



## **Consensus Assessment Initiative Questionnaire (CAIQ) for InterSystems TrakCare As A Service**

October 2022

## 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, v4.0.2.

If you have specific questions about this document, please engage with your InterSystems account representative.

The answers contained in this CAIQ are related to InterSystems TrakCare Cloud Services on Telecom Italia.

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	Information about the Global Trust program, including technical and organizational controls and measures are available through the Global Trust site, <a href="https://www.intersystems.com/globaltrust">https://www.intersystems.com/globaltrust</a> . The IaaS Provider has audit and assurance policies and procedures and standards related to operation of the infrastructure.	The Customer is responsible for audit and assurance policies and procedures and standards related to their use of the system.	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Audit and Assurance Policy and Procedures	
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	Shared CSP and CSC	InterSystems Global Trust program is designed in compliance with global standards including ISO 27001, ISO 22301, and ISO 20000. 1 which includes at least annual review of all relevant documentation. The IaaS Provider reviews and updates documentation at least annually.	The Customer is responsible for audit and assurance policies and procedures and standards related to their use of the system.				
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	Shared CSP and CSC	InterSystems maintains a formal audit program that includes independent external audits regarding the design of controls and operational effectiveness for information security under the ISO 27001 standard. The IaaS Provider has external independent assessments to validate the implementation and operating effectiveness of the IaaS Provider control environment.	The Customer is responsible for assessments of audit and assurance policies and procedures and standards related to their use of the system.	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	Shared CSP and CSC	The Global Trust monitors legislative and regulatory requirements relative to the delivery of the InterSystems Managed Service. The IaaS Provider 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.	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	Shared CSP and CSC	The Global Trust monitors legislative and regulatory requirements relative to the delivery of the InterSystems Managed Service.	The Customer is responsible for its own monitoring of regulatory requirements relating to its use and operation of the Customer's solution.	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	Audit & Assurance
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	Shared CSP and CSC	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. The IaaS Provider has established a formal periodic audit program regarding the IaaS Provider controls.	The Customer is responsible for its own monitoring of regulatory requirements relating to its use and operation of the Customer's solution.	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	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. The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.	The Customer is responsible for its own monitoring of regulatory requirements relating to its use and operation of the Customer's solution.	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	Shared CSP and CSC	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. The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.	The Customer is responsible for its own monitoring of regulatory requirements relating to its use and operation of the Customer's solution.				
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	CSP-owned	InterSystems uses industry standards in association with the development of product. Please see the related official document: <a href="https://www.intersystems.com/https://cdn.intersystems.psdops.co/m/67/c9/952651b84c07a7dc408a2759ef36/secure-coding-practices-wp.pdf">https://www.intersystems.com/https://cdn.intersystems.psdops.co/m/67/c9/952651b84c07a7dc408a2759ef36/secure-coding-practices-wp.pdf</a> .		AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	Application and Interface Security Policy and Procedures	
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	InterSystems Global Trust program is designed in compliance with global standards including ISO 27001, ISO 22301, and ISO 20000. 1 which includes at least annual review of all relevant documentation.					
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	InterSystems uses industry standards in association with the development of product. Please see the related official document: <a href="https://www.intersystems.com/https://cdn.intersystems.psdops.co/m/67/c9/952651b84c07a7dc408a2759ef36/secure-coding-practices-wp.pdf">https://www.intersystems.com/https://cdn.intersystems.psdops.co/m/67/c9/952651b84c07a7dc408a2759ef36/secure-coding-practices-wp.pdf</a> .		AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	InterSystems maintains the Global Trust program designed in accordance with global standards including ISO27001 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 <a href="https://www.intersystems.com/GTDPSPS">https://www.intersystems.com/GTDPSPS</a> , and for information about the Global Trust program, see <a href="https://www.intersystems.com/globaltrust">https://www.intersystems.com/globaltrust</a> .		AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	InterSystems uses industry standards in association with the development of product. Please see the related official document: <a href="https://www.intersystems.com/https://cdn.intersystems.psdops.co/m/67/c9/952651b84c07a7dc408a2759ef36/secure-coding-practices-wp.pdf">https://www.intersystems.com/https://cdn.intersystems.psdops.co/m/67/c9/952651b84c07a7dc408a2759ef36/secure-coding-practices-wp.pdf</a> .		AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	Application & Interface Security
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned	InterSystems uses industry standards in association with the development of product. Please see the related official document: <a href="https://www.intersystems.com/https://cdn.intersystems.psdops.co/m/67/c9/952651b84c07a7dc408a2759ef36/secure-coding-practices-wp.pdf">https://www.intersystems.com/https://cdn.intersystems.psdops.co/m/67/c9/952651b84c07a7dc408a2759ef36/secure-coding-practices-wp.pdf</a> .		AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application Security Testing	
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	Automated testing is used wherever possible.					
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	Shared CSP and CSC	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. Please see, <a href="https://www.intersystems.com/MSGSPS">https://www.intersystems.com/MSGSPS</a> .		AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	Automated deployment and integration tools are used where possible.					
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSP-owned	The InterSystems vulnerability management program, processes, and procedures include managing antivirus / malicious software in alignment with ISO 27001 standards.			Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability	

<b>AIS-07.2</b>	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSP-owned	The InterSystems vulnerability management program, processes, and procedures include managing antivirus / malicious software in alignment with ISO 27001 standards.	AIS-07		Remediation
<b>BCR-01.1</b>	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	InterSystems delivers offerings using a business continuity and disaster recovery process consistent with ISO 22301.  The IaaS Provider provides business continuity and disaster recovery through a framework to recover and reconstitute the IaaS Provider infrastructure through an Activation and Notification Phase, a Recovery Phase, and a Reconstitution Phase. InterSystems Global Trust program is designed in compliance with global standards including ISO 27001, ISO 22301, and ISO 20000 1 which includes at least annual review of all relevant documentation.		Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and Procedures
<b>BCR-01.2</b>	Are the policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	IaaS Provider reviews and updates the policies and procedures at least annually.	BCR-01		
<b>BCR-02.1</b>	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	Shared CSP and CSC	Both InterSystems and the IaaS Provider perform Business Impact Assessments relative 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.	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis
<b>BCR-03.1</b>	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	Shared CSP and 3rd-party	InterSystems delivers offerings using a business continuity and disaster recovery process consistent with ISO 22301.  The IaaS Provider provides business continuity and disaster recovery through a framework to recover and reconstitute the IaaS Provider's infrastructure through an Activation and Notification Phase, a Recovery Phase, and a Reconstitution Phase.	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy
<b>BCR-04.1</b>	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	Shared CSP and 3rd-party	InterSystems delivers offerings using a business continuity and disaster recovery process consistent with ISO 22301.  The IaaS Provider provides business continuity and disaster recovery through a framework to recover and reconstitute the IaaS Provider's infrastructure through an Activation and Notification Phase, a Recovery Phase, and a Reconstitution Phase.	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning
<b>BCR-05.1</b>	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	Shared CSP and 3rd-party	InterSystems delivers offerings using a business continuity and disaster recovery process consistent with ISO 22301. The IaaS Provider provides business continuity and disaster recovery through a framework to recover and reconstitute the IaaS Provider infrastructure through an Activation and Notification Phase, a Recovery Phase, and a Reconstitution Phase. InterSystems and the IaaS Provider make Documentation available internally to their respective personnel through the use of each organization's Intranet sites. Refer to ISO 27001 Appendix A Domain 12.		Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	
<b>BCR-05.2</b>	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	Shared CSP and 3rd-party	InterSystems and the IaaS Provider make Documentation available internally to their respective personnel through the use of each organization's Intranet sites. Refer to ISO 27001 Appendix A Domain 12. InterSystems maintains the Global Trust program designed in accordance with global standards including ISO27001 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 <a href="https://www.intersystems.com/GTDPSP">https://www.intersystems.com/GTDPSP</a> , and for information about the Global Trust program, see <a href="https://www.intersystems.com/globaltrust">https://www.intersystems.com/globaltrust</a> .	BCR-05		Documentation
<b>BCR-05.3</b>	Is business continuity and operational resilience documentation reviewed periodically?	Yes	Shared CSP and 3rd-party	InterSystems Global Trust program is designed in compliance with global standards including ISO 27001, ISO 22301, and ISO 20000 1 which includes at least annual review of all relevant documentation.  IaaS Provider will make documentation available to authorized stakeholders and review periodically.			Business Continuity Management and Operational Resilience
<b>BCR-06.1</b>	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 and ISO 22301 standards. Refer to ISO 27001 standard, annex A domain 17 and ISO 22301 for further details on business continuity controls.	BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises
<b>BCR-07.1</b>	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	Shared CSP and 3rd-party	InterSystems' and IaaS Provider Business Continuity plans include processes to communicate with stakeholders as appropriate.	BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication
<b>BCR-08.1</b>	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	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.	
<b>BCR-08.2</b>	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	Shared CSP and CSC	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 solution is applied (upgrade, patch install).	BCR-08	Customer is responsible to determine the nature and extent required to ensure confidentiality, integrity and availability of backup data.	Backup
<b>BCR-08.3</b>	Can backups be restored appropriately for resiliency?	Yes	Shared CSP and CSC	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.	
<b>BCR-09.1</b>	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	Shared CSP and 3rd-party	InterSystems delivers offerings using a business continuity and disaster recovery process consistent with ISO 22301.  The IaaS Provider provides business continuity and disaster recovery through a framework to recover and reconstitute the IaaS Provider infrastructure through an Activation and Notification Phase, a Recovery Phase, and a Reconstitution Phase.	BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Disaster Response Plan
<b>BCR-09.2</b>	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	Shared CSP and 3rd-party	InterSystems delivers offerings using a business continuity and disaster recovery process consistent with ISO 22301.  The IaaS Provider provides business continuity and disaster recovery through a framework to recover and reconstitute the IaaS Provider's infrastructure through an Activation and Notification Phase, a Recovery Phase, and a Reconstitution Phase.			
<b>BCR-10.1</b>	Is the disaster response plan exercised annually or when significant changes occur?	Yes	Shared CSP and 3rd-party	InterSystems' Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 and ISO 22301 standards. Refer to ISO 27001 standard, annex A domain 17 and ISO 22301 for further details on business continuity controls.  IaaS Provider will test its disaster response plan annually or when significant changes occur.	BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	Response Plan Exercise

BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Yes	Shared CSP and 3rd-party	Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 and ISO 22301 standards. Refer to ISO 27001 standard, annex A domain 17 and ISO 22301 for further details on business continuity controls.  IaaS Provider will test its disaster response plan annually or when significant changes occur. Each of the IaaS Provider's data centers is evaluated to determine the controls that must be implemented to mitigate, prepare, monitor, and respond to identified risks. Refer to ISO 27001 standard, Annex A domain 11 and link below for Data center controls overview.  <a href="https://aws.amazon.com/compliance/datacenter/controls/">https://aws.amazon.com/compliance/datacenter/controls/</a> InterSystems maintains the Global Trust program designed in accordance with global standards including ISO 27001 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.  IaaS Provider maintains risk management policies and procedures associated with changing organizations assets. InterSystems Global Trust program is designed in compliance with global standards including ISO 27001, ISO 22301, and ISO 20000 which includes at least annual review of all relevant documentation.  IaaS Provider will review and update its policies and procedures at least annually.				
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes	3rd-party outsourced		BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy	
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	Shared CSP and CSC				Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy and Procedures
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC					
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	Shared CSP and CSC	InterSystems and the IaaS Provider apply a systematic approach to managing change to ensure that all changes 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. Obtain approval for the change by an authorized individual.	To the extent that modifications can be made by the Customer, they must have a change management process to monitor those changes.		Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	
CCC-02.1					CCC-02			Quality Testing
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	Shared CSP and CSC				Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	Change Management Technology
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	Shared CSP and CSC	InterSystems 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. Obtain approval for the change by an authorized individual.	The Customer must restrict the unauthorized addition, removal, update, and management of organizational assets.		Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection
CCC-04.1					CCC-04			Change Control and Configuration Management
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Yes	Shared CSP and CSC	InterSystems and the IaaS Provider 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.	To the extent that modifications can be made by the Customer, they must have a change management process to monitor those changes.		Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	Shared CSP and CSC	The IaaS Provider has established baseline infrastructure standards, including for network components. The IaaS Provider host configuration settings are monitored to validate compliance with the IaaS Provider's security standards and automatically pushed to the host fleet. Firewall policies (configuration files) are automatically pushed to firewall devices every 24 hours. The solution has the capability to monitor all the accesses and the operations performed against the Customer solution and provide relevant reporting to allow for monitoring of security level adopted by the Customer.	To the extent that modifications can be made by the Customer, they must have a change management process to monitor those changes.		Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	Shared CSP and CSC				Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	Shared CSP and CSC	IaaS Provider implements detection measures with proactive notifications in case of changes deviating from the established baseline.  InterSystems apply a systematic approach to managing change to ensure that all changes to a production environment, including emergency changes, are reviewed, tested, and approved.  IaaS Provider implements a procedure for the management of exceptions, including emergencies, in the change and configuration process.	To the extent that modifications can be made by the Customer, they must have a change management process to monitor those changes.		'Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.'	Exception Management
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	Yes	Shared CSP and CSC	InterSystems apply a systematic approach to managing change to ensure that all changes to a production environment, including emergency changes, are reviewed, tested, and approved.  IaaS Provider implements a procedure for the management of exceptions, including emergencies, in the change and configuration process.	To the extent that modifications can be made by the Customer, they must have a change management process to monitor those changes including exceptions.			

CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	Shared CSP and CSC	<p>InterSystems 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:</p> <ol style="list-style-type: none"> <li>1. Document and communicate the change via the appropriate change management tool.</li> <li>2. Plan implementation of the change and rollback procedures to minimize disruption.</li> <li>3. Test the change in a logically segregated, nonproduction environment.</li> <li>4. Complete a peer-review of the change with a focus on business impact and technical rigor. The review should include a code review.</li> <li>5. Obtain approval for the change by an authorized individual.</li> </ol> <p>aaS Provider defines and implements a process to proactively roll back changes to a previous known good state in case of errors or security concerns.</p>	To the extent that modifications can be made by the Customer, they must have a change management process to monitor and roll-back those changes.	CCC-09	Define and implement a process to proactively roll back changes to a previously known good state in case of errors or security concerns.	Change Restoration
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	Encryption and Key Management Policy and Procedures
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-06	Manage and adopt changes to cryptography, encryption, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Encryption Change Cost Benefit Analysis
CEK-06.1	Are changes to cryptography, encryption, and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	CSP-owned	<p>InterSystems 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:</p> <ol style="list-style-type: none"> <li>1. Document and communicate the change via the appropriate change management tool.</li> <li>2. Plan implementation of the change and rollback procedures to minimize disruption.</li> <li>3. Test the change in a logically segregated, nonproduction environment.</li> <li>4. Complete a peer-review of the change with a focus on business impact and technical rigor. The review should include a code review.</li> <li>5. Obtain approval for the change by an authorized individual.</li> </ol>		CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Yes	Shared CSP and CSC	The solution 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 encryption keys for Customers.		CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	Encryption and Key Management Audit
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSC-owned	The solution 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 encryption keys for Customers.		CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entry is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	CSC-owned	The solution 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 encryption keys for Customers.				
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entry is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.				

CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.	CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.	CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.	CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Key Suspension
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.	CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys, at the time of their expiration date, which include provisions for legal and regulatory requirements.	Key Deactivation
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.	CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Key Archival
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.	CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstances, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Key Compromise
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.	CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Key Recovery
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	CSC-owned	The solution 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 encryption keys for Customers.	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Key Inventory Management
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	Shared CSP and 3rd-party	InterSystems and the IaaS Provider engage with external certifying bodies and independent auditors to review and validate operational compliance with policies.  The IaaS Provider SOC reports provide additional details on the specific asset management related policies and control activities executed by the IaaS Provider.	DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	Off-Site Equipment Disposal Policy and Procedures
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	Shared CSP and 3rd-party	InterSystems and the IaaS Provider engage with external certifying bodies and independent auditors to review and validate operational compliance with policies.  The IaaS Provider SOC reports provide additional details on the specific asset management related policies and control activities executed by the IaaS Provider.	DCS-01		Off-Site Equipment Disposal Policy and Procedures
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	InterSystems Global Trust program is designed in compliance with global standards including ISO 27001, ISO 22301, and ISO 20000 1 which includes at least annual review of all relevant documentation.  IaaS Provider reviews and updates its policies and procedures for the secure disposal of equipment used outside the organization's premises at least annually.	DCS-01		Off-Site Equipment Disposal Policy and Procedures
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Yes	Shared CSP and CSC	With regard to the solution, because the relocation or transfer of the Customer solution is a complex process, the process must be fully analyzed and coordination and agreement are required between the Customer, InterSystems, and the IaaS Provider before proceeding.  As for hardware, the environments used for the delivery of the Customer solution using the IaaS Provider's services are managed by authorized personnel and are located in one of the IaaS Provider's managed data centers. Media handling controls for the data centers are managed by the IaaS Provider in alignment with the IaaS Provider's 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-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	Off-Site Transfer Authorization Policy and Procedures
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	Shared CSP and CSC	With regard to the solution, because the relocation or transfer of the Customer solution is a complex process, the process must be fully analyzed and coordination and agreement are required between the Customer, InterSystems, and the IaaS Provider before proceeding.  As for hardware, the environments used for the delivery of the Customer solution using the IaaS Provider's services are managed by authorized personnel and are located in one of the IaaS Provider's managed data centers. Media handling controls for the data centers are managed by the IaaS Provider in alignment with the IaaS Provider's 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-02		Off-Site Transfer Authorization Policy and Procedures
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Yes	Shared CSP and CSC	With regard to the solution, because the relocation or transfer of the Customer solution is a complex process, the process must be fully analyzed and coordination and agreement are required between the Customer, InterSystems, and the IaaS Provider before proceeding.  As for hardware, the environments used for the delivery of the Customer solution using the IaaS Provider's services are managed by authorized personnel and are located in one of the IaaS Provider's managed data centers. Media handling controls for the data centers are managed by the IaaS Provider in alignment with the IaaS Provider's 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-02		Off-Site Transfer Authorization Policy and Procedures

DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	Shared CSP and 3rd-party	InterSystems and the IaaS Provider engage with external certifying bodies and independent auditors to review and validate operational compliance with policies.  The IaaS Provider's SOC reports provide additional details on the specific physical security control activities executed by the IaaS Provider. Refer to ISO 27001 standards: Annex A, domain 11 for additional details. The IaaS Provider has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	InterSystems Global Trust program is designed in compliance with global standards including ISO 27001, ISO 22301, and ISO 20000 1 which includes at least annual review of all relevant documentation.  IaaS Provider reviews and updates its policies and procedures for maintaining safe, secure working environments at least annually.				
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	InterSystems and the IaaS Provider engage with external certifying bodies and independent auditors to review and validate operational compliance with policies.  The IaaS Provider SOC reports provide additional details on the specific physical security control activities executed by the IaaS Provider.	DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	Datacenter Security
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.  IaaS Provider reviews and updates its policies and procedures for the secure transportation of physical media at least annually. In alignment with ISO 27001 standards, InterSystems and IaaS assets are assigned an owner, tracked and monitored.				
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	Shared CSP and 3rd-party		DCS-05	Classify and document the physical and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	Shared CSP and 3rd-party	In alignment with ISO 27001 standards, InterSystems and IaaS assets are assigned an owner, tracked and monitored.	DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloging and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	3rd-party outsourced	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 IaaS Provider SOC reports provide additional details on the specific control activities executed by the IaaS Provider. Refer to ISO 27001 standards: Annex A, domain 11 for further information. The IaaS Provider has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	Controlled Access Points	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	3rd-party outsourced	Physical access is strictly controlled, by IaaS, 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 IaaS Provider's Data Center Physical Security Policy				
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	3rd-party outsourced	The IaaS Provider manages equipment identification in alignment with ISO 27001 standards. The IaaS Provider has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	DCS-08	Use equipment identification as a method for connection authentication.	Equipment Identification	
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	3rd-party outsourced	Physical access is strictly controlled, by IaaS, 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 IaaS Provider's Data Center Physical Security Policy	DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	3rd-party outsourced	Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the IaaS Provider's Data Center Physical Security Policy				
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	3rd-party outsourced	IaaS Provider's 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 IaaS Provider SOC reports provide additional details on the specific control activities executed by the IaaS Provider. Refer to ISO 27001 standards: Annex A, domain 11 for further information. The IaaS Provider has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	3rd-party outsourced	In alignment with ISO 27001 standard, all InterSystems and the IaaS Provider 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.	DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	3rd-party outsourced	The IaaS Provider has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. The IaaS Provider 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.	DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Cabling Security	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	3rd-party outsourced	The IaaS Provider has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. The IaaS Provider 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.	DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Environmental Systems	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	3rd-party outsourced	The IaaS Provider has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. The IaaS Provider 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.	DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness as planned intervals.	Secure Utilities	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	3rd-party outsourced	Each of the IaaS Provider's data centers 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.	DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Equipment Location	



DSP-0-1.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	Security and Privacy Policy and Procedures
DSP-0-1.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.			
DSP-0-2.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	Shared CSP and CSC	The solution can support several methods to perform secure data deletion 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, the InterSystems solution includes a decommissioning process that is designed to prevent Customer data from being exposed to unauthorized individuals. The InterSystems solution uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.	The solution can support several methods to perform secure data deletion and it is the responsibility of the Customer to decide whether to use these methods or not.	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal
DSP-0-3.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	Management and documentation of data flows and the data stored within the platform is part of the solution design and it is the Customer's responsibility.	DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory
DSP-0-4.1	Is data classified according to type and sensitivity levels?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	Management and documentation of data flows and the data stored within the platform is part of the solution design and it is the Customer's responsibility.	DSP-04	Classify data according to its type and sensitivity level.	Data Classification
DSP-0-5.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	Management and documentation of data flows and the data stored within the platform is part of the solution design and it is the Customer's responsibility.		Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	
DSP-0-5.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	Management and documentation of data flows and the data stored within the platform is part of the solution design and it is the Customer's responsibility.	DSP-05		Data Flow Documentation
DSP-0-6.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	InterSystems Customers maintain ownership of their data and data management is the responsibility of the Customer.		Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	
DSP-0-6.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	InterSystems Customers maintain ownership of their data and data management is the responsibility of the Customer.	DSP-06		Data Ownership and Stewardship
DSP-0-7.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	InterSystems maintains the Global Trust program designed in accordance with global standards regarding obligations for data protection, privacy, security, and risk governance. A white paper about InterSystems Secure Coding Practices is available at <a href="https://www.intersystems.com/https://cdn.intersystems.psdops.com/m67/c9f92651b44c07a7dc408a2759ef36/secure-coding-practices-wp.pdf">https://www.intersystems.com/https://cdn.intersystems.psdops.com/m67/c9f92651b44c07a7dc408a2759ef36/secure-coding-practices-wp.pdf</a>		DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default
DSP-0-8.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned	InterSystems maintains the Global Trust program designed in accordance with global standards regarding obligations for data protection, privacy, security, and risk governance. A white paper about InterSystems Secure Coding Practices is available at <a href="https://www.intersystems.com/https://cdn.intersystems.psdops.com/m67/c9f92651b44c07a7dc408a2759ef36/secure-coding-practices-wp.pdf">https://www.intersystems.com/https://cdn.intersystems.psdops.com/m67/c9f92651b44c07a7dc408a2759ef36/secure-coding-practices-wp.pdf</a>		DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Security and Privacy Lifecycle Management
DSP-0-8.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	No	Shared CSP and CSC	Appropriate configurations are determined upon solution designed, as between Customer and InterSystems.	Appropriate configurations are determined upon solution designed, as between Customer and InterSystems.			
DSP-0-9.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	Yes	Shared CSP and CSC	InterSystems will collaborate with Customers in the production of appropriate DPIA.	The Customers maintain ownership of their data and data management is the responsibility of the Customer.	DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment
DSP-1-0.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	The solution provides encryption mechanisms or allows the Customer to use their own encryption mechanisms for at-rest and in-transit data.	DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer
DSP-1-1.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	Shared CSP and CSC	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities of the solution. Customers retain control and ownership of their data and may implement data security and privacy policies and procedures to meet their requirements.	The Customers maintain ownership of their data and data management is the responsibility of the Customer.	DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion
DSP-1-2.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	CSC-owned	InterSystems is a data processor. InterSystems does not access, process, or change Customer data in the course of providing the services without Customer approval. InterSystems does not utilize Customer data for testing (production or non-production).	The Customers maintain ownership of their data and data management is the responsibility of the Customer.	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing
DSP-1-3.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	CSC-owned	InterSystems is a data processor. InterSystems does not access, process, or change Customer data in the course of providing the services without Customer approval. InterSystems does not utilize Customer data for testing (production or non-production).	The Customers maintain ownership of their data and data management is the responsibility of the Customer.	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing
DSP-1-4.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	Shared CSP and CSC	The Global Trust program incorporates an integrated management system appropriately tailored on ISO Annex SL to ensure roles and responsibilities for the management of risk, including data protection, privacy, and security risks, are addressed and understood. Data Processor controls are included.	The Customers maintain ownership of their data and data management is the responsibility of the Customer.	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors

DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes	Shared CSP and CSC	InterSystems does not access, process, or change Customer data in the course of providing the services without Customer approval. InterSystems does not utilize Customer data for testing (production or non-production).	The Customers maintain ownership of their data and are responsible for authorizing processing.	DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	Shared CSP and CSC	InterSystems and the IaaS Provider 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 retention policies.	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSC-owned	InterSystems is a data processor. InterSystems does not access, process, or change Customer data in the course of providing the services without Customer approval. InterSystems does not utilize Customer data for testing (production or non-production).	The InterSystems solution can be deployed as the Customer determines appropriate using the data security capabilities provided. Customers retain control and ownership of their data and may implement policies and procedures to meet their requirements.	DSP-17	Define and implement processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Sensitive Data Protection
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes	CSP-owned	InterSystems shall notify the Customer of any legally binding requests for disclosure of personal information.		DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	Disclosure Notification
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	CSP-owned	InterSystems shall notify the Customer of any legally binding requests for disclosure of personal information.		DSP-19	Define and implement processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	Shared CSP and CSC	InterSystems and the IaaS Provider shall specify and document the countries and international organizations to which personal information can possibly be transferred.	This requirement would be determined by the Customer and address as part of the terms of agreement for the delivery of the Customer solution.	DSP-19	Define and implement processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	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 appropriately tailored to ISO Annex SL to ensure roles and responsibilities for the management of risk, including data protection, privacy, and security risks, are addressed and understood.	The Customer must maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Policies and procedures are reviewed and updated at least annually.	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	Governance Program Policy and Procedures
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	InterSystems Global Trust program is designed in compliance with global standards, which includes at least annual review of all relevant documentation.	The Customer must maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Policies and procedures are reviewed and updated at least annually.	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	Governance Program Policy and Procedures
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	Shared CSP and CSC	The IaaS Provider maintains policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Policies and procedures are reviewed and updated at least annually.	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.	GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	Shared CSP and CSC	InterSystems Global Trust program is designed in compliance with global standards, which includes at least annual review of all relevant documentation.	The Customer program must include at least an annual review.	GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	Shared CSP and CSC	The IaaS Provider program includes at least an annual review. InterSystems has an exception process within the Global Trust program.	The Customer must have an exception process for deviation from established policy.	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	Shared CSP and CSC	The IaaS Provider has an exception process for deviation from established policy. Customer can review the InterSystems Global Trust Data Protection, Privacy and Security Policy, which defines the Information Security Management Program, at <a href="https://www.intersystems.com/GDPPS">https://www.intersystems.com/GDPPS</a> .	The Customer must have an established information security program.	GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Information Security Program
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	Shared CSP and CSC	The IaaS Provider has an established information security program as detailed in their ISMP. 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 appropriately tailored to ISO Annex SL to ensure roles and responsibilities for the management of risk, including data protection, privacy, and security risks, are addressed and understood.	Roles and responsibilities for the Customer governance program must be documented.	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	Shared CSP and CSC	The Global Trust monitors legislative and regulatory requirements relative to the delivery of the InterSystems Managed Service.	The Customer is responsible for its own monitoring of regulatory requirements relating to its use and operation of the Customer's solution.	GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	Shared CSP and CSC	The IaaS Provider 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.	GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Special Interest Groups
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	InterSystems and the IaaS Provider 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.	The Customer is responsible for maintaining background verification policies and procedures of all new employees (including but not limited to remote employees, contractors and third parties).		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be processed, the business requirements, and applicable	

HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes	Shared CSP and CSC	InterSystems and the IaaS Provider 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.	The Customer is responsible for maintaining background verification policies and procedures according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk.	HRS-01	to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	Background Screening Policy and Procedures
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.	The Customer must review and update background verification policies and procedures at least annually.			
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	IaaS Provider reviews and updates background verification policies and procedures at least annually. Both InterSystems and the IaaS Provider have implemented data handling and classification requirements that provide specifications around: <ul style="list-style-type: none"> <li>• Data encryption</li> <li>• Content in transit and during storage</li> <li>• Access</li> <li>• Retention</li> <li>• Physical controls</li> <li>• Mobile devices</li> <li>• Data handling requirements</li> </ul> Employees are required to review and sign-off on an employment contract, which acknowledges their responsibilities to overall data protection, privacy, and security policies and procedures.	The Customer program must identify acceptable use policies.	HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	Acceptable Use of Technology Policy and Procedures
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	Shared CSP and CSC	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.	The Customer program must include at least annual review and update.			
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	IaaS Provider reviews and updates policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets at least annually. 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.	The Customer is responsible for establishing processes to secure unattended workspaces.	HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	Clean Desk Policy and Procedures
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	Shared CSP and CSC	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.	The Customer must review and update policies and procedures requiring unattended workspaces to conceal confidential data at least annually.			
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	The IaaS Provider maintains the Global Trust program designed in accordance with global standards regarding obligations for data protection, privacy, security, and risk governance. Information about the Global Trust program, including technical and organization controls and measures are available through the Global Trust site, <a href="https://www.intersystems.com/globaltrust">https://www.intersystems.com/globaltrust</a> .	The Customer is responsible for establishing processes in place regarding processing at remote sites.	HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	Remote and Home Working Policy and Procedures
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	Shared CSP and CSC	The IaaS Provider has established processes in place regarding processing at remote sites.	The Customer program must include at least annual review and update.			
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	Shared CSP and CSC	The IaaS Provider program includes at least annual review and update. Upon termination of InterSystems 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.	The Customer must have processes in place to ensure return of assets by terminated employees.	HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	Shared CSP and CSC	The IaaS Provider has processes in place to ensure return of assets by terminated employees. The Human Resources team at InterSystems defines internal management responsibilities to be followed for role change of employees and vendors.	The Customer must have roles and responsibilities identified for changes in employment.	HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Employment Termination
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	Shared CSP and CSC	The IaaS Provider has roles and responsibilities identified for changes in employment. 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.	The Customer must ensure non-disclosure agreements are in place prior to access to systems and data.	HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	Shared CSP and CSC	InterSystems Personnel supporting the IaaS Provider's 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.	The Customer must ensure that terms for adherence to security policies are included in employment agreements.	HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	Shared CSP and CSC	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 solution with regard to information security controls.	The Customer must document and communicate roles and responsibilities of employees as they relate to information assets and security.	HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	Shared CSP and CSC	IaaS Provider documents and communicates employee roles and responsibilities relating to information assets and security. The Global Trust program reviews and, as necessary, updates related non-disclosure and confidentiality agreements on a periodic basis, but not less than annually.	The Customer program must ensure at least annual review.	HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Non-Disclosure Agreements

HRS-1.1.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	Shared CSP and CSC	All InterSystems Personnel complete general privacy and security training which requires 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. 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 solution with regard to information security controls.  IaaS Provider maintains security awareness training for all employees of the organization. In alignment with ISO 27001 standard, all InterSystems and the IaaS Provider's 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. 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 solution with regard to information security controls.	The Customer is responsible for ensuring security awareness training for its staff.	HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training
HRS-1.1.2	Are regular security awareness training updates provided?	Yes	Shared CSP and CSC	IaaS Provider maintains security awareness training for all employees of the organization. In alignment with ISO 27001 standard, all InterSystems and the IaaS Provider's 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. 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 solution with regard to information security controls.	The Customer is responsible for ensuring security awareness training for its staff.			
HRS-1.2.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	Shared CSP and CSC	All InterSystems Personnel complete general privacy and security training which requires 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. 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 solution with regard to information security controls.  IaaS Provider provides all employees that are granted access to sensitive organizational and personal data with appropriate security awareness training.	The Customer is responsible for ensuring security awareness training for its staff.		Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	
HRS-1.2.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	Shared CSP and CSC	In alignment with ISO 27001 standard, all InterSystems and the IaaS Provider's 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. 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 solution with regard to information security controls.  IaaS Provider provides all employees that are granted access to sensitive organizational and personal data with regular updates in procedures, processes, and policies relating to their professional functions.	The Customer is responsible for ensuring security awareness training for its staff.	HRS-12		Personal and Sensitive Data Awareness and Training
HRS-1.3.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	Shared CSP and CSC	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 solution with regard to information security controls.  The need to maintain awareness and compliance with requirements is notified to all IaaS Provider staff.	The Customer must ensure that all staff are aware of their responsibilities for compliance.	HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Compliance User Responsibility
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	In alignment with ISO 27001, InterSystems and the IaaS Provider 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.	The Customer is responsible for establishing policies and procedures for identity and access management. The Customer must review and update these policies and procedures at least annually.	IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.  IaaS Provider reviews and updates identity and access management policies and procedures at least annually.	The Customer must review and update these policies and procedures at least annually.			
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	InterSystems maintains the Global Trust program designed in accordance with global standards regarding obligations for data protection, privacy, security, and risk governance. Information about the Global Trust program, including technical and organization controls and measures are available through the Global Trust site, <a href="https://www.intersystems.com/globaltrust">https://www.intersystems.com/globaltrust</a> . The solution provides capabilities to address password support consistent with NIST SP 800-63-3.	The Customer must establish policies and procedures for strong passwords.	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.	The Customer must review and update these policies and procedures at least annually.			
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	Shared CSP and CSC	InterSystems and the IaaS Provider 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 the IaaS Provider employ the concept of least privileges, allowing only the necessary access for users to accomplish their job function.  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.  The IaaS Provider's personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate IaaS Provider 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.	The Customer is responsible for identity and access management controls related to the application.	IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	Shared CSP and CSC	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 separation of duties related to access to the Customer solution.	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 separation of duties related to access to the Customer solution.	IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties

IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	Shared CSP and CSC	InterSystems and the IaaS Provider 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 the IaaS Provider employ the concept of least privilege, allowing only the necessary access for users to accomplish their job function.	The Customer is responsible for identity and access management controls related to the application.	IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	Shared CSP and CSC	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.	The Customer must define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	Shared CSP and CSC	The Human Resources team at InterSystems defines internal management responsibilities to be followed for role change of employees and vendors. Upon termination, Human Resources at both InterSystems and the IaaS Provider 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 Customer must de-provision or respectively modifies access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	Shared CSP and CSC	The following processes must be addressed upon the termination of an employee or contractor: • 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.	The Customer must review and revalidate user access for least privilege and separation of duties as frequent as is commensurate with organizational risks.	IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	Shared CSP and CSC	IaaS Provider reviews and revalidates user access for least privilege and separation of duties as frequent as is commensurate with organizational risks.	The Customer must review and revalidate user access for least privilege and separation of duties.	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separate.	Segregation of Privileged Access Roles
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	Shared CSP and CSC	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.	The Customer must define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	Shared CSP and CSC	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.	The Customer must define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	Yes	Shared CSP and CSC	InterSystems has established policies and procedures for Customer participation in the granting of access to privileged roles at the application level.	The Customer must define and implement processes and procedures, at the application level, for the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	CSCs Approval for Agreed Privileged Access Roles
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	The audit system of the solution is controlled by security restrictions and only authorized users can access it, but solely in read only mode and therefore cannot be altered by any user.	The Customer must ensure that logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	The audit system of the solution is controlled by security restrictions and only authorized users can access it, but solely in read only mode and therefore cannot be altered by any user.	The Customer must ensure that logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	Shared CSP and CSC	InterSystems and IaaS Provider creates unique user identifiers 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. Group or shared accounts are not permitted.	The Customer must implement processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	Uniquely Identifiable Users
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	Shared CSP and CSC	In alignment with ISO 27001, InterSystems and the IaaS Provider 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. The solution allows several methods to authenticate at the same time for the same system or function; all the methods can be put in a hierarchical order to grant multifactor authentication.	The Customer must implement processes, procedures and technical measures for authentication access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. The Customer adopts digital certificates or alternatives which achieve an equivalent level of security for system identities.	IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	Shared CSP and CSC	The solution allows several methods to authenticate at the same time for the same system or function; all the methods can be put in a hierarchical order to grant multifactor authentication.	The Customer is responsible for adopting digital certificates or alternatives which achieve an equivalent level of security for system identities.	IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	Shared CSP and CSC	InterSystems maintains the Global Trust program designed in accordance with global standards regarding obligations for data protection, privacy, security, and risk governance. Information about the Global Trust program, including technical and organization controls and measures are available through the Global Trust site, <a href="https://www.intersystems.com/globaltrust">https://www.intersystems.com/globaltrust</a> .	The Customer must implement processes, procedures and technical measures for the secure management of passwords.	IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	Shared CSP and CSC	The IaaS Provider has controls in place to manage passwords. In alignment with ISO 27001, InterSystems and the IaaS Provider 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.	The Customer must implement processes, procedures and technical measures to verify access to data and system functions is authorized.	IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms

IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g. APIs)?	Yes	CSP-owned	Interoperability and portability is addressed in the product documentation.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for:		
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSP-owned	Interoperability and portability is addressed in the product documentation.		a. Communications between application interfaces		
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	Interoperability and portability is addressed in the product documentation.		b. Information processing interoperability	IPY-01	Interoperability and Portability Policy and Procedures
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSP-owned	Interoperability and portability is addressed in the product documentation.		c. Application development portability		
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Interoperability and portability is addressed in the product documentation.		d. Information/Data exchange, usage, portability, integrity, and persistence		
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	CSC-owned	Customers can export their data via application interfaces.	IPY-02	Review and update the policies and procedures at least annually.		
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	Shared CSP and CSC	The solution permits data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols.	IPY-03	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	Shared CSP and CSC	InterSystems and the Customer will agree upon appropriate decommissioning responsibilities as part of contract termination.	IPY-04	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	InterSystems maintains the Global Trust program designed in accordance with global standards regarding obligations for data protection, privacy, security, and risk governance. Information about the Global Trust program, including technical and organization controls and measures are available through the Global Trust site, <a href="https://www.intersystems.com/globaltrust">https://www.intersystems.com/globaltrust</a> .  IaaS Provider establishes, documents, approves, communicates, applies, evaluates and maintains infrastructure and virtualization security policies and procedures.	IVS-01	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Data Portability Contractual Obligations	
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.		Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	Infrastructure and Virtualization Security Policy and Procedures	
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	CSP-owned	IaaS Provider reviews and updates infrastructure and virtualization security policies and procedures at least annually. This requirement is addressed within the terms of the agreement for the Managed Service delivery of the Customer solution.	IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning	
IVS-03.1	Are communications between environments monitored?	Yes	Shared CSP and CSC	InterSystems coordinates with the Customer to develop the appropriate solution architecture, including necessary network infrastructure and monitoring, as part of the business requirements for the Customer solution.	IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Network Security	
IVS-03.2	Are communications between environments encrypted?	Yes	Shared CSP and CSC	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-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	Shared CSP and CSC	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-03			
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	InterSystems reviews network configuration at least annually.				
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	Shared CSP and CSC	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.			Infrastructure & Virtualization Security	
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	CSP-owned	InterSystems deploys the solution through hardened images to construct the baseline build standard necessary for the delivery of the operating solution.	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	Shared CSP and CSC	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. The IaaS Provider ensures that InterSystems can create Customer environments that 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.	IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	Shared CSP and 3rd-party		IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSC-owned		IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSC-owned	Customer must define requirements for network architecture based upon the determination by the Customer of the legal compliance impacts.	IVS-08	Identify and document high-risk environments.	Network Architecture Documentation	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	3rd-party outsourced	The IaaS Provider Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include Customer instances). The IaaS Provider's 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 the IaaS Provider's leadership.	IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	

LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	InterSystems maintains the Global Trust program designed in accordance with global standards regarding obligations for data protection, privacy, security, and risk governance. Information about the Global Trust program, including technical and organization controls and measures are available through the Global Trust site, <a href="https://www.intersystems.com/globaltrust">https://www.intersystems.com/globaltrust</a> .	LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.			
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	The audit system of the solution is controlled by security restrictions and only authorized users can access it, but solely in read only mode and therefore cannot be altered by any user. The solution 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.	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider incident response programs, plans, and procedures have been developed in alignment with ISO 27001 standard. InterSystems and the IaaS Provider's 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.	LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	Security Monitoring and Alerting
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	CSP-owned	InterSystems maintains a log alerting process to ensure prompt notification of alerts based upon events and their respective risk.			
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	The audit system of the solution is controlled by security restrictions and only authorized users can access it, but solely in read only mode and therefore cannot be altered by any user.	LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	Shared CSP and CSC	InterSystems maintains a log alerting process to ensure prompt notification of alerts based upon events and their respective risk. The Customer is responsible for monitoring security audit logs to detect activity outside of typical or expected patterns.	LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Audit Log Monitoring and Response
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	Shared CSP and CSC	InterSystems maintains a log alerting process to ensure prompt notification of alerts based upon events and their respective risk. The Customer must establish and follow a process to review and take appropriate and timely actions to detect anomalies.	LOG-05		
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	The solution uses the OS clock in the default, but it can integrate any synchronized time-service protocols.	LOG-06	Use a reliable time source across all relevant information processing systems.	Clock Synchronization
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	Logging requirements are addressed in the product documentation.	LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	Logging Scope
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	InterSystems incident management process includes periodic reviews done at least annually or when there is a change in the threat environment.			
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	The solution uses a central audit system that logs all relevant system, application, and user events.	LOG-08	Generate audit records containing relevant security information.	Log Records
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	The audit system of the solution is controlled by security restrictions and only authorized users can access it, but solely in read only mode and therefore cannot be altered by any user.	LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	Shared CSP and CSC	InterSystems manages cryptographic keys related to internal solutions operations. The Customer has responsibility for managing cryptographic keys for all external connectivity.	LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	Shared CSP and CSC	InterSystems manages cryptographic keys related to internal solutions operations. The Customer has responsibility for managing cryptographic keys for all external connectivity.	LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	3rd-party outsourced	Physical access is strictly controlled by IaaS, 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 IaaS Provider's Data Center Physical Security Policy.	LOG-12	Monitor and log physical access using an auditable access control system.	Access Control Logs
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	Shared CSP and 3rd-party	InterSystems and the IaaS Provider's employees are trained on how to recognize suspected privacy and security incidents and where to report them.	LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Failures and Anomalies Reporting
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	Shared CSP and 3rd-party	When appropriate, incidents are reported to relevant authorities and notified to Customers, including security and privacy events affecting the delivered services. IaaS Provider immediately notifies accountable parties about anomalies and failures.			
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider incident response programs, plans, and procedures have been developed in alignment with ISO 27001 standard.	SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	Security Incident Management Policy and Procedures
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	Shared CSP and 3rd-party	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation. IaaS Provider establishes, documents, approves, communicates, applies, evaluates, and maintains.			
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider incident response programs, plans, and procedures have been developed in alignment with ISO 27001 standard.	SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	Service Management Policy and Procedures
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.			
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	IaaS Provider reviews and updates policies and procedures for timely management of security incidents at least annually. The InterSystems and the IaaS Provider incident response programs, plans, and procedures have been developed in alignment with ISO 27001 standard. Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 and ISO 22301 standards. Refer to ISO 27001 standard, annex A domain 17 and ISO 22301 for further details on business continuity controls.	SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.'	Incident Response Plans

SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider Incident response programs, plans, and procedures have been developed in alignment with ISO 27001 standard. Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 and ISO 22301 standards. Refer to ISO 27001 standard, annex A domain 17 and ISO 22301 for further details on business continuity controls.	SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing
SEF-05.1	Are information security incident metrics established and monitored?	Yes	Shared CSP and 3rd-party	Security metrics are monitored and analyzed in accordance with ISO 27001 standard. Refer to ISO 27001 Annex A, domain 16 for further details.  IaaS Provider establishes and monitors information security incident metrics.	SEF-05	Establish and monitor information security incident metrics.	Incident Response Metrics
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider Incident response programs, plans, and procedures have been developed in alignment with ISO 27001 standard.	SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider Incident response programs, plans, and procedures have been developed in alignment with ISO 27001 standard. 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 the IaaS Provider) 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 the IaaS Provider's personnel, the IaaS Provider's CISO and the IaaS Provider's Legal team) for a security review. The DPO and Legal Dept review the evidence and determine if a data breach has occurred. If confirmed, affected Customers are notified in accordance with their reporting agreements.	SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider Incident response programs, plans, and procedures have been developed in alignment with ISO 27001 standard. 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 the IaaS Provider) 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 the IaaS Provider's personnel, the IaaS Provider's CISO and the IaaS Provider's Legal team) for a security review. The DPO and Legal Dept review the evidence and determine if a data breach has occurred. If confirmed, affected Customers are notified in accordance with their reporting agreements.	SEF-07		Security Breach Notification
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	Shared CSP and 3rd-party	InterSystems and the IaaS Provider maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard.	SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	Points of Contact Maintenance
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	InterSystems and IaaS Provider maintain appropriate policies and procedures. The Customer must maintain appropriate policies and procedures.	STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	SSRM Policy and Procedures
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	Shared CSP and CSC	InterSystems and IaaS Provider reviews and updates appropriate policies and procedures annually. The Customer must review and update appropriate policies and procedures annually.			
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	Shared CSP and CSC	InterSystems and IaaS Provider maintain appropriate policies and procedures. The Customer must maintain appropriate policies and procedures.	STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSP-owned	InterSystems provides the Customer relevant guidance within product specification.	STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	Shared CSP and CSC	InterSystems and IaaS Provider maintain appropriate policies and procedures. The Customer must maintain appropriate policies and procedures.	STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	Shared CSP and CSC	InterSystems reviews and validates SSRM documentation for any third-party cloud services made part of the delivered solution. The Customer must review and validate SSRM documentation for any third-party services used with the delivered solution.	STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	Shared CSP and CSC	InterSystems and IaaS Provider maintain appropriate policies and procedures. The Customer must maintain appropriate policies and procedures.	STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	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	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory



<b>STA-08.1</b>	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	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. 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	CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management	Supply Chain Management, Transparency, and Accountability
<b>STA-09.1</b>	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	CSP-owned	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. 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. All contracts must contain provisions supporting the InterSystems Information Privacy and Security Requirements, <a href="https://www.intersystems.com/ISCPISR">https://www.intersystems.com/ISCPISR</a>	STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy	Primary Service and Contractual Agreement	
<b>STA-10.1</b>	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned	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-10	Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review	
<b>STA-1.1.1</b>	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	Shared CSP and 3rd-party	Both InterSystems and the IaaS Provider 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 the IaaS Provider's 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-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	Internal Compliance Testing	
<b>STA-12.1</b>	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	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-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	Supply Chain Service Agreement Compliance	
<b>STA-13.1</b>	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned	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-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	Supply Chain Governance Review	
<b>STA-14.1</b>	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSP-owned	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-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment	
<b>TVM-01.1</b>	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider vulnerability management programs, processes, and procedures include managing antivirus, malicious software, and vulnerabilities, in alignment with ISO 27001 standards. InterSystems Managed Services performs regular vulnerability scans on the Customer solution environment on the IaaS Provider's cloud infrastructure using a variety of tools.	TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	Threat and Vulnerability Management Policy and Procedures	
<b>TVM-01.2</b>	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.				
<b>TVM-02.1</b>	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	IaaS Provider reviews and updates threat and vulnerability management policies and procedures at least annually. The InterSystems and the IaaS Provider's vulnerability management programs, processes, and procedures include managing antivirus, malicious software, and vulnerabilities, in alignment with ISO 27001 standards.	TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy and Procedures	
<b>TVM-02.2</b>	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	InterSystems Global Trust program is designed in compliance with global standards which includes at least annual review of all relevant documentation.				
<b>TVM-03.1</b>	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	Shared CSP and 3rd-party	IaaS Provider reviews and updates asset management and malware protection policies and procedures at least annually. The InterSystems and the IaaS Provider's vulnerability management programs, processes, and procedures include managing antivirus, malicious software, and vulnerabilities, in alignment with ISO 27001 standards.	TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
<b>TVM-04.1</b>	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider's vulnerability management programs, processes, and procedures include managing antivirus, malicious software, and vulnerabilities, in alignment with ISO 27001 standards.	TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	Threat & Vulnerability Management
<b>TVM-05.1</b>	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider's vulnerability management programs, processes, and procedures include managing antivirus, malicious software, and vulnerabilities, in alignment with ISO 27001 standards.	TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	
<b>TVM-06.1</b>	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned	InterSystems Managed Services performs regular vulnerability scans on the Customer solution environment on the IaaS Provider's cloud infrastructure using a variety of tools.	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Penetration Testing	

<b>TVM-07.1</b>	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	CSP-owned	InterSystems Managed Services performs regular vulnerability scans on the Customer solution environment on the IaaS Provider's cloud infrastructure using a variety of tools.	Customer would be responsible for any end user access to Customer solution.	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	Universal Endpoint Management
<b>TVM-08.1</b>	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider's vulnerability management programs, processes, and procedures include managing antivirus, malicious software, and vulnerabilities, in alignment with ISO 27001 standards.	Customer would be responsible for any end user access to Customer solution.	TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization	
<b>TVM-09.1</b>	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider's vulnerability management programs, processes, and procedures include managing antivirus, malicious software, and vulnerabilities, in alignment with ISO 27001 standards.	Customer would be responsible for any end user access to Customer solution.	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
<b>TVM-10.1</b>	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	Shared CSP and 3rd-party	The InterSystems and the IaaS Provider's vulnerability management programs, processes, and procedures include managing antivirus, malicious software, and vulnerabilities, in alignment with ISO 27001 standards.	Customer would be responsible for any end user access to Customer solution.	TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	
<b>UEM-01.1</b>	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	Endpoint Devices Policy and Procedures	
<b>UEM-01.2</b>	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-01			
<b>UEM-02.1</b>	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	
<b>UEM-03.1</b>	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility	
<b>UEM-04.1</b>	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned		Customer would be responsible for any end user access to Customer solution.	UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	
<b>UEM-05.1</b>	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
<b>UEM-06.1</b>	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	
<b>UEM-07.1</b>	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	
<b>UEM-08.1</b>	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption	
<b>UEM-09.1</b>	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	
<b>UEM-10.1</b>	Are software firewalls configured on managed endpoints?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
<b>UEM-11.1</b>	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention	
<b>UEM-12.1</b>	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate	
<b>UEM-13.1</b>	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes	CSC-owned		Customer would be responsible for any end user access to Customer solution.	UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe	
<b>UEM-14.1</b>	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Yes	Shared CSP and CSC	InterSystems and IaaS Provider maintain appropriate policies and procedures regarding third-party endpoint access.	Customer must maintain appropriate policies and procedures regarding third-party endpoint access.	UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	Third-Party Endpoint Security Posture	
End of Standard									