to be deployed by the customer to access the solution.
AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?			X	Customer	Customer determines appropriate data management process to be implemented in the solution that can use existing capabilities of our product for audit and data integrity.
AIS-03.2	Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			Customer	The customer can implementation integrity routines in the solution or from other software sources, including third party SDK/IDE.
AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			Combined	The solution (and underlying AWS infrastructure) Data Security Architecture was designed to incorporate industry leading practices. Refer to ISO 27001 standard, Annex A, domain 10.8 for additional details.
AAC-01.1	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	X			Combined	The InterSystems Global Trust program includes periodic audits that include independent internal and external assessments to validate the control design and operational effectiveness of the InterSystems control environment. AWS has established a formal periodic audit program regarding AWS controls.
AAC-01.2	Does your audit program take into account effectiveness of implementation of security operations?	X			Combined	The internal and external audits conducted by InterSystems (and AWS) assess the operational effectiveness of the information security controls.
AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			Combined	Upon executing an appropriate confidentiality agreement, InterSystems will share independent audit reports with the customer for the customer's use.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			AWS	Although AWS Security regularly engages carefully selected industry experts and independent security firms to perform recurring penetration testing, AWS do not share the results directly with their customers. Instead, the results are reviewed and validated by AWS auditors as part of their external security audits of the AWS cloud service infrastructure. Customers can request from InterSystems that penetration testing be preformed and InterSystems can request from AWS permission to conduct penetration testing to or originating from any AWS resources as long as they are limited to the Customer s instances and the testing requested by the Customer does not violate the AWS Acceptable Use Policy.
AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			InterSystems	In coordinatation with the AWS infrastructure testing noted in AAC-02.2, InterSystems conducts penetration testing of the customer solution and shares the results with the customer.
AAC-02.4	Do you conduct internal audits at least annually?	X			InterSystems	Internal audits are performed at a regular basis to cover the delivery of Managed Services supporting the customer solution using an ISO Annex SL approach. The Global Trust function that performs internal audit processes operates independently of Managed Services and establishes a risk based approach to reviewing compliance to standards at InterSystems.
AAC-02.5	Do you conduct independent audits at least annually?	X			Combined	InterSystems maintains a formal audit program that include independent external audits regarding the design of controls and operational effectiveness for information security under the ISO 27001 standard. AWS has external independent assessments validate the implementation and operating effectiveness of the AWS control environment.
AAC-02.6	Are the results of the penetration tests available to tenants at their request?	X			InterSystems	InterSystems conducts penetration testing of the customer solution and shares the results with the customer. Although AWS Security regularly engages carefully selected industry experts and independent security firms to perform recurring penetration testing, AWS do not share the results directly with their customers.
AAC-02.7	Are the results of internal and external audits available to tenants at their request?	X			Combined	InterSystems provides third-party attestations, certifications, Service Organization Controls (SOC) reports and other relevant compliance reports directly to our customers under NDA. AWS also provides third-party attestations, certifications, Service Organization Controls (SOC) reports and other relevant compliance reports with InterSystems under NDA. Both InterSystems and AWS share the results of their respective internal audits with each organization's external auditors but not directly with customers.
AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			All	The Global Trust monitors legislative and regulatory requirements relative to the delivery of the InterSystems Managed Service. AWS maintains relationships with internal and external parties to monitor legal, regulatory, and contractual requirements. The customer is responsible for its own monitoring of regulatory requirements relating to its use and operation of the customer's solution.
BCR-01.1	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			Combined	InterSystems delivers Managed Services using a business continuity and disaster recovery process consistent with ISO 22301. AWS provides business continuity and disaster recovery through a framework to recover and reconstitute the AWS infrastructure through an Activation and Notification Phase, a Recovery Phase, and a Reconstitution Phase.
BCR-01.2	Do you have more than one provider for each service you depend on?	X			Combined	Both InterSystems and AWS plan the delivery of services using an N+1 architecture to eliminate, the extent possible, single points of failure.
BCR-01.3	Do you provide a disaster recovery capability?	X			Customer	InterSystems makes available to customers the AWS flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone.
BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?	X			Combined	InterSystems Managed Services includes ongoing solution health and performance monitoring. Further, AWS maintains a ubiquitous security control environment across all regions. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing an n+1 redundancy model to ensure system availability in the event of component failure. Components (N) have at least one independent backup component (+1), so the backup component is active in the operation even if all other components are fully functional in order to eliminate single points of failure.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
BCR-01.5	Do you provide access to operational redundancy reports, including the services you rely on?		X		N/A	The information is shared with independent third party auditors and the results of those audit engagements are shared with customers.
BCR-01.6	Do you provide a tenant-triggered failover option?	X			Customer	InterSystems (and AWS) provides publicly available mechanisms for customers to report security and/or privacy events, including disasters
BCR-01.7	Do you share your business continuity and redundancy plans with your tenants?	X			Shared	InterSystems works with the customer to integrated a business continuity and disaster recovery plan for the customer's solution with the customer's overall BC/DR plan.
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Combined	Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on business continuity controls.
BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	X			AWS	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11 and link below for Data center controls overview: https://aws.amazon.com/compliance/datacenter/controls/
BCR-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	X			AWS	AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provide additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. Please refer to link below for Data center controls overview: https://aws.amazon.com/compliance/datacenter/controls/
BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			Combined	InterSystems and AWS make Information System Documentation available internally to their respective personnel through the use of each organization's Intranet sites. Refer to ISO 27001 Appendix A Domain 12
BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?	X			AWS	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11 or AWS SOC2 report and link below for Data center controls overview: https://aws.amazon.com/compliance/datacenter/controls/
BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		X		AWS	Each AWS data center is evaluated to determine the controls that must be implemented to mitigate, prepare, monitor, and respond to natural disasters or malicious acts that may occur. Refer to ISO 27001 standard, Annex A domain 11 and link below for Data center controls overview: https://aws.amazon.com/compliance/datacenter/controls/
BCR-07.1	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	X			AWS	AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. In order to ensure maintenance procedures are properly executed, AWS assets are assigned an owner, tracked and monitored with AWS proprietary inventory management tools. AWS asset owner procedures are carried out by method of utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. Third party auditors test AWS equipment maintenance controls by validating that the asset owner is documented and that the condition of the assets are visually inspected according to the documented maintenance policy.
BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?	X			AWS	AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. In order to ensure maintenance procedures are properly executed, AWS assets are assigned an owner, tracked and monitored with AWS proprietary inventory management tools. AWS asset owner procedures are carried out by method of utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. Third party auditors test AWS equipment maintenance controls by validating that the asset owner is documented and that the condition of the assets are visually inspected according to

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			AWS	AWS equipment is protected from utility service outages in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provide additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities
BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			AWS	Policies and Procedures for continued service operations have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/compliance/programs
BCR-09.2	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			All	Both InterSystems and AWS perform Business Impact Assessments related to their service delivery to assign business criticality to supporting processes and identification of operational processes, teams and dependencies to sustain operations during a business disruption. The customer would develops a Business Impact Assessment relative to the customer's use and operation of the customer solution.
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations roles?	X			Combined	InterSystems and AWS make Information System Documentation available internally to their respective personnel through the use of each organization's Intranet sites. Refer to ISO 27001 Appendix A Domain 12.
BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	X			All	InterSystems and AWS each maintain a retention policy applicable to their respective internal data and system components in order to continue operations of business and services. Critical system components, including audit evidence and logging records, are replicated and backups are maintained and monitored. Customers retain control and ownership of their content. The customer retains complete control of how they choose to classify their content, where it is stored, used and applicable
BCR-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	X			All	InterSystems and AWS each maintain a retention policy applicable to their respective internal data and system components in order to continue operations of business and services. Critical system components, including audit evidence and logging records, are replicated and backups are maintained and monitored. Customers retain control and ownership of their content. The customer retains complete control of how they choose to classify their content, where it is stored, used and applicable
BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			Shared	InterSystems provides backup and recovery consistent with the contractual requirements for the delivery of the customer solution. Customer is responsible to determine the nature and extent required to ensure compliance with relevant regulatory, statutory, and legal requirements
BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			Combined	If the customer takes advantage of AWS recovery utilities as part of the customer solution, the instance can be recovered if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair
BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?		X		N/A	InterSystems maintains the virtual machines for the environments deployed in support of the customer solution.
BCR-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?	X			Customer	Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions).
BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	X			Shared	InterSystems provides testing of backup and recovery consistent with the contractual requirements for the delivery of the customer solution and recommends testing on at least an annual basis. The redundancy mechanism for the customer solution is tested every time a change to the platform is applied (upgrade, patch install).
CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			Combined	The design of all new services or any significant changes to current services follow secure software development practices and are controlled through a project management system with multi-disciplinary participation. InterSystems offers a platform for developing complete integration solutions. If a specific component or service that is not included in the platform is needed, the customer must develop or obtain it and manage its life cycle.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
CCC-02.1	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	X			All	Both InterSystems and AWS apply a systematic approach to managing change for their respective delivery services to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on internal guidelines and tailored to the specifics of each service. More information is available from InterSystems through the Documentation Portal (https://docs.intersystems.com/). Refer to AWS SOC 2 report for additional information on AWS change management mechanisms.
CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	X			All	Both InterSystems and AWS apply a systematic approach to managing change for their respective delivery services to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on internal guidelines and tailored to the specifics of each service. More information is available from InterSystems through the Documentation Portal (https://docs.intersystems.com/). Refer to AWS SOC 2 report for additional information on AWS change management mechanisms.
CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			Combined	InterSystems and AWS maintain ISO 9001 certifications, which is an independent validation of each organization's quality system and determined that those organization's activities comply with ISO 9001 requirements.
CCC-03.2	Is documentation describing known issues with certain products/services available?	X			Combined	InterSystems communicates alerts and advisories about privacy and security issues to the customer through direct notifications and the Product Alerts and Advisories page (https://www.intersystems.com/support-learning/support/product-news-alerts/). AWS Security Bulletins notify customers of security and privacy events. Customers can subscribe to the AWS Security Bulletin RSS feed on our website. Refer to https://aws.amazon.com/security/security-bulletins/ AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to AWS Service Health Dashboard.
CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			Combined	InterSystems maintains product support and vulnerability handling processes to address product bugs or security vulnerabilities reported to InterSystems by the customer. These processes are supported through communication channels with the customer using WRC Direct, https://wrc.intersystems.com, which is used by the customer to notify InterSystems of potential bugs and security vulnerabilities. The AWS Security team notifies and coordinates with the appropriate Service Teams when conducting security-related activities within the system boundary. Activities include, vulnerability scanning, contingency testing, and incident response exercises.
CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?	X			Combined	InterSystems has a Quality Control department that tests and ensures the quality of the platform and its component or services before releasing it. AWS uses a quality management system surrounding the development of software related to AWS services.
CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?			X	N/A	InterSystems does not outsource any software development activities.
CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			Combined	The InterSystems system development lifecycle (SDLC) incorporates industry best practices, which include formal design reviews by the Quality Control department, threat modeling, and completion of a threat and vulnerability risk assessment. A white paper about InterSystems Secure Coding Practices is available at https://www.intersystems.com/isc-resources/wp-content/uploads/sites/24/Secure_Coding_Practices_WP.pdf
CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			All	For the underlying platform and cloud infrastructure, general users do not have rights to install software to customer environments. Before being installed to production environments, all software goes through standard change management process enforced by InterSystems or AWS, including appropriate approvals. Customer can restrict the customer personnel access to the solution in order to limit them in terms available operation and functionalities, preventing any unauthorized software change or installation. Moreover the soluion does not require any external software so any new software would be considered a module to be integrated and outside the platform control.
CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		X		N/A	InterSystems and AWS do not provide this level of granularity to their customers. Both notify customers of changes to the underlying service offering in accordance with their contractual commitments.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?	X			Combined	InterSystems and AWS apply a systematic approach to managing change to ensure that all changes to a production environment are reviewed, tested, and approved. Each organization's change management approach requires that the following steps be complete before a change is deployed to the production environment: 1. Document and communicate the change via the appropriate change management tool. 2. Plan implementation of the change and rollback procedures to minimize disruption. 3. Test the change in a logically segregated, nonproduction environment. 4. Complete a peer-review of the change with a focus on business impact and technical rigor. The review should include a code review. 5. Attain approval for the change by an authorized individual.
CCC-05.3	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	X			Combined	InterSystems and AWS require that access to production environments by non-operations personnel must be through an explicit request for access through the appropriate access management system, have the access reviewed and approved by the appropriate owner, and, upon approval, obtain authentication. Service teams maintain service specific change management standards that inherit and build on each organization's change management requirements.
DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	X			AWS	AWS provides the ability to tag EC2 resources. A form of metadata, EC2 tags can be used to create user- friendly names, enhance searchability, and improve coordination between multiple users. The AWS Management Console also supports tagging. AWS does not provide hardware to customers but virtual machines are assigned to customers as part of the EC2 service.
DSI-01.2	Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			X	N/A	No hardware is provided in the delivery of a customer solution.
DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?		X		Customer	InterSystems offers the solution through an integration platform; how to manage and document data flows and the data stored within the platform is part of the solution design and it is a customer s responsibility.
DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	X			Combined	The customer in agreement with InterSystems and AWS designate in which physical region their content will be located. InterSystems and AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities.
DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			Combined	Both InterSystems and AWS provide standardized encryption algorithms for integration with the customer solution, which enables the customer to encrypt all traffic to and from the solution.
DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			All	Both InterSystems and AWS provide standardized encryption algorithms for integration with the customer solution, which enables the customer to encrypt all traffic to and from the solution. The customer would determine which algorithms to integrate as well as be responsible for the management of any encryption keys.
DSI-04.1	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?			X	Customer	The InterSystems platform can deployed as the customer determines appropriate using the data security capabilities of the platform. Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.
DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?			X	Customer	The InterSystems platform can deployed as the customer determines appropriate using the data security capabilities of the platform. Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.
DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	Customer	The InterSystems platform can deployed as the customer determines appropriate using the data security capabilities of the platform. Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.
DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			InterSystems	InterSystems does not access, process, or change customer data in the course of providing the services without customer approval. InterSystems customers maintain ownership of their data and InterSystems does not utilize customer data for testing (production or non-production)

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?			X	Customer	InterSystems customers maintain ownership of their data and data management is the responsibility of the customer and the customer must to ensure that data is not copied, moved or misused.
DSI-07.1	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			Combined	The platform can support several methods to perform secure data deletion related to the solution and it is the responsibility of the customer to decide whether to use these methods or not. With regard to the cloud infrastructure, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. Refer to AWS: Overview of Security Processes Whitepaper for additional details - available at: http://aws.amazon.com/security/security-learning/
DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			InterSystems	InterSystems provides in the platform documentation processes for the secure deletion of data from the solution at the termination of the service.
DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			AWS	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools
DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X			AWS	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools.
DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	X			AWS	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provide additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?	X			Customer	Using delegated authentication, the platform allows integrating geographic locator systems to its authentication methods.
DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			AWS	AWS manages equipment identification in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			All	With regard to the platform, because the relocation or transfer of the customer solution is a complex process, the process must be fully analysed and coordination and agreement are required between the customer, InterSystems, and AWS before proceeding. As for hardware, the environments used for the delivery of the customer solution using AWS services are managed by authorized personnel and are located in an AWS managed data centers. Media handling controls for the data centers are managed by AWS in alignment with the AWS Media Protection Policy. This policy includes procedures around access, marking, storage, transporting, and sanitation. Live media transported outside of data center secure zones is escorted by authorized personnel.
DCS-05.1	Can you provide tenants with your asset management policies and procedures?	X			Combined	InterSystems and AWS do not provide confidential AWS policies and procedures directly to the customers. Both InterSystems and AWS engage with external certifying bodies and independent auditors to review and validate operational compliance with policies. AWS SOC reports provide additional details on the specific asset management related policies and control activities executed by AWS.
DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			Combined	InterSystems and AWS engage with external certifying bodies and independent auditors to review and validate operational compliance with with policies. AWS SOC reports provide additional details on the specific physical security control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			Combined	In alignment with ISO 27001 standard, all InterSystems and AWS employees complete periodic Information Security training which includes an assessment and requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. For more information about InterSystems Data Protection, Privacy, and Security practices see https://www.intersystems.com/GTDPPS. Refer to AWS: Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security/security-learning/ AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. In addition, AWS SOC 1 and SOC 2 reports provides further information.
DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	X			AWS	Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass twofactor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy
DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			AWS	Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass twofactor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy
DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	X			AWS	Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy.
EKM-01.1	Do you have key management policies binding keys to identifiable owners?			N/A	Customer	The platform allows the customer to generate keys, which must be managed by the customer. Consistent with industry best practices, InterSystems cannot manage the encryption keys for a customer solution and, as such, InterSystems does not hold, manage or store any encryptiion keys for customers.
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	X			Customer	The customer can create as many encryption keys as needed and associate them to a specific scope installation tenant or otherwise.
EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?		X		Customer	The platform allows the customer to generate keys, which must be managed by the customer. Consistent with industry best practices, InterSystems cannot manage the encryption keys for a customer solution and, as such, InterSystems does not hold, manage or store any encryptiion keys for customers
EKM-02.3	Do you maintain key management procedures?			N/A	Customer	The platform allows the customer to generate keys, which must be managed by the customer. Consistent with industry best practices, InterSystems cannot manage the encryption keys for a customer solution and, as such, InterSystems does not hold, manage or store any encryptiion keys for customers
EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?			N/A	Customer	The platform allows the customer to generate keys, which must be managed by the customer. Consistent with industry best practices, InterSystems cannot manage the encryption keys for a customer solution and, as such, InterSystems does not hold, manage or store any encryptiion keys for customers.
EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X			Customer	Customer can use the key management mechanisms provide by the platform in the customer solution for integration as determined by the customer.
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?			N/A	Customer	The platform offers an “at rest” encryption mechanism that can be applied to specific information stored in the database or across the entire database.
EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			Customer	The platform provide encryption mechanisms or allows the customer to use their own encryption mechanisms for at-rest and in-transit data.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			Combined	Internally, both InterSystems and AWS establish and manage cryptographic keys for required cryptography employed within the platform and cloud infrastructure, respectfully. Each organization produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An secure key and credential manager is used to create, protect and distribute symmetric keys, credentials needed on hosts, RSA public/private keys and X.509 Certifications.
EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?			N/A	Customer	The platform allows the customer to generate keys, which must be managed by the customer. Consistent with industry best practices, InterSystems cannot manage the encryption keys for a customer solution and, as such, InterSystems does not hold, manage or store any encryptiion keys for customers.
EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			Customer	The platform allows the customer to generate keys, which must be managed by the customer. Consistent with industry best practices, InterSystems cannot manage the encryption keys for a customer solution and, as such, InterSystems does not hold, manage or store any encryptiion keys for customers.
EKM-04.3	Do you store encryption keys in the cloud?			N/A	Customer	The platform allows the customer to generate keys, which must be managed by the customer. Consistent with industry best practices, InterSystems cannot manage the encryption keys for a customer solution and, as such, InterSystems does not hold, manage or store any encryptiion keys for customers.
EKM-04.4	Do you have separate key management and key usage duties?			N/A	Customer	The platform allows the customer to generate keys, which must be managed by the customer. Consistent with industry best practices, InterSystems cannot manage the encryption keys for a customer solution and, as such, InterSystems does not hold, manage or store any encryptiion keys for customers.
GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			AWS	AWS has established baseline infrastructure standards, including for network components. AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet. Firewall policies (configuration files) are automatically pushed to firewall devices every 24 hours.
GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			Combined	The platform has the capability to monitor all the accesses and the operations performed against in the customer solution and provide relevant reporting to allow for monitoring of security level adopted by the customer. The platform can also be configured to monitor external elements of the infrastructure related to the operation of the customer solution.
GRM-02.1	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X			All	The platform configuration is monitored for compliance with the Global Privacy & Security Specification, available at https://www.intersystems.com/, which establishes the level of security related to the delivery of the operational platform through Managed Services. AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet. Firewall policies (configuration files) are automatically pushed to firewall devices every 24 hours. The customer has responsibility for ensuring its operational use of the customer solutiion, including end user access, external gateway transfers, data transformations, and data retention comply with the obligations of the customer for data protection and classification.
GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	X			All	In alignment with ISO 27001 standard, both InterSystems and AWS maintain a Risk Management program to mitigate and manage risk. In addition, the customer retains control and ownership of their data and can implement data residency, security and retention requirements based on appropriate and relevant legal and regulatory requirements.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			Combined	InterSystems maintains the Global Trust program designed to provide assurances to customers and stakeholders regarding obligations for data protection, privacy, security, and risk governance and ensure appropriate risk management processes throughout the organization. Under Global Trust all executives, managers, and employees have responsibility for compliance with the required data protection, privacy, and security controls defined under Global Trust and relevant to each area of responsibility. For the Global Trust Data Protection, Privacy, and Security Policy, see https://www.intersystems.com/GTDPPS, and for information about the Global Trust program, see https://www.intersystems.com/globaltrust. For AWS compliance, refer to AWS Risk & Compliance whitepaper for additional details - available at http://aws.amazon.com/compliance.
GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			Combined	Customer can review the InterSystems Global Trust Data Protection, Privacy and Security Policy, which defines the Information Security Management Program, at https://www.intersystems.com/GTDPPS. For information regarding the AWS ISMP, refer to the AWS Compliance ISO 27001 FAQ website: https://aws.amazon.com/compliance/iso27001-faqs/
GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	X			InterSystems	InterSystems ISMP is reviewed by the Global Trust management team on an annual basis.
GRM-05.1	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X			InterSystems	The InterSystems Data Protection Officer oversees the Global Trust program, which integrates the risk management processes with leadership through periodic management reviews to ensure alignment with business objectives while incorporating risk governance and appropriate and necessary controls into operational processes.
GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X			InterSystems	All InterSystems Personnel, which includes employees and contractors, can access the policies, procedures, and standards throught the Global Trust intranet site to ensure alignment with relevant data protection, privacy, and information security standards, including ISO 27001.
GRM-06.2	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?					The InterSystems Data Protection Officer authorizes the information security policies that support the risk management processes and technical and organizational controls for the Global Trust program. The Global Trust program incorporates an integrated management system appropriate tailored on ISO Annex SL to ensure roles and responsibilities for the management of risk, including data protection, privacy, and security risks, are addresses and understood.
GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			InterSystems	All third party vendors must adher to data protection, privacy, and security requirements defined to address the operational model under Global Trust.
GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X			InterSystems	Information about the Global Trust program, including technical and organization controls and measures are available through the Global Trust site, https://www.intersystems.com/globaltrust.
GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			InterSystems	Information about the Global Trust program, including technical and organization controls and measures are available through the Global Trust site, https://www.intersystems.com/globaltrust.
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			InterSystems	The Global Trust program includes a formal sanctions policy to address violations of data protection, privacy, and security policies.
GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			InterSystems	The Global Trust program includes a formal sanctions policy to address violations of data protection, privacy, and security policies.
GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			InterSystems	The risk management process within Global Trust incorporates issue management to ensure the updating of policies and procedures based upon changes in identified risks and requirements.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?		X		N/A	The policies and procedures supporting the Global Trust program are subject to change based on various inputs, including, risk assessment activities, regulatory or legal guidance, follow-up to audit reviews etc. We do not provide policy details to customers, but these are validated and/or certified by internal audits and through independent external audits that confirm our compliance with ISO 27001. Any changes to the Data Protection, Privacy, and Security Policy is published to customers as part of published compliance reports and audit documents on the Global Trust site, see https://www.intersystems.com/GTDPPS.
GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			InterSystems	InterSystems privacy and security policies are reviewed by the Global Trust management team on an annual basis.
GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			InterSystems	The risk management process within Global Trust incorporates issue management that includes risk assessments as necessary, but at least annually, to evaluate and rate both the inherent and residual risks to ensure the updating of policies and procedures based upon changes in identified risks and requirements.
GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X			InterSystems	The risk management process within Global Trust incorporates issue management that includes risk assessments as necessary, but at least annually, to evaluate and rate both the inherent and residual risks to ensure the updating of policies and procedures based upon changes in identified risks and requirements.
GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	X			InterSystems	The risk management process within Global Trust incorporates issue management that includes risk assessments as necessary, but at least annually, to evaluate and rate both the inherent and residual risks to ensure the updating of policies and procedures based upon
GRM-11.2	Do you make available documentation of your organization-wide risk management program?		X			The Global Trust program is validated and/or certified by internal audits and through independent external audits that confirm our compliance with ISO 27001.
HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			Combined	Upon termination, Human Resources at both InterSystems and AWS ensures that a formal checklist, which includes steps for access removal and collection of assets, is completed by HR or the terminated employee's manager. The following processes must be addressed upon the termination of an employee or contractors: • Communicating termination responsibilities, such as security requirements, legal responsibilities, and nondisclosure obligations to terminated personnel. • Revoking information system access (including disabling any credentials). • Retrieving all company-information system-related property (e.g. authentication tokens, keys, badges). • Disabling badge access
HRS-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?	X			Combined	Upon termination of employee or contractors, company assets in their possessions are retrieved on the date of termination. In case of immediate termination, the employee/contractor manager retrieves all company assets (e.g., Authentication tokens, keys, badges) and escorts them out of the company facility.
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			Combined	InterSystems and AWS conduct criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee s position and level of access to facilities and relevant information assets, including customer assets.
HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			Combined	In alignment with ISO 27001 standard, employees and contractors complete periodic role-based training that includes privacy and security training and requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
HRS-03.2	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	X			Combined	InterSystems Personnel sign a non-disclosure agreement prior to being provided any credentials for access and must also attest to their acceptance of their data protection, privacy, and security obligations under the GLobal Trust program. AWSS Personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy.
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			Combined	The Human Resources team at both InterSystems and AWS defines internal management responsibilities to be followed for termination and role change of employees and vendors.
HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			Combined	Upon termination, Human Resources at both InterSystems and AWS ensures that a formal checklist, which includes steps for access removal and collection of assets, is completed by HR or the terminated employee's manager. The following processes must be addressed upon the termination of an employee or contractors: • Communicating termination responsibilities, such as security requirements, legal responsibilities, and nondisclosure obligations to terminated personnel. • Revoking information system access (including disabling any credentials). • Retrieving all company-information system-related property (e.g. authentication tokens, keys, badges). • Disabling badge access.
HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization s facilities)?	X			All	InterSystems and AWS maintain formal access control policies that are reviewed and updated on an annual basis (or when any major change to the platform or cloud infrastructure occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment and employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. All access from remote devices to either the InterSystems or the AWS corporate environment is managed via VPN and MFA. The InterSystems Managed Services AWS tenent is separate and distinct for any other AWS tenents held by InterSystems. The AWS production network is separated from the corporate network by multiple layers of security documented in various control documents. Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer s content.
HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			InterSystems	The Global Trust program reviews and, as necessary, updates related non-disclosure and confidentiality agreements on a periodic basis but not less than annually.
HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			Shared	The Global Privacy and Security Specification, https://www.intersystems.com/MSGPSS, addresses the responsibilities of InterSystems and the customer relating to access to the solution with InterSystems responsible for administrative accounts and the customer responsible for end user accounts (Authorized Persons).
HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			Combined	Both InterSystems and AWS have implemented data handling and classification requirements that provide specifications around: • Data encryption • Content in transit and during storage • Access • Retention • Physical controls • Mobile devices • Data handling requirements Employees are required to review and sign-off on an employment contract, which acknowledges their responsibilities to overall data protection, privacy, and security policies
HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?			N/A	InterSystems	InterSystems does not permit the use of BYOD devices to access Managed Services environments.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			Combined	All InterSystems Personnel complete general privacy and security training which require an acknowledgement to complete. For specific trainings about cloud security, the cloud provider provides advanced security trainings, which InterSystems Personnel are required to attend, if they have the need to work on cloud.
HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			Combined	In alignment with ISO 27001 standard, all InterSystems and AWS employees complete periodic Information Security training on at least an annual basis, which requires an acknowledgement to complete, which is documented. Compliance audits are periodically performed to validate that employees understand and follow the established policies.
HRS-09.3	Do you document employee acknowledgment of training they have completed?	X			Combined	In alignment with ISO 27001 standard, all InterSystems and AWS employees complete periodic Information Security training on at least an annual basis, which requires an acknowledgement to complete, which is documented. Compliance audits are periodically performed to validate that employees understand and follow the established policies.
HRS-09.4	Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			Combined	In alignment with ISO 27001 standard, all InterSystems and AWS employees complete periodic Information Security training on at least an annual basis, which requires an acknowledgement to complete, which is documented. Compliance audits are periodically performed to validate that employees understand and follow the established policies.
HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	X			Combined	In alignment with ISO 27001 standard, all InterSystems and AWS employees complete periodic Information Security training on at least an annual basis, which requires an acknowledgement to complete, which is documented. Compliance audits are periodically performed to validate that employees understand and follow the established policies.
HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			Combined	In alignment with ISO 27001 standard, all InterSystems and AWS employees complete periodic Information Security training on at least an annual basis, which requires an acknowledgement to complete, which is documented. Compliance audits are periodically performed to validate that employees understand and follow the established policies.
HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			InterSystems	The Global Trust program uses various communication channels to include awareness, training, and education to ensure effective understanding of the responsibilities related to the protection of information and obligations to safeguard the platform with regard to information security controls.
HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			InterSystems	The Global Trust program uses various communication channels to include awareness, training, and education to ensure effective understanding of the responsibilities related to the protection of information and obligations to safeguard the platform with regard to information security controls.
HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			InterSystems	The Global Trust program uses various communication channels to include awareness, training, and education to ensure effective understanding of the responsibilities related to the protection of information and obligations to safeguard the platform with regard to information security controls.
HRS-11.1	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			InterSystems	InterSystems has established baseline infrastructure standards in alignment with industry best practices. These include automatic lockout after defined period of inactivity and technical/organizational measures regarding protection for unattended workspaces.
HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X			InterSystems	InterSystems has established baseline infrastructure standards in alignment with industry best practices. These include automatic lockout after defined period of inactivity and technical/organizational measures regarding protection for unattended workspaces.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			Combined	InterSystems and AWS maintain formal access control policies that are reviewed and updated on an annual basis (or when any major change to the platform or cloud infrastructure occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment and employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. All access from remote devices to either the InterSystems or the AWS corporate environment is managed via VPN and MFA. The InterSystems Managed Services AWS tenent is separate and distinct for any other AWS tenents held by InterSystems. The AWS production network is separated from the corporate network by multiple layers of security documented in various control documents. Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer s content.
IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			Combined	InterSystems Managed Services monitors the platform underlying the customer solution and regularly reviews administrative level access for any improper or unauthorize access. Further, AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on InterSystems AWS teams receive automated alerts in the event of an monitoring event or audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved.
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			Combined	Access privilege reviews are triggered upon job and/or role transfers initiated from HR system. IT access privileges are reviewed on a quarterly basis by appropriate personnel on a regular cadence. IT access from AWS systems is terminated within 24 hours of termination or deactivation.
IAM-02.2	Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	X			Combined	In alignment with ISO 27001, InterSystems and AWS have a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. Access control procedures are systematically enforced through proprietary tools. Refer to ISO 27001 Annex A, domain 9 for additional details.
IAM-02.3	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	X			Combined	InterSystems and AWS have a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. InterSystems and AWS employ the concept of least privilege, allowing only the necessary access for users to accomplish their job function.
IAM-02.4	Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X			Customer	Data segmentation in the platform can be achieved in several ways, both physically and logically. Procedures to configure segmentation are described in the platform documentation. Technical measures are granted by the monitoring system and the business intelligence components of the platform.
IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X			Customer	The platform enforces data access permissions based on the rules of Authentication and Authorization; in addiction, Accountability is achieved granting appropriate privileges to each user based on its role.
IAM-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	X			Customer	The platform allows several methods to authenticate (login and password, via Kerberos, via LDAP, through Operating System, based on the delegate authentication, allowing the use of tokens, biometrics, etc.) at the same time for the same system or function; all the methods can be put in a hierarchical order to grant multifactor authentication.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
IAM-02.7	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		X		Customer	Customers are responsible for the management of all end user access.
IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			Combined	InterSystems and AWS have a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. InterSystems and AWS employ the concept of least privilege, allowing only the necessary access for users to accomplish their job function.
IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			Combined	InterSystems Personnel with a business need to access the customer solution are required to first use multi-factor authentication, distinct from their normal corporate InterSystems credentials, to gain access to the bastion host for accessing the environments related to the customer solution. AWS personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate AWS credentials, to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked.
IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			Combined	InterSystems Personnel with a business need to access the customer solution are required to first use multi-factor authentication, distinct from their normal corporate InterSystems credentials, to gain access to the bastion host for accessing the environments related to the customer solution. AWS personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate AWS credentials, to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked.
IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			Shared	InterSystems develops a customer-specific Information Security Management Plan with the customer for the security controls related to the customer solution, which will include methods for the customer to determine the proper controls for seggration of duties related to access to the customer solution.
IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			InterSystems	Access to the InterSystem code repository is strictly limited to only personnel with appropriate need-to-know and all access to the code repository is logged for audit purposes.
IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			InterSystems	The platform includes access logging capabilities.
IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?	X			InterSystems	All third party that will have access to customer environments and/or customer information assets are reviewed and approved through the Third Party Risk Management process maintained as part of the Global Trust program.
IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	X			InterSystems	InterSystems has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy), which includes appropriate compensating controls to address third party access. The policy addresses purpose, scope, roles, responsibilities and management commitment. InterSystems employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function.
IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	X			Combined	InterSystems and AWS have a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. InterSystems and AWS employ the concept of least privilege, allowing only the necessary access for users to accomplish their job function.
IAM-08.2	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	X			Combined	InterSystems and AWS have a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. InterSystems and AWS employ the concept of least privilege, allowing only the necessary access for users to accomplish their job function.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
IAM-08.3	Do you limit identities' replication only to users explicitly defined as business necessary?	X			Combined	Access is allocated based on least privilege, approved by an authorized individual prior to access provisioning, and assigned a different user ID than used for normal business use. Duties and areas of responsibility (for example, access request and approval, change management request and approval, change development, testing and deployment, etc.) are segregated across different individuals to reduce opportunities for an unauthorized or unintentional modification or misuse. Group or shared accounts are not permitted.
IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			Combined	Unique user identifiers are created as part of the onboarding workflow process in the human resources management system. The device provisioning process helps ensure unique identifiers for devices. Both processes include manager approval to establish the user account or device. Initial authenticators are delivered to users directly and to devices as part of the provisioning process. Administrative account authenticators are provided to the requestor as part of the account creation process after the identity of the requestor is verified.
IAM-09.2	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X			Combined	Controls are established to address the threat of inappropriate insider access. All certifications and third party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.
IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			Combined	In alignment with ISO 27001 standard, all access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked
IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			Combined	In alignment with ISO 27001 standard, all access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked
IAM-10.3	Do you ensure that remediation actions for access violations follow user access policies?	X			InterSystems	The formal sanctions policy requires risk remediation following violation of Global Trust policies.
IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?			X	N/A	Customer controls all end user access to customer solution. If InterSystems discovers any unauthorized administrative access to customer solution, through Global Trust, InterSystems will open an incident for response and resolution, including appropriate notification to the customer.
IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			Combined	Upon termination, Human Resources at both InterSystems and AWS ensures that a formal checklist, which includes steps for access removal and collection of assets, is completed by HR or the terminated employee's manager. The following processes must be addressed upon the termination of an employee or contractors: • Communicating termination responsibilities, such as security requirements, legal responsibilities, and nondisclosure obligations to terminated personnel. • Revoking information system access (including disabling any credentials). • Retrieving all company-information system-related property (e.g. authentication tokens, keys, badges). • Disabling badge access.
IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			Combined	Upon termination, Human Resources at both InterSystems and AWS ensures that a formal checklist, which includes steps for access removal and collection of assets, is completed by HR or the terminated employee's manager. The following processes must be addressed upon the termination of an employee or contractors: • Communicating termination responsibilities, such as security requirements, legal responsibilities, and nondisclosure obligations to terminated personnel. • Revoking information system access (including disabling any credentials). • Retrieving all company-information system-related property (e.g. authentication tokens, keys, badges). • Disabling badge access.
IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			Shared	The platform provide the necessary capabilities to integrate with a Single Sign-On solution for the customer to manage access.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	X			Shared	The platform can use open standard solutions for delegate authentication. Delegate authentication is a mechanism that allows to define a custom authentication solution based on any mechanism, integration and standard. The customer determines the process for the delegate authentication
IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X			Shared	The platform offers multiple options for federating customer identities.With federation, the customer can use single sign-on (SSO) to access the customer solution using credentials from the customer corporate directory. Federation uses open standards, such as Security Assertion Markup Language 2.0 (SAML), to exchange identity and security information between an identity provider (IdP) and an application.
IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	X			Shared	Customers can enable Policy Enforcement capability using their existing Identity Providers and established fine grained policies to manage permissions to the customer solution.
IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X			Shared	The platform supports the integration of both role-based and context-based entitlement to data in the customer solution.
IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			Shared	The platform provide capabilities to use strong MFA authentication optiosn depending on the customer requirements controlling access to the customer solution.
IAM-12.7	Do you allow tenants to use third-party identity assurance services?	X			Shared	The platform support the use of third party Identity Providers (IdP).
IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X			Shared	The platform provides capabilities to address password support consistent with NIST SP 800-63-3.
IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			Shared	The platform provides capabilities to address password support consistent with NIST SP 800-63-3.
IAM-12.10	Do you support the ability to force password changes upon first logon?	X			Shared	The platform provides capabilities to address password support consistent with NIST SP 800-63-3.
IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			Shared	The platform provides capabilities to address password support consistent with NIST SP 800-63-3.
IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			Combined	InterSystems and AWS have established and maintains company-wide policy that defines roles, responsibilities and classifications for managing changes to the production environment. Changes to services and features follow secure software development practices, which include a security risk review prior to launch. Developers that require access to production environments must explicitly request access through the access management system, have the access reviewed and approved by the appropriate owner, and upon approval obtain authentication. Service teams maintain service specific change management standards that inherit and build on the change management process.
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			All	InterSystems Managed Services conducts periodic vulnerability and penetration scans of the customer solution and the platform management interface. AWS Security performs regular vulnerability scans on the underlying cloud infrastructure in the AWS environment using a variety of tools. External vulnerability ssessments are conducted by an AWS approved third party vendor at least quarterly, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. The customer can choose to integrate AWS tools as part of the service delivering the customer solution (e.g. CloudWatch, CloudTrail, Amazon GuardDuty, Amazon Inspector)
IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	X			InterSystems	The audit system of the platform is controlled by the platform security restrictions and only authorized users can access it, but solely in read only mode and therefore cannot be altered by any user
IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?		X		Customer	Customer is responsible to ensure that the proper mapping of relevant legislation and regulation is done.
IVS-01.4	Are audit logs centrally stored and retained?	X			Shared	The platform uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an indeterminate period of time or a purge strategy can be adopted according to the laws and/or customer requirements.
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?		X		Customer	Customer is responsible for the regular review of user access logs. InterSystems does perform periodic access reviews of any administrative accounts.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?		X		N/A	The customer can determine if this service would be integrated into the customer solution to the extent the control is available through the capabilies of the AWS cloud infrastructure.
IVS-02.2	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?		X		N/A	The customer can determine if this service would be integrated into the customer solution to the extent the control is available through the capabilies of the AWS cloud infrastructure.
IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?		X		N/A	The customer can determine if this service would be integrated into the customer solution to the extent the control is available through the capabilies of the AWS cloud infrastructure.
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			InterSystems	The platform uses the OS clock in the default, but it can integrate any synchronized time-service protocols.
IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	X			InterSystems	This requirement is addressed within the terms of the agreement for the Managed Service delivery of the customer solution.
IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			InterSystems	This requirement is addressed within the terms of the agreement for the Managed Service delivery of the customer solution.
IVS-04.3	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			InterSystems	This requirement is addressed within the terms of the agreement for the Managed Service delivery of the customer solution.
IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			InterSystems	This requirement is addressed within the terms of the agreement for the Managed Service delivery of the customer solution.
IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			AWS	The Amazon EC2 hypervisor is based on open source platforms. Independent auditors regularly assess the security of Amazon EC2 for new and existing vulnerabilities and internal and external penetration teams regularly search for attack vectors. As such, Amazon EC2 is well suited for maintaining strong isolation between guest virtual machines. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with ISO 27001
IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			X	N/A	This is not part of the product offering.
IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X			Shared	InterSystems coordinates with the customer to develop the appropriate solution architecture, including necessary network infrastructure, as part of the business requirements for the customer solution.
IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X			Shared	InterSystems coordinates with the customer to develop the appropriate solution architecture, including necessary network infrastructure, as part of the business requirements for the customer solution.
IVS-06.4	Are all firewall access control lists documented with business justification?	X			Shared	InterSystems coordinates with the customer to develop the appropriate solution architecture, including necessary network infrastructure, as part of the business requirements for the customer solution.
IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			InterSystems	InterSystems deploys the platform for the customer solution through hardened images construct the baseline build standard necessary for the delivery of the operating solution.
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			InterSystems	Deployment of a customer solution must include multiple environments with Base, Test, and Production at a minimum. The extent of necessary environments will be determined by the customers and addressed in the terms of agreement for the delivery of the customer solution.
IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			X		This is not part of the product offering.
IVS-08.3	Do you logically and physically segregate production and non-production environments?	X			Shared	Non-production environments must be segregated and only through the use of change management tools can code and configurations be promoted from non-production to production.
IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			Shared	This requirement is addressed within the terms of the agreement for the Managed Service delivery of the customer solution.
IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			Customer	This requirement is addressed within the terms of the agreement for the Managed Service delivery of the customer solution.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	X			Combined	AWS ensures that InterSystems can create customer environments are logically segregated to prevent end users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data. Services which provide virtualized operational environments to customers ensure that customers are segregated from one another and prevent cross-customer privilege escalation and information disclosure via instance isolation. Different instances running on the same physical machine are isolated from each other. In addition, the Amazon EC2 firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance s neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical random-access memory (RAM) is separated using similar mechanisms.
IVS-09.4	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			Customer	The customer can determine to use the encryption capabilities of the platform for the encryption of the data flowing through or stored in the customer solution.
IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			Combined	The platform delivering the customer solution operates in the environment protected by the AWS firewall.
IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			Customer	InterSystems requires any communication of customer data from customer physical servers be encrypted in transit to the customer solution.
IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	X			Customer	Non-production environments must be segregated and only through the use of change management tools can code and configurations be promoted from non-production to production.
IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			Combined	InterSystems and AWS have a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. InterSystems and AWS employ the concept of least privilege, allowing only the necessary access for users to accomplish their job function.
IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	N/A	There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system.
IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X	N/A	There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system.
IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			X	N/A	There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system.
IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?			X	Customer	Customer must define requirements for network architecture based upon the determination by the customer of the legal compliance impacts.
IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	X			AWS	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership.
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			InterSystems	InterSystems provides information on platform API within the product documentation.
IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			Shared	Based upon agreed upon requirements in the terms of agreement, the customer solution on the platform can provide unstructured data in an industry standard format.
IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	X			Shared	SLAs must be agreed with the customer and associated to a solution implemented in the platform. Any external services are part of an agreement between the customer and the service providers and are the customer s responsibility.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	X			InterSystems	Customers can export their AMIs and use them on premise or at another cloud (infrastructure) provider (subject to software licensing restrictions).
IPY-03.3	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X			InterSystems	InterSystems provides procedures for migrating solutions and data from one environment to another (subject to software licensing restrictions). Customer retain control and ownership of their content. Customers can choose how they migrate applications and content at their discretion.
IPY-04.1	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			Shared	The platform permits data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols, but the customer must decide whether to use them and which ones.
IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			InterSystems	Interoperability and portability is addressed in the product documentation.
IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			InterSystems	Standard industry-recognized virtualization platform and virtualization formats are supported by the platform and the online documentation lists all the supported virtualization platforms.
IPY-05.2	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	X			InterSystems	Customers can export their AMIs and use them on premise or at another cloud (infrastructure) provider (subject to software licensing restrictions).
IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			X	AWS	AWS uses customized Xen and/or KVM based hypervisor technology. AWS does not share internal proprietary information with customers.
MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	N/A	Global Trust policies prohibit InterSystems Personnel from accessing Managed Services environments through mobile devices. Customer would be responsible for any end user access to customer solution using a mobile device.
SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			Combined	InterSystems and AWS maintain contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard.
SEF-02.1	Do you have a documented security incident response plan?	X			Combined	The InterSystems and AWS incident response programs, plans, and procedures have been developed in alignment with ISO 27001 standard.
SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	X			Shared	InterSystems develops a customer-specific Information Security Management Plan with the customer for the security controls related to the customer solution, which will include customer specific requirements for incident response including notification channels and regular testing.
SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X			Shared	Security requirements for deployment and operation of cloud-based solutions for customer are provided in the Global Privacy & Security Requirements addendum under the managed services agreement. See, https://www.intersystems.com/MSGPSS.
SEF-02.4	Have you tested your security incident response plans in the last year?	X			Shared	InterSystems develops a customer-specific Information Security Management Plan with the customer for the security controls related to the customer solution, which will include customer specific requirements for incident response including notification channels and regular testing.
SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	X			Combined	InterSystems and AWS employees are trained on how to recognize suspected privacy and security incidents and where to report them. When appropriate, incidents are reported to relevant authorities and notified to customers, including security and privacy events affecting the delivered services.
SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			Combined	InterSystems and AWS employees are trained on how to recognize suspected privacy and security incidents and where to report them. When appropriate, incidents are reported to relevant authorities and notified to customers, including security and privacy events affecting the delivered services.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			Combined	Contingency plans and incident response processes are defined, documented, and tested to detect, mitigate, investigate, and report a privacy or security incident. These include guidelines for responding to and reporting a data breach in accordance with customer agreements. Personnel follow a protocol when responding to a data security incident. The protocol involves steps which include validating customer data existence within impacted environment, determining the encryption status of a customer s content, and determining unauthorized access to a customer s content to the extent possible. If any step in the event does not reveal a positive indicator, the personnel document the findings in internal tools used to track the security incident. The Data Protection Officer (DPO) and Senior Executive Management at InterSystems (Executive management at AWS) receives updates on all data security investigations. In the event there are positive indicators for all steps in the security incident protocol, personnel engage with InterSystems DPO and Legal Department (in the case of AWS personnel, the AWS CISO and AWS Legal team) for a security review. The DPO and Legal Dep't review the evidence and determine if a data breach has occurred. If confirmed, affected customers are notified in accordance with their reporting agreements.
SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			Combined	Contingency plans and incident response processes are defined, documented, and tested to detect, mitigate, investigate, and report a privacy or security incident. These include guidelines for responding to and reporting a data breach in accordance with customer agreements. Personnel follow a protocol when responding to a data security incident. The protocol involves steps which include validating customer data existence within impacted environment, determining the encryption status of a customer s content, and determining unauthorized access to a customer s content to the extent possible. If any step in the event does not reveal a positive indicator, the personnel document the findings in internal tools used to track the security incident. The Data Protection Officer (DPO) and Senior Executive Management at InterSystems (Executive management at AWS) receives updates on all data security investigations. In the event there are positive indicators for all steps in the security incident protocol, personnel engage with InterSystems DPO and Legal Department (in the case of AWS personnel, the AWS CISO and AWS Legal team) for a security review. The DPO and Legal Dep't review the evidence and determine if a data breach has occurred. If confirmed, affected customers are notified in accordance with their reporting agreements.
SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			Shared	It is possible to freeze a specific customer without impacting other customers. For example, it is possible to dismount a database, put offline a namespace, remove accesses to tenant resources, block all information for the specified customer identification code, etc.
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			Shared	Each customer solution operates in its own segregated environment separate and isolated from other customer solutions.
SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			Combined	Security metrics are monitored and analyzed in accordance with ISO 27001 standard. Refer
SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	X			Shared	InterSystems will share incident data related to the customer solution with the customer.
STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?			X	Customer	The platform offers the capability to store data and process tthis data, but the customer retains control and ownership over the quality of their data and potential quality errors that may arise through their usage of the platform services.
STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X			InterSystems	InterSystems performs periodic reviews of service providers to validate adherence with InterSystems security and operational standards. InterSystems maintains standard contract review and signature processes that include legal reviews with consideration of protecting InterSystems resources, including customer information assets. InterSystems proactively informs our customers of any subcontractors who have access to customer information assets in the customer solution, including information that may contain personal data. There are no subcontractors authorized by InterSystems to access any customer information assets unless the customer specifically approves such access.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			InterSystems	The InterSystems incident response program, plans, and procedures have been developed in alignment with ISO 27001 standard. Depending on contract requirements, InterSystems maintains procedures for notifying customers of customer-impacting issues using the our product support environment or direct email notification.
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			InterSystems	InterSystems continuously monitors operational levels to project infrastructure needs to support availability commitments and requirements. InterSystems maintains a capacity planning model to assess infrastructure usage and demands on a regular basis. Furthermore, the InterSystems capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.
STA-03.2	Do you provide tenants with capacity planning and use reports?	X			Shared	Before preparing the environment for the customer, InterSystems collects information about the customer solution in terms of data exchanged, messages and transactions, number of expected users, interested population and among other metrics. These estimations are used to generate capacity planning and are used to size the customer solution. Then during the solution operation performances and data volumes and component usage are monitored to verify that the initial assumptions were correct and modify the available capaciity accordingly.
STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			Combined	Both InterSystems and AWS periodically evaluate risks and assess conformance to the existing security processes. Further, independent assurance is also provided by internal Compliance teams (such as Global Trust for InterSystems) or by independent third-party assessors. These assessors provide an independent assessment of risk management content/processes by performing periodic security assessments and compliance audits or examinations to evaluate the security, integrity, confidentiality, and availability of information and resources. InterSystems and AWS management also collaborate with these evaluations to determine the health of the control environment and leverages this information to fairly present the assertions made to other parties, including customers.
STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			InterSystems	The Third Party Risk Management process reviews supplier/vendors/providers to ensure compliance with appropriate legislative, regulatory, and legal obligations as well as InterSystems requirements for the protection of privacy and safeguards for security to ensure the confidentiality, integrity, and availability of information assets, including customer data, and technology resources, especially customer solutions.
STA-05.2	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			InterSystems	The Third Party Risk Management process reviews supplier/vendors/providers to ensure compliance with appropriate legislative, regulatory, and legal obligations as well as InterSystems requirements for the protection of privacy and safeguards for security to ensure the confidentiality, integrity, and availability of information assets, including customer data, and technology resources, especially customer solutions.
STA-05.3	Does legal counsel review all third-party agreements?	X			InterSystems	Legal Counsel and the Data Protection Officer review all third party contracts that include access and use of information assets, including customer data, and technology resources, especially customer solutiions.
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	X			InterSystems	All contracts must contain provisions supporting the InterSystems Information Privacy and Security Requirements https://www.intersystems.com/ISCIPSR
STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			Shared	The platform use several strategies for avoiding failures or data loss, from mirroring to different types of backup, but the customer must decide which strategy to implement.
STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			Customer	This requirement would be determined by the customer and address as part of the terms of agreement for the delivery of the customer solution.
STA-05.7	Can you provide the physical location/geography of storage of a tenant s data upon request?	X			Customer	This requirement would be determined by the customer and address as part of the terms of agreement for the delivery of the customer solution.
STA-05.8	Can you provide the physical location/geography of storage of a tenant's data in advance?	X			Customer	This requirement would be determined by the customer and address as part of the terms of agreement for the delivery of the customer solution.
STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X			Customer	This requirement would be determined by the customer and address as part of the terms of agreement for the delivery of the customer solution.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?		X		Customer	InterSystems Managed Services monitors the customer solution for security events, but because the customer determines the proper and authorized use for the personal data residing in the customer solution, the customer maintains responsbility to moniotr for privacy events. InterSystems and AWS will report any unauthorized access or use of customer data of which they become aware.
STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	X			InterSystems	The customer owns and controls the data processed by the customer solution.
STA-05.12	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	X			InterSystems	InterSystems provides customers with a list any subcontractors used for the delivery of the service.
STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	X			InterSystems	The Third Party Risk Management process reviews supplier/vendors/providers to ensure compliance with appropriate legislative, regulatory, and legal obligations as well as InterSystems requirements for the protection of privacy and safeguards for security to ensure the confidentiality, integrity, and availability of information assets, including customer data, and technology resources, especially customer solutions.
STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X			InterSystems	Through the use of established assessment procedures, InterSystems assesses and continuously monitors suppliers to ensure that they are conforming to specific InterSystems requirements. The extent of assessment for a supplier is dependent upon the significance of the product and/or service purchased and, where applicable, upon previously demonstrated performance.
STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?			X	N/A	The terms of agreement related to the delivery of the customer solution are based upon the InterSystems standard operating model, which is used to determine the requirements for any related suppliers.
STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?			X	N/A	The terms of agreement related to the delivery of the customer solution are based upon the InterSystems standard operating model, which is used to determine the requirements for any related suppliers.
STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?			X	N/A	The terms of agreement related to the delivery of the customer solution are based upon the InterSystems standard operating model, which is used to determine the requirements for any related suppliers.
STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?			X	N/A	The terms of agreement related to the delivery of the customer solution are based upon the InterSystems standard operating model, which is used to determine the requirements for any related suppliers.
STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?			X	N/A	The terms of agreement related to the delivery of the customer solution are based upon the
STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?			X	N/A	Customers are responsible for data management policies and procedures.
STA-07.8	Do you review all service level agreements at least annually?	X			InterSystems	Through the use of established assessment procedures, InterSystems assesses and continuously monitors suppliers to ensure that they are conforming to specific InterSystems requirements. The extent of assessment for a supplier is dependent upon the significance of the product and/or service purchased and, where applicable, upon previously demonstrated performance.
STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			InterSystems	Through the use of established assessment procedures, InterSystems assesses and continuously monitors suppliers to ensure that they are conforming to specific InterSystems requirements. The extent of assessment for a supplier is dependent upon the significance of the product and/or service purchased and, where applicable, upon previously demonstrated performance.
STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			InterSystems	Through the use of established assessment procedures, InterSystems assesses and continuously monitors suppliers to ensure that they are conforming to specific InterSystems requirements. The extent of assessment for a supplier is dependent upon the significance of the product and/or service purchased and, where applicable, upon previously demonstrated performance.
STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	X			InterSystems	Through the use of established assessment procedures, InterSystems assesses and continuously monitors suppliers to ensure that they are conforming to specific InterSystems
STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			InterSystems	InterSystems provides for third party penetration and vulnerability testing on an annual basis of all customer solutions.
TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	X			Combined	The InterSystems and AWS vulnerability management programs, processes, and procedures include managing antivirus / malicious software is in alignment with ISO 27001 standards.

Question ID	Consensus Assessment Questions	Answer			Control Responsibility	Notes
		Yes	No	N/A		
TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X			Combined	The InterSystems and AWS vulnerability management programs, processes, and procedures include managing antivirus / malicious software is in alignment with ISO 27001 standards.
TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			InterSystems	InterSystems Managed Services performs regular vulnerability scans on the customer solutiion environement on the AWS cloud infrastructure using a variety of tools.
TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			InterSystems	InterSystems Managed Services performs regular vulnerability scans on the customer solutiion environement on the AWS cloud infrastructure using a variety of tools.
TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			InterSystems	InterSystems Managed Services performs regular vulnerability scans on the customer solutiion environement on the AWS cloud infrastructure using a variety of tools.
TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	X			InterSystems	InterSystems Managed Services performs regular vulnerability scans on the customer solution environement on the AWS cloud infrastructure using a variety of tools.
TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			InterSystems	InterSystems will patch the underlying service delivery infrastructure based upon the CVSS score rating of the discovered vulnerability.
TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?			X	N/A	Customer data is not used as part of InterSystem's delivery of the service. Customer notification responsibilities are mutually agreed per contracts.
TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	Customer	Customer is responsible for the deployment of mobile code and any assessments necessary to authorize the code.
TVM-03.2	Is all unauthorized mobile code prevented from executing?			X	Customer	Customer is responsible for the deployment of mobile code and any assessments necessary to authorize the code.