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

InterSystems develops, updates, and documents policies and standards in alignment with relevant standards and regulatory requirements. InterSystems maintains a formal audit program that includes periodic audits and external assessments to validate the control design and operational effectiveness of the InterSystems solution.

The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

InterSystems (CSA) Consensus Assessments Initiative Questionnaire for InterSystems TrakCare

**A&A-01.3** Are independent audits and assurance assessments conducted regarding InterSystems standards at least annually?

Yes

Shared CSP and CSC

The IaaS Provider has an independent external assurance assessment, which includes periodic vulnerability scans and external assessments to validate the control design and operational effectiveness of the IaaS Provider controls.

The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**A&A-01.1** Is an independent audits and assurance assessments performed according to risk-based plans and policies?

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 controlled environment.

The IaaS Provider has established a formal periodic audit program regarding the IaaS Provider controls.

The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**A&A-01.1** Is the remediation status of audit findings monitored and reported to relevant stakeholders?

Yes

Shared CSP and CSC

InterSystems maintains the Global Trust program as designed and documented in accordance with relevant standards and regulatory requirements relating to the delivery of the InterSystems-managed service.

The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**AB-01.1** Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to support safe planning, risk analysis, security control assessment, configuration, remediation schedules, report generation, and review of past reports and supporting evidence?

Yes

CSP-owned

InterSystems relies on standards in association with the development of products and services in accordance with the InterSystems-managed service. Please see the related official document:


The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**AB-01.1** Are application security policies and procedures maintained in least annually?

Yes

CSP-owned

InterSystems maintains the Global Trust program as designed in accordance with relevant standards and regulatory requirements relating to the delivery of the InterSystems-managed service.

The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**AB-01.1** Are baseline requirements to secure internal applications established, documented, and maintained?

Yes

CSP-owned

InterSystems relies on standards in association with the development of products and services in accordance with the InterSystems-managed service. Please see the related official document:


The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**AB-01.1** Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?

Yes

CSP-owned

InterSystems relies on standards in association with the delivery of products and services in accordance with the InterSystems-managed service. Please see the related official document:


The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**AB-01.1** Is BLSA process defined and implemented for application design, development, deployment, and operations per organizationally designed security requirements?

Yes

CSP-owned

InterSystems relies on standards in association with the development of products. Please see the related official document:


The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**AB-01.1** Does the engineering security review process to assess new information systems, applications, and new services while ensuring application security, compliance adherence, and operational speed of delivery goals?

Yes

CSP-owned

InterSystems relies on standards in association with the development of products. Please see the related official document:


The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**AB-01.2** Is property protection defined and implemented to protect application code in a secure, standardized, and compliant manner?

Yes

CSP-owned

InterSystems relies on standards in association with the delivery of products and services in accordance with the InterSystems-managed service. Please see the related official document:


The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**AB-01.2** Is the deployment and integration of application code protected and validated?

Yes

CSP-owned

InterSystems relies on standards in association with the development of products and services in accordance with the InterSystems-managed service. Please see the related official document:


The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**AB-01.2** Are application security vulnerabilities remediated following defined processes?

Yes

CSP-owned

InterSystems relies on standards in association with the delivery of products and services in accordance with the InterSystems-managed service. Please see the related official document:


The IaaS Provider has a risk-based corrective action plan to remediate audit findings and report remediation status to relevant stakeholders.

**CCM**

<table>
<thead>
<tr>
<th>CCM Domain Title</th>
<th>CCM Control Title</th>
<th>CCM Control Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Access Control</td>
<td>A&amp;A-01.1 Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?</td>
</tr>
<tr>
<td>Security</td>
<td>Audit and Assurance Policy and Procedures</td>
<td>A&amp;A-01.3 Are independent audits and assurance assessments conducted regarding InterSystems standards at least annually?</td>
</tr>
<tr>
<td>Security</td>
<td>Audit and Assurance Process</td>
<td>A&amp;A-01.1 Is an independent audits and assurance assessments performed according to risk-based plans and policies?</td>
</tr>
<tr>
<td>Security</td>
<td>Accountability</td>
<td>A&amp;A-01.1 Is the remediation status of audit findings monitored and reported to relevant stakeholders?</td>
</tr>
<tr>
<td>Security</td>
<td>Architecture and Design</td>
<td>A&amp;A-01.1 Are application security policies and procedures maintained in least annually?</td>
</tr>
<tr>
<td>Security</td>
<td>Application and Software Assurance</td>
<td>A&amp;A-01.1 Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to support safe planning, risk analysis, security control assessment, configuration, remediation schedules, report generation, and review of past reports and supporting evidence?</td>
</tr>
<tr>
<td>Security</td>
<td>Authorization</td>
<td>AB-01.1 Are baseline requirements to secure internal applications established, documented, and maintained?</td>
</tr>
<tr>
<td>Security</td>
<td>Configuration Management</td>
<td>AB-01.1 Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?</td>
</tr>
<tr>
<td>Security</td>
<td>Cryptography</td>
<td>AB-01.1 Is BLSA process defined and implemented for application design, development, deployment, and operations per organizationally designed security requirements?</td>
</tr>
<tr>
<td>Security</td>
<td>Data Maintenance</td>
<td>AB-01.1 Does the engineering security review process to assess new information systems, applications, and new services while ensuring application security, compliance adherence, and operational speed of delivery goals?</td>
</tr>
<tr>
<td>Security</td>
<td>Identity, Credential, and Access Management</td>
<td>AB-01.2 Is property protection defined and implemented to protect application code in a secure, standardized, and compliant manner?</td>
</tr>
<tr>
<td>Security</td>
<td>Integrity</td>
<td>AB-01.2 Is the deployment and integration of application code protected and validated?</td>
</tr>
<tr>
<td>Security</td>
<td>Media Protection</td>
<td>AB-01.2 Are application security vulnerabilities remediated following defined processes?</td>
</tr>
<tr>
<td>Security</td>
<td>Physical and Environmental Protection</td>
<td>AB-01.2 Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?</td>
</tr>
<tr>
<td>Security</td>
<td>Security Assessment and Awareness</td>
<td>AB-01.2 Are application security policies and procedures maintained in least annually?</td>
</tr>
<tr>
<td>Security</td>
<td>Security Continuous Monitoring and Assumptions Verification</td>
<td>AB-01.2 Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to support safe planning, risk analysis, security control assessment, configuration, remediation schedules, report generation, and review of past reports and supporting evidence?</td>
</tr>
<tr>
<td>Security</td>
<td>Security Testing, Measurement, and Articulation</td>
<td>AB-01.2 Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?</td>
</tr>
<tr>
<td>Security</td>
<td>Security Incident Response</td>
<td>AB-01.2 Is the deployment and integration of application code protected and validated?</td>
</tr>
<tr>
<td>Security</td>
<td>Security Program</td>
<td>AB-01.2 Are application security vulnerabilities remediated following defined processes?</td>
</tr>
<tr>
<td>Compliance</td>
<td>Record of Processing Activities</td>
<td>AB-01.2 Is the deployment and integration of application code protected and validated?</td>
</tr>
<tr>
<td>Compliance</td>
<td>Requirements Compliance</td>
<td>AB-01.2 Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>Information System Continuous Monitoring and Assumptions Verification</td>
<td>AB-01.2 Are application security vulnerabilities remediated following defined processes?</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>Information System Security Testing and Measurement</td>
<td>AB-01.2 Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>Information System Security Configuration Management</td>
<td>AB-01.2 Are application security vulnerabilities remediated following defined processes?</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>Information System Security Incident Response</td>
<td>AB-01.2 Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>Information System Security Continuous Monitoring and Assurance</td>
<td>AB-01.2 Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>Information System Security Program</td>
<td>AB-01.2 Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>Information System Security Compliance and Audit</td>
<td>AB-01.2 Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?</td>
</tr>
<tr>
<td><strong>AIS-07.2</strong></td>
<td>Is the remediation of application security vulnerabilities automated when possible?</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>CSP-Compliant</td>
<td><strong>AIS-07</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-01.1</strong></th>
<th>Are business continuity management and operational resilience plans and procedures documented, approved, communicated, applied, evaluated, and maintained?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and 3rd-party</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-01.2</strong></th>
<th>Are the policies and procedures remainder and updated at least annually?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and 3rd-party</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-02.1</strong></th>
<th>Are criteria for developing business continuity and operational resilience strategies and capabilities established based on business disruption and risk exposures?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and CDIC</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-03.1</strong></th>
<th>Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk exposures?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and 3rd-party</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-04.1</strong></th>
<th>Are operational resilience strategies and capability metrics incorporated into business continuity and disaster recovery plans?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and 3rd-party</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-05.1</strong></th>
<th>Is business continuity and operational resilience documentation available to authorized stakeholders?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and 3rd-party</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-06.1</strong></th>
<th>Are the business continuity and operational resilience plans exercised and tested at least annually when significant changes occur?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and 3rd-party</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-07.1</strong></th>
<th>Can backup be restored appropriately for recovery?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and CDIC</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-08.1</strong></th>
<th>Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and 3rd-party</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCR-09.1</strong></th>
<th>Are changes to the operational resilience strategy reviewed and approved before implementation to ensure compliance with required legal and regulatory requirements?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Shared CSP and CDIC</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>BCT-01</strong></th>
<th>InterSystems delivers offerings using a business continuity and disaster recovery process consistent with ISO 22301.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>InterSystems and IaaS Provider provide 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. InterSystems and the IaaS Provider maintain documentation available internally to their respective personnel through the use of each organization's Intranet sites. Refer to ISO 27001 Appendix A Domain 12.</td>
</tr>
</tbody>
</table>
InterSystems (CSA) Consensus Assessments Initiative Questionnaire for InterSystems TrakCare

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 (as per ISO 27001 and ISO 22301 standards). Refer to ISO 27001 standard, Annex A, domain 17 and ISO 22301 for further details on business continuity standards.

BCR-11
Are business-critical systems supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?  

Yes  3rd-party outsourced

Each of the IaaS Provider’s data centers is evaluated to follow the Data Centered Map (DCM) standard. Aroma, A, Domain 17 and link for Data Centered Map standards.

CCC-01.1
Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configurations, etc., established, documented, approved, reviewed, executed, evaluated and maintained (regardless of whether asset management is internal or external)?  

Yes  Shared CSP and CSC

Intersystems implementation of Global Trust program is designed to incorporate methodologies and processes to provide assurance and compliance with the Data Centered Map (DCM), Crisis Management, Business Continuity, and Business Resilience standards. The IaaS Provider will test its disaster response plan annually or when changes are implemented to the production environment.

CCC-08.2
Are risks associated with changing organizational assets (including applications, systems, infrastructure, configurations, etc.) managed, regardless of whether asset management is internal or external (i.e., outsourced)?  

Yes  Shared CSP and CSC

To the intent that realizations can be made by the Customer, they may have a change management processes to manage those changes.

CCC-08.1
Is a defined quality change control approval and review process (backed by established baseline, testing and release standards) followed?  

Yes  Shared CSP and CSC

Follow a defined quality change control, approval and review process (backed by established baseline, testing and release standards).

CCC-03.1
Are all critical change control approvals and reviews (backed by established baseline, testing and release standards) reviewed?  

Yes  Shared CSP and CSC

Review all critical change control approvals and reviews (backed by established baseline, testing and release standards).

CCC-02.1
Is the unauthorized addition, removal, update, and management of organizational assets to include application, systems, infrastructure, configuration, etc., managed, regardless of whether asset management is internal or external?  

Yes  Shared CSP and CSC

To the intent that realizations can be made by the Customer, they may have a change management processes to manage those changes.

CCC-01.2
Are risks associated with changing organizational assets (including applications, systems, infrastructure, configurations, etc.) managed, regardless of whether asset management is internal or external (i.e., outsourced)?  

Yes  Shared CSP and CSC

To the intent that realizations can be made by the Customer, they may have a change management processes to manage those changes.

CCC-08.1
Is a defined quality change control approval and review process (backed by established baseline, testing and release standards) followed?  

Yes  Shared CSP and CSC

Follow a defined quality change control, approval and review process (backed by established baseline, testing and release standards).

CCC-03.1
Are all critical change control approvals and reviews (backed by established baseline, testing and release standards) reviewed?  

Yes  Shared CSP and CSC

Review all critical change control approvals and reviews (backed by established baseline, testing and release standards).

CCC-02.1
Is the unauthorized addition, removal, update, and management of organizational assets to include application, systems, infrastructure, configuration, etc., managed, regardless of whether asset management is internal or external?  

Yes  Shared CSP and CSC

To the intent that realizations can be made by the Customer, they may have a change management processes to manage those changes.

CCC-01.2
Are risks associated with changing organizational assets (including applications, systems, infrastructure, configurations, etc.) managed, regardless of whether asset management is internal or external (i.e., outsourced)?  

Yes  Shared CSP and CSC

To the intent that realizations can be made by the Customer, they may have a change management processes to manage those changes.

CCC-08.1
Is a defined quality change control approval and review process (backed by established baseline, testing and release standards) followed?  

Yes  Shared CSP and CSC

Follow a defined quality change control, approval and review process (backed by established baseline, testing and release standards).

CCC-03.1
Are all critical change control approvals and reviews (backed by established baseline, testing and release standards) reviewed?  

Yes  Shared CSP and CSC

Review all critical change control approvals and reviews (backed by established baseline, testing and release standards).

CCC-02.1
Is the unauthorized addition, removal, update, and management of organizational assets to include application, systems, infrastructure, configuration, etc., managed, regardless of whether asset management is internal or external?  

Yes  Shared CSP and CSC

To the intent that realizations can be made by the Customer, they may have a change management processes to manage those changes.

CCC-01.2
Are risks associated with changing organizational assets (including applications, systems, infrastructure, configurations, etc.) managed, regardless of whether asset management is internal or external (i.e., outsourced)?  

Yes  Shared CSP and CSC

To the intent that realizations can be made by the Customer, they may have a change management processes to manage those changes.

CCC-08.1
Is a defined quality change control approval and review process (backed by established baseline, testing and release standards) followed?  

Yes  Shared CSP and CSC

Follow a defined quality change control, approval and review process (backed by established baseline, testing and release standards).

CCC-03.1
Are all critical change control approvals and reviews (backed by established baseline, testing and release standards) reviewed?  

Yes  Shared CSP and CSC

Review all critical change control approvals and reviews (backed by established baseline, testing and release standards).

CCC-02.1
Is the unauthorized addition, removal, update, and management of organizational assets to include application, systems, infrastructure, configuration, etc., managed, regardless of whether asset management is internal or external?  

Yes  Shared CSP and CSC

To the intent that realizations can be made by the Customer, they may have a change management processes to manage those changes.

CCC-01.2
Are risks associated with changing organizational assets (including applications, systems, infrastructure, configurations, etc.) managed, regardless of whether asset management is internal or external (i.e., outsourced)?  

Yes  Shared CSP and CSC

To the intent that realizations can be made by the Customer, they may have a change management processes to manage those changes.
InterSystems (CSA) Consensus Assessments Initiative Questionnaire for InterSystems TrakCare

CCC-09.1
Is a process to manage changes, including residual risk, cost, and benefits analysis.

Encryption Change Cost Benefit Analysis
CEK-07

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-11.1
Key Purpose
CSC-owned
CSC-owned
CSC-owned
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-10.1
CEK Roles and Responsibilities
InterSystems apply a systematic approach to managing change to ensure that all changes to production environment are reviewed, tested, and approved. This organization’s change management approach ensures that the following steps occur before a change is deployed to the production environment:

CEK-09.1
1. Document and communicate the change to the appropriate change management notification list.
2. Test the change in a logically segregated, nonproduction environment.
3. Complete a risk review of the change with a focus on business impact and technical rigor. The review should include a business impact analysis to determine the potential business impact of the change:
   a. Business impact analysis is performed to determine the potential business impact of the change.
   b. Cost and benefits analysis is performed to determine the economic impact of the change.
   c. Residual risk assessment is performed to determine the potential risk remaining after the change is implemented.
4. Review and update the policies and procedures at least annually.
5. Retain approval for the change by an authorized individual.

CEK-08.1
Provide detailed and comprehensive process to protect, test, and implement changes that accommodate internal and external sources.

CEK-07.1
Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures managed and updated at a frequency proportional to the system’s risk exposure, and after any security audit?

Yes
Yes
Yes
Yes

CEK-06.1
Are cryptographic keys revoked and removed before the end of the established cryptoperiod?

Yes
Yes
Yes
Yes

CEK-05.1
Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures evaluated for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?

Yes
Yes
Yes
Yes

CEK-04.1
Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures reviewed, approved, and implemented, and maintained that includes provisions for legal and regulatory requirements.

Yes
Yes
Yes
Yes

CEK-03.1
Are cryptographic keys generated using industry-accepted and approved cryptographic libraries certified to approved standards?

Yes
Yes
Yes
Yes

CEK-02.1
Are cryptographic keys revoked and removed before the end of the established cryptoperiod?

Yes
Yes
Yes
Yes

CEK-01.1
Is a cryptographic and key management risk program established and maintained that includes risk assessment, risk management, risk controls, monitoring, and feedback provisions?

Yes
Yes
Yes
Yes

CEK-00.1
Are cryptographic and key management policies, procedures, and technology changes that accommodate internal and external sources managed and updated at a frequency proportional to the system’s risk exposure, and after any security audit?

Yes
Yes
Yes
Yes

CEK-09
CSP-owned
CSC-owned
CSC-owned
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
CSP-owned
CSC-owned
CSC-owned
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-07
CSP-owned
CSC-owned
CSC-owned
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
CSP-owned
CSC-owned
CSC-owned
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
CSP-owned
CSC-owned
CSC-owned
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
CSP-owned
CSC-owned
CSC-owned
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
CSP-owned
CSC-owned
CSC-owned
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
CSP-owned
CSC-owned
CSC-owned
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
CSP-owned
CSC-owned
CSC-owned
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-00
CSP-owned
CSC-owned
CSC-owned
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.
### ARE POLICIES AND PROCEDURES FOR THE RELocations OR TRANSFER OF HARDWARE, SOFTWARE, OR DATA/INFORMATION TO AN OFFSITE OR ALTERNATE LOCATION ESTABLISHED, DOCUMENTED, COMMUNICATED, APPLIED, MONITORED, AND MAINTAINED?

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Yes/No/NA</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CER-14.1</td>
<td>Are processes, procedures, and technical measures to destroy unneeded keys defined, implemented, and evaluated to include legal and regulatory requirement provisions?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>CER-14.2</td>
<td>The solution allows the Customer to manage the encryption keys for a Customer solution and, as such, InterSystems does not hold, manage or store any encryption keys for a Customer solution and, as such, InterSystems does not hold, manage or store any encryption keys for Customers.</td>
<td>Yes</td>
<td>Key Protection</td>
</tr>
<tr>
<td>CER-14.3</td>
<td>Do processes, procedures, and technical measures to deactivate keys (at the end of their operational life) defined, implemented, and evaluated to include legal and regulatory requirement provisions?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>CER-14.4</td>
<td>The solution allows the Customer to manage the encryption keys for a Customer solution and, as such, InterSystems does not hold, manage or store any encryption keys for a Customer solution and, as such, InterSystems does not hold, manage or store any encryption keys for Customers.</td>
<td>Yes</td>
<td>Key Suppression</td>
</tr>
<tr>
<td>CER-14.5</td>
<td>Are key management system processes, procedures, and technical measures to deactivate keys, which include provisions for legal and regulatory requirement provisions?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>CER-14.6</td>
<td>The solution allows the Customer to manage the encryption keys for a Customer solution and, as such, InterSystems does not hold, manage or store any encryption keys for a Customer solution and, as such, InterSystems does not hold, manage or store any encryption keys for Customers.</td>
<td>Yes</td>
<td>Key Suppression</td>
</tr>
<tr>
<td>CER-14.7</td>
<td>Are key management system processes, procedures, and technical measures to destroy unneeded keys defined, implemented, and evaluated to include legal and regulatory requirement provisions?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>CER-14.8</td>
<td>The solution allows the Customer to manage the encryption keys for a Customer solution and, as such, InterSystems does not hold, manage or store any encryption keys for a Customer solution and, as such, InterSystems does not hold, manage or store any encryption keys for Customers.</td>
<td>Yes</td>
<td>Key Suppression</td>
</tr>
</tbody>
</table>

---

### ARE POLICIES AND PROCEDURES FOR THE MANAGEMENT OF CRYPTOGRAPHIC MATERIALS (INCLUDING BUT NOT LIMITED TO KEYS) DEFINED, IMPLEMENTED, AND EVALUATED TO INCLUDE LEGAL AND REGULATORY REQUIREMENT PROVISIONS?

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Yes/No/NA</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCS-01.1</td>
<td>Are policies and procedures for the secure disposal of equipment used within the enterprise system established, documented, approved, communicated, implemented, and maintained?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-01.2</td>
<td>The IaaS Provider SOC reports provide additional details on the specific asset management related policies and control activities.</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-01.3</td>
<td>The IaaS Provider SOC reports provide additional details on the specific asset management related policies and control activities.</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-01.4</td>
<td>The IaaS Provider SOC reports provide additional details on the specific asset management related policies and control activities.</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-02.1</td>
<td>Is a class determination procedure utilized that redacts information recovery information regarding a non-personally identifiable?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-02.2</td>
<td>The IaaS Provider SOC reports provide additional details on the specific asset management related policies and control activities.</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-03.1</td>
<td>Are policies and procedures for the destruction or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, and maintained?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-03.2</td>
<td>Are policies and procedures for the destruction or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, and maintained?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-04.1</td>
<td>Are key management system processes, procedures, and technical measures to manage archived keys in a secure repository requiring least privilege access defined, implemented, and evaluated to include legal and regulatory requirement provisions?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-04.2</td>
<td>The IaaS Provider SOC reports provide additional details on the specific asset management related policies and control activities.</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-05.1</td>
<td>Are policies and procedures for the destruction or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, and maintained?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-05.2</td>
<td>Are policies and procedures for the destruction or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, and maintained?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-06.1</td>
<td>Are policies and procedures for the destruction or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, and maintained?</td>
<td>Yes</td>
<td>CISC-owned</td>
</tr>
<tr>
<td>DCS-03.1</td>
<td>Are policies and procedures for the management of physical security processes, including at all ingress and egress points implemented, maintained, and operated?</td>
<td>Yes</td>
<td>Shared CSP and 3rd party. Intersystems and the IaaS Provider engage with external auditors to evaluate operational compliance with policies.</td>
</tr>
<tr>
<td>DCS-03.2</td>
<td>Are policies and procedures for the management of physical security processes, including at all ingress and egress points implemented, maintained, and operated?</td>
<td>Yes</td>
<td>Intersystems' Data Center Physical Security Policy is designed to ensure compliance with global standards including ISO 27001, ISO 27002, and ISO 270038 standards.</td>
</tr>
<tr>
<td>DCS-04.1</td>
<td>Are physical security perimeters established to safeguard personnel, data, and information systems?</td>
<td>Yes</td>
<td>Physical security perimeters 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's Physical Security Policy includes details on the controls and standards that are in place to safeguard personnel, data, and information systems.</td>
</tr>
<tr>
<td>DCS-04.2</td>
<td>Are physical security perimeters established to safeguard personnel, data, and information systems?</td>
<td>Yes</td>
<td>Physical security perimeters 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's Physical Security Policy includes details on the controls and standards that are in place to safeguard personnel, data, and information systems.</td>
</tr>
<tr>
<td>DCS-04.3</td>
<td>Are physical security perimeters established to safeguard personnel, data, and information systems?</td>
<td>Yes</td>
<td>Physical security perimeters 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's Physical Security Policy includes details on the controls and standards that are in place to safeguard personnel, data, and information systems.</td>
</tr>
<tr>
<td>DCS-05.1</td>
<td>Are policies and procedures for the management of physical security processes, including at all ingress and egress points implemented, maintained, and operated?</td>
<td>Yes</td>
<td>Policies and procedures for the management of physical security processes, including at all ingress and egress points are reviewed and updated at least annually.</td>
</tr>
<tr>
<td>DCS-06.1</td>
<td>Are all relevant physical and logical assets catalogued and tracked within a secured system?</td>
<td>Yes</td>
<td>Intersystems' Data Center Physical Security Policy is designed to ensure compliance with global standards including ISO 27001, ISO 27002, and ISO 270038 standards.</td>
</tr>
<tr>
<td>DCS-07.1</td>
<td>Are all relevant physical and logical assets catalogued and tracked within a secured system?</td>
<td>Yes</td>
<td>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's Physical Security Policy includes details on the controls and standards that are in place to safeguard personnel, data, and information systems.</td>
</tr>
<tr>
<td>DCS-07.2</td>
<td>Are all relevant physical and logical assets catalogued and tracked within a secured system?</td>
<td>Yes</td>
<td>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's Physical Security Policy includes details on the controls and standards that are in place to safeguard personnel, data, and information systems.</td>
</tr>
<tr>
<td>DCS-08.1</td>
<td>Are major changes to the physical security perimeters documented and reviewed?</td>
<td>Yes</td>
<td>Major changes to the physical security perimeters are documented and reviewed.</td>
</tr>
<tr>
<td>DCS-09.1</td>
<td>Are access control devices regularly tested?</td>
<td>Yes</td>
<td>Access control devices are regularly tested and monitored.</td>
</tr>
<tr>
<td>DCS-09.2</td>
<td>Are access control devices regularly tested?</td>
<td>Yes</td>
<td>Access control devices are regularly tested and monitored.</td>
</tr>
<tr>
<td>DCS-10.1</td>
<td>Are main access control devices verified and tested at least annually?</td>
<td>Yes</td>
<td>Main access control devices are verified and tested at least annually.</td>
</tr>
<tr>
<td>DCS-11.1</td>
<td>Are policies and procedures for the management of physical security processes, including at all ingress and egress points implemented, maintained, and operated?</td>
<td>Yes</td>
<td>Policies and procedures for the management of physical security processes, including at all ingress and egress points are reviewed and updated at least annually.</td>
</tr>
<tr>
<td>DCS-12.1</td>
<td>Are policies and procedures for the management of physical security processes, including at all ingress and egress points implemented, maintained, and operated?</td>
<td>Yes</td>
<td>Policies and procedures for the management of physical security processes, including at all ingress and egress points are reviewed and updated at least annually.</td>
</tr>
<tr>
<td>DCS-13.1</td>
<td>Are policies and procedures for the management of physical security processes, including at all ingress and egress points implemented, maintained, and operated?</td>
<td>Yes</td>
<td>Policies and procedures for the management of physical security processes, including at all ingress and egress points are reviewed and updated at least annually.</td>
</tr>
<tr>
<td>DCS-14.1</td>
<td>Are policies and procedures for the management of physical security processes, including at all ingress and egress points implemented, maintained, and operated?</td>
<td>Yes</td>
<td>Policies and procedures for the management of physical security processes, including at all ingress and egress points are reviewed and updated at least annually.</td>
</tr>
<tr>
<td>DCS-15.1</td>
<td>Are policies and procedures for the management of physical security processes, including at all ingress and egress points implemented, maintained, and operated?</td>
<td>Yes</td>
<td>Policies and procedures for the management of physical security processes, including at all ingress and egress points are reviewed and updated at least annually.</td>
</tr>
</tbody>
</table>
DSP-01.1 Are policies and procedures established, documented, approved, communicated, reviewed, and updated on an ongoing basis according to applicable laws and regulations, and any changes made to the solution are documented? Yes Shown CSP and CSC

The InterSystems solution can be deployed as the Customer determines appropriate using the data security, protection, privacy, and risk management principles of the solution. The solution can support several methods to perform secure data destruction or disposal, including physical destruction, media sanitization, and destruction on premises. The solution can support several methods to perform secure data destruction or disposal, including physical destruction, media sanitization, and destruction on premises.

Are systems, products, and business practices based on security principles orDo CSPs own and maintain data ownership and data management documentation to meet their requirements? Yes Shown CSP and CSC

The solution can support several methods to perform secure data destruction or disposal, including physical destruction, media sanitization, and destruction on premises. The solution can support several methods to perform secure data destruction or disposal, including physical destruction, media sanitization, and destruction on premises. The solution can support several methods to perform secure data destruction or disposal, including physical destruction, media sanitization, and destruction on premises.

Are policies and procedures established, documented, approved, communicated, reviewed, and updated on an ongoing basis according to applicable laws and regulations? Shown CSP and CSC

The InterSystems solution can be deployed as the Customer determines appropriate using the data security, protection, privacy, and risk management principles of the solution. The solution can support several methods to perform secure data destruction or disposal, including physical destruction, media sanitization, and destruction on premises.

Is a data inventory created and maintained for sensitive and personal information? Yes Shown CSP and CSC

The InterSystems solution can be deployed as the Customer determines appropriate using the data security, protection, privacy, and risk management principles of the solution. The solution can support several methods to perform secure data destruction or disposal, including physical destruction, media sanitization, and destruction on premises.

Is a data inventory created and maintained for sensitive and personal information (on-premise)? Shown CSP and CSC

The InterSystems solution can be deployed as the Customer determines appropriate using the data security, protection, privacy, and risk management principles of the solution. The solution can support several methods to perform secure data destruction or disposal, including physical destruction, media sanitization, and destruction on premises.

Are systems, products, and business practices based on privacy principles orDo CSPs own and maintain data ownership and data management documentation to meet their requirements? Yes Shown CSP and CSC

The InterSystems solution can be deployed as the Customer determines appropriate using the data security, protection, privacy, and risk management principles of the solution. The solution can support several methods to perform secure data destruction or disposal, including physical destruction, media sanitization, and destruction on premises.
InterSystems (CSA) Consensus Assessments Initiative Questionnaire for InterSystems TrakCare

DSP-15.1 Is authorization from data sources obtained, and the associated risk managed, before replacing or using production data in non-production environments?  
Yes  Shared CSP and CSC

DSP-16.1 On-site, remote, and cloud are captured, shared, and distributed in accordance with business requirements, applicable laws, and regulations?  
Yes  Shared CSP and CSC

DSP-17.1 Are processes, procedures, and technical measures defined and implemented to preserve original data throughout its lifecycle?  
Yes  CSC-owned

DSP-18.1 Does the CSP go to plan, and describe CSPs, the processes to manage and report on requirements for disposal of Personally Identifiable Information (PII)?  
Yes  CSP-owned

DSP-18.2 Does the CSP go special attention to the non-preservation to increase CSPs, unless otherwise prohibited?  
Yes  CSP-owned

The Global Trust monitors legislative and regulatory requirements, but not limited to remote employees, contractors, and third parties (including but not limited to remote employees, contractors, and third parties). The InterSystems and the IaaS Provider shall specify and document physical data locations, including locales where data is processed or backed up.

GRC-01.1 Are data policies and procedures maintained and updated at least annually?  
Yes  Shared CSP and CSC

GRC-01.2 Are the established formal, documented, and leadership sponsored processes, policies, and procedures for the Global Trust program?  
Yes  CSP-owned

GRC-02.1 Is there an established formal, documented, and leadership sponsored processes, policies, and procedures for the Global Trust program?  
Yes  CSP-owned

GRC-03.1 Are there established formal, documented, and leadership sponsored processes, policies, and procedures for the Global Trust program?  
Yes  CSP-owned

GRC-04.1 In an approved exception process managed by the governance program established and followed whenever a deviation from an established policy occurs?  
Yes  Shared CSP and CSC

GRC-04.2 The CSP has an established information security program (ISPP) which includes policies and procedures for information governance, including business continuity and disaster recovery. The CSP must maintain ownership of their data and be responsible for authorizing processing.  
Yes  Shared CSP and CSC

GRC-05.1 Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?  
Yes  Shared CSP and CSC

GRC-06.1 How is the security information program (including programs of all relevant SGCC domains) been developed and implemented?  
Yes  Shared CSP and CSC

GRC-07.1 Are all relevant standards, regulations, high-level, and secondary requirements applicable to their organization identified and documented?  
Yes  Shared CSP and CSC

GRC-08.1 Is control established and maintained with cloud-related special interest groups and other relevant alliances?  
Yes  Shared CSP and CSC

GRC-09.1 Are background and identification checks of all new employees (including non-full time, contract employees, vendors, and third-party partners, subcontracted, approved, contracted, audited, evaluated, and evaluated)  
Yes  Shared CSP and CSC

GRC-10.1 Is the InterSystems and the CSP provide background checks and verification of all new employees (including non-full time, contract employees, vendors, and third-party partners, subcontracted, approved, contracted, audited, evaluated, and evaluated)  
Yes  Shared CSP and CSC
Are background verification policies and procedures designed according to local laws, regulations, rules, and contractual constraints and proportional to the level of access to facilities and resources? Are employment screening practices for employees commensurate with the employer's need and level of access to facilities and resources? Is the processing of information on an employee's background reviewed and updated at least annually?

Yes Shown in COP and CSCP

InterSystems and the IaaS Provider conduct criminal background checks of prospective employees in conformance with local laws, regulations, rules, and contractual constraints and proportional to the level of access to facilities and resources. Employment screening practices are reviewed and updated at least as required by local laws, regulations, rules, and contractual constraints.

The Customer is responsible for maintaining background verification policies and procedures required by the Customer's laws, regulations, rules, and contractual constraints and proportional to the level of access to facilities and resources. The Customer is responsible for reviewing and updating employment screening practices at least as required by the Customer's laws, regulations, rules, and contractual constraints.

HRS-01.2

Are background verification policies and procedures designed and updated at least annually?

Yes Shown in COP and CSCP

InterSystems Global Trust program is designed in compliance with global standards regarding obligations for data protection, privacy, and security. The IaaS Provider is responsible for establishing processes to secure and manage data classified as sensitive. The IaaS Provider must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

Upon termination of InterSystems employee or contractors, the IaaS Provider must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-02.1

Are policies and procedures defining dimensions and conditions for the acceptable use of organizationally-owned or managed assets designed and documented?

Yes Shown in COP and CSCP

The Customer must provide employees with documented instructions on acceptable use of organizationally-owned or managed assets. The IaaS Provider must have documented instructions on acceptable use of organizationally-owned or managed assets.

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-02.2

Are policies and procedures for identifying, evaluating, and resolving incidents and disputes relating to the use and classification of sensitive data designed and documented?

Yes Shown in COP and CSCP

The IaaS Provider must have documented instructions on acceptable use of organizationally-owned or managed assets. The IaaS Provider must have documented instructions on acceptable use of organizationally-owned or managed assets.

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-03.1

Are background verification policies and procedures designed and updated at least annually?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-04.1

Are policies and procedures for protecting sensitive information, personal or sensitive asset returns?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-04.2

Are policies and procedures for handling and classification of sensitive data included in employment agreements?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-04.3

Are employee roles and responsibilities relating to information assets and security defined, documented, approved, communicated, applied, included, and maintained?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-05.1

Are policies and procedures for handling and classification of sensitive data included in employment agreements?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-05.2

Are policies and procedures for handling and classification of sensitive data included in employment agreements?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-05.3

Are policies and procedures for handling and classification of sensitive data included in employment agreements?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-05.4

Are policies and procedures for handling and classification of sensitive data included in employment agreements?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-05.5

Are employee roles and responsibilities relating to information assets and security defined, documented, approved, communicated, applied, included, and maintained?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-06.1

Are employee roles and responsibilities relating to information assets and security defined, documented, approved, communicated, applied, included, and maintained?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-06.2

Are employee roles and responsibilities relating to information assets and security defined, documented, approved, communicated, applied, included, and maintained?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-06.3

Are employee roles and responsibilities relating to information assets and security defined, documented, approved, communicated, applied, included, and maintained?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-06.4

Are employee roles and responsibilities relating to information assets and security defined, documented, approved, communicated, applied, included, and maintained?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-06.5

Are employee roles and responsibilities relating to information assets and security defined, documented, approved, communicated, applied, included, and maintained?

Yes Shown in COP and CSCP

The Customer is responsible for establishing processes to secure and manage data classified as sensitive. The Customer must have an acceptable use policy that requires unattended workspaces to conceal confidential data visible in the company facility.

HRS-06.6
### InterSystems (CSA) Consensus Assessments Initiative Questionnaire for InterSystems TrakCare

**HRS-11.1**

<table>
<thead>
<tr>
<th><strong>Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

**HRS-11.2**

<table>
<thead>
<tr>
<th><strong>Are regular security awareness testing updates provided?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

**HRS-11.3**

<table>
<thead>
<tr>
<th><strong>Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**IAM-01.1**

<table>
<thead>
<tr>
<th><strong>Are employees provided access to sensitive organizational and personal data with appropriate security awareness training?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

**IAM-01.2**

<table>
<thead>
<tr>
<th><strong>Are employees modified at their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and compliance legal, statutory, or regulatory compliance obligations?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

**IAU-01.1**

<table>
<thead>
<tr>
<th><strong>Are changes in access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated and maintained?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**IAM-02.1**

<table>
<thead>
<tr>
<th><strong>Are changes in access management policies and procedures maintained and updated at least annually?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

**IAM-02.2**

<table>
<thead>
<tr>
<th><strong>Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated and maintained?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

**IAM-02.3**

<table>
<thead>
<tr>
<th><strong>Are strong password policies and procedures maintained and updated at least annually?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

**IAM-02.4**

<table>
<thead>
<tr>
<th><strong>Is system identity information and limits of access managed, stored, and reviewed?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>
IAM-05.1 Is the least privilege principle employed when implementing information system access?
Yes: InterSystems and the IaaS Provider share a formal access control policy for all policies, processes, procedures, and controls, and no user has system-level privileges. InterSystems and the IaaS Provider communicate and coordinate concerning the access control polices. InterSystems and the IaaS Provider maintain formal access control policies for system identities.
No: InterSystems and the IaaS Provider share no access control policies. InterSystems and the IaaS Provider communicate and coordinate concerning the access control policies. InterSystems and the IaaS Provider maintain no formal access control policies for system identities.

IAM-06.1 Is user access provisioning performed defined and implemented without associated risk assessments, and羌communicate identity and access management policies?
Yes: InterSystems and the IaaS Provider enforce access control procedures that are centrally defined and implemented for all users without associated risk assessments. InterSystems and the IaaS Provider communicate and coordinate concerning the access control procedures. InterSystems and the IaaS Provider maintain formal access control procedures for system identities.
No: InterSystems and the IaaS Provider share no access control procedures. InterSystems and the IaaS Provider communicate and coordinate concerning the access control procedures. InterSystems and the IaaS Provider maintain no formal access control procedures for system identities.

IAM-07.1 Are review and revocation of user access for least privilege and separation of duties ensured with a frequent communication with organizational risk assessment?
Yes: InterSystems and the IaaS Provider ensure that least privilege and separation of duties are ensured through frequent communication with the organizational risk assessment.
No: InterSystems and the IaaS Provider share no least privilege and separation of duties. InterSystems and the IaaS Provider communicate and coordinate concerning the least privilege and separation of duties. InterSystems and the IaaS Provider maintain no formal least privilege and separation of duties.

IAM-11.1 Is or are processes defined and implemented to ensure privileged access roles and rights are granted for a limited period?
Yes: InterSystems and the IaaS Provider define and implement processes for ensuring that privileged access roles and rights are granted for a limited period. InterSystems and the IaaS Provider ensure that the process is applied consistently for all users. InterSystems and the IaaS Provider maintain formal access control processes for system identities.
No: InterSystems and the IaaS Provider share no processes for ensuring that privileged access roles and rights are granted for a limited period. InterSystems and the IaaS Provider communicate and coordinate concerning the processes for ensuring that privileged access roles and rights are granted for a limited period. InterSystems and the IaaS Provider maintain no formal processes for ensuring that privileged access roles and rights are granted for a limited period.

IAM-12.1 Is the ability to disable the "read-only" configuration of logging infrastructure prevented?
Yes: InterSystems enforce the ability to disable the "read-only" configuration of logging infrastructure.
No: InterSystems do not enforce the ability to disable the "read-only" configuration of logging infrastructure.

IAM-13.1 Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that accountability is evident through access control procedures?
Yes: InterSystems and the IaaS Provider define and implement processes, procedures, and technical measures for the segregation of privileged access roles such that accountability is evident through access control procedures. InterSystems and the IaaS Provider ensure that the process is applied consistently for all users. InterSystems and the IaaS Provider maintain formal processes, procedures, and technical measures for the segregation of privileged access roles.
No: InterSystems and the IaaS Provider share no processes, procedures, and technical measures for the segregation of privileged access roles. InterSystems and the IaaS Provider communicate and coordinate concerning the processes, procedures, and technical measures for the segregation of privileged access roles. InterSystems and the IaaS Provider maintain no formal processes, procedures, and technical measures for the segregation of privileged access roles.

IAM-14.1 Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated for all privileged accounts?
Yes: InterSystems and the IaaS Provider define and implement processes, procedures, and technical measures for the secure management of passwords for all privileged accounts. InterSystems and the IaaS Provider ensure that the process is applied consistently for all users. InterSystems and the IaaS Provider maintain formal processes, procedures, and technical measures for the secure management of passwords.
No: InterSystems and the IaaS Provider share no processes, procedures, and technical measures for the secure management of passwords. InterSystems and the IaaS Provider communicate and coordinate concerning the processes, procedures, and technical measures for the secure management of passwords. InterSystems and the IaaS Provider maintain no formal processes, procedures, and technical measures for the secure management of passwords.

IAM-15.1 Are processes, procedures, and technical measures for authenticating access to resources defined, implemented, and evaluated such that accountability is evident through access control procedures?
Yes: InterSystems and the IaaS Provider define and implement processes, procedures, and technical measures for authenticating access to resources such that accountability is evident through access control procedures. InterSystems and the IaaS Provider ensure that the process is applied consistently for all users. InterSystems and the IaaS Provider maintain formal processes, procedures, and technical measures for authenticating access to resources.
No: InterSystems and the IaaS Provider share no processes, procedures, and technical measures for authenticating access to resources. InterSystems and the IaaS Provider communicate and coordinate concerning the processes, procedures, and technical measures for authenticating access to resources. InterSystems and the IaaS Provider maintain no formal processes, procedures, and technical measures for authenticating access to resources.

IAM-16.1 Are processes, procedures, and technical measures for determining and implementing the least privilege and separation of duties ensured with a frequent communication with organizational risk assessment?
Yes: InterSystems and the IaaS Provider ensure that least privilege and separation of duties are ensured through frequent communication with the organizational risk assessment.
No: InterSystems and the IaaS Provider share no least privilege and separation of duties. InterSystems and the IaaS Provider communicate and coordinate concerning the least privilege and separation of duties. InterSystems and the IaaS Provider maintain no formal least privilege and separation of duties.

IAM-20.1 Are procedures implemented to protect the sub-system of segregated privileged access?
Yes: InterSystems and the IaaS Provider implement procedures to protect the sub-system of segregated privileged access.
No: InterSystems and the IaaS Provider share no procedures to protect the sub-system of segregated privileged access. InterSystems and the IaaS Provider communicate and coordinate concerning the procedures to protect the sub-system of segregated privileged access. InterSystems and the IaaS Provider maintain no formal procedures to protect the sub-system of segregated privileged access.
Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability is addressed in the product documentation.

IPY-01.1

Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability is addressed in the product documentation.

IPY-01.2

Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability is addressed in the product documentation.

IPY-01.3

Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability is addressed in the product documentation.

IPY-01.4

Are interoperability and portability policies and procedures restated and updated at least annually?

Yes CSCI7 written

Interoperability and portability is addressed in the product documentation.

IPY-01.5

Are security processes, procedures, and controls designed, developed, reviewed, implemented, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability policies are restated and updated at least annually.

IPY-01.6

Are security processes, procedures, and controls designed, developed, reviewed, implemented, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability policies are restated and updated at least annually.

IPY-01.7

Are security processes, procedures, and controls designed, developed, reviewed, implemented, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability policies are restated and updated at least annually.

IPY-01.8

Are security processes, procedures, and controls designed, developed, reviewed, implemented, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability policies are restated and updated at least annually.

IPY-01.9

Are security processes, procedures, and controls designed, developed, reviewed, implemented, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability policies are restated and updated at least annually.

IPY-01.10

Are security processes, procedures, and controls designed, developed, reviewed, implemented, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability policies are restated and updated at least annually.

IPY-01.11

Are security processes, procedures, and controls designed, developed, reviewed, implemented, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability policies are restated and updated at least annually.

IPY-01.12

Are security processes, procedures, and controls designed, developed, reviewed, implemented, and maintained for information security, regulatory/compliance, operational, and business continuity requirements?

Yes CSCI7 written

Interoperability and portability policies are restated and updated at least annually.

IPY-01.13
LOG-01.1: Are logging and monitoring policies and procedures established, documented, approved, communicated, signed, reviewed, and maintained?
Yes

InterSystems maintains the Global Trust program designed to assist in security incident response, including handling, evaluation, and response to security incidents. This program leverages logical and physical infrastructure to provide additional layers of defense to protect information and data from unauthorized access, use, modification, and disclosure.

LOG-01.2: Are policies and procedures reviewed and updated at least annually?
Yes

InterSystems maintains a log alerting process to ensure prompt notification of detected vulnerabilities. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

LOG-01.3: Are logging requirements for information meta-data system events established, documented, approved, communicated, applied, evaluated, and maintained?
Yes

The Customer is responsible for monitoring security audit logs to identify activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions to address anomalies.

LOG-01.4: Is a reliable time source used across all relevant information processing systems?
Yes

InterSystems manages cryptographic keys related to internal cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained.

LOG-01.5: Are security audit logs monitored to detect activity outside of typical or expected patterns?
Yes

The Customer has responsibility for managing cryptographic keys related to internal security. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

LOG-01.6: Are security-related events identified and monitored across applications and the underlying infrastructure?
Yes

InterSystems maintains a log alerting process to ensure prompt notification of detected vulnerabilities. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

LOG-01.7: Do policies and procedures for Security Incident Management, E-Discovery, and Cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?
Yes

InterSystems maintains a log alerting process to ensure prompt notification of detected vulnerabilities. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

LOG-01.8: Are monitoring and internal reporting capabilities established to report on cryptographic keys' usage?
Yes

The Customer has responsibility for managing cryptographic keys related to internal security. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

LOG-01.9: Are monitoring and internal reporting capabilities established to report on cryptographic keys' usage?
Yes

The Customer has responsibility for managing cryptographic keys related to internal security. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

LOG-01.10: Is a security incident response plan, which includes but is not limited to: relevant policies and procedures at least annually.
Yes

InterSystems maintains a log alerting process to ensure prompt notification of detected vulnerabilities. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

LOG-01.11: Are log management events logged and monitored on a continuous basis?
Yes

InterSystems maintains a log alerting process to ensure prompt notification of detected vulnerabilities. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

LOG-01.12: Are physical access logs logged and monitored on a continuous basis?
Yes

InterSystems maintains a log alerting process to ensure prompt notification of detected vulnerabilities. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

LOG-01.13: Are security-related events identified and monitored across applications and the underlying infrastructure?
Yes

InterSystems maintains a log alerting process to ensure prompt notification of detected vulnerabilities. The solution uses a central audit system that logs all relevant system, application, and user events. Logs can be retained for an extended period of time to allow for the review of historical events and trends.

SVF-01.1: Are policies and procedures for security incident management, governance, and management established, documented, approved, communicated, signed, reviewed, and maintained?
Yes

InterSystems maintains the Global Trust program designed to assist in security incident response, including handling, evaluation, and response to security incidents. This program leverages logical and physical infrastructure to provide additional layers of defense to protect information and data from unauthorized access, use, modification, and disclosure.

SVF-01.2: Are policies and procedures reviewed and updated at least annually?
Yes

InterSystems maintains the Global Trust program designed to assist in security incident response, including handling, evaluation, and response to security incidents. This program leverages logical and physical infrastructure to provide additional layers of defense to protect information and data from unauthorized access, use, modification, and disclosure.

SVF-01.3: Are policies and procedures for security incident management, governance, and management established, documented, approved, communicated, signed, reviewed, and maintained?
Yes

InterSystems maintains the Global Trust program designed to assist in security incident response, including handling, evaluation, and response to security incidents. This program leverages logical and physical infrastructure to provide additional layers of defense to protect information and data from unauthorized access, use, modification, and disclosure.

SVF-01.4: Are policies and procedures reviewed and updated at least annually?
Yes

InterSystems maintains the Global Trust program designed to assist in security incident response, including handling, evaluation, and response to security incidents. This program leverages logical and physical infrastructure to provide additional layers of defense to protect information and data from unauthorized access, use, modification, and disclosure.

SVF-01.5: Are policies and procedures for security incident management, governance, and management established, documented, approved, communicated, signed, reviewed, and maintained?
Yes

InterSystems maintains the Global Trust program designed to assist in security incident response, including handling, evaluation, and response to security incidents. This program leverages logical and physical infrastructure to provide additional layers of defense to protect information and data from unauthorized access, use, modification, and disclosure.

SVF-01.6: Are policies and procedures reviewed and updated at least annually?
Yes

InterSystems maintains the Global Trust program designed to assist in security incident response, including handling, evaluation, and response to security incidents. This program leverages logical and physical infrastructure to provide additional layers of defense to protect information and data from unauthorized access, use, modification, and disclosure.

SVF-01.7: Are policies and procedures for security incident management, governance, and management established, documented, approved, communicated, signed, reviewed, and maintained?
Yes

InterSystems maintains the Global Trust program designed to assist in security incident response, including handling, evaluation, and response to security incidents. This program leverages logical and physical infrastructure to provide additional layers of defense to protect information and data from unauthorized access, use, modification, and disclosure.

SVF-01.8: Are policies and procedures reviewed and updated at least annually?
Yes

InterSystems maintains the Global Trust program designed to assist in security incident response, including handling, evaluation, and response to security incidents. This program leverages logical and physical infrastructure to provide additional layers of defense to protect information and data from unauthorized access, use, modification, and disclosure.
SEP-86.1 Is the security breach response plan and updated for all environments, as necessary, as changes occur in key personnel and/or changing business needs? Yes Shown CISP and 360pathway

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

Are security breaches and security breach notifications defined and implemented? Yes Shown CISP and 360pathway

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

SEP-87.1 Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities? Yes Shown CISP and 360pathway

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

SEP-9.1 Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities? Yes Shown CISP and 360pathway

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

STA-01.1 Are the policies and procedures that apply to the IaaS environment updated and implemented annually? Yes Shown CISP and CSCI

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

STA-02.1 Are the policies and procedures that apply to the IaaS environment updated and implemented annually? Yes Shown CISP and CSCI

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

STA-06.1 Are the persons of the CSP or organization responsible for implementation, operation, audit, or assurance? Yes Shown CISP and CSCI

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

STA-07.1 Is an inventory of all supply chain relationships developed and maintained? Yes CISP noted

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

STA-08.1 Are the persons of the CSP or organization responsible for implementation, operation, audit, or assurance? Yes Shown CISP and CSCI

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

STA-09.1 Are the policies and procedures that apply to the IaaS environment updated and implemented annually? Yes Shown CISP and CSCI

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

STA-10.1 Are the policies and procedures that apply to the IaaS environment updated and implemented annually? Yes Shown CISP and CSCI

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

STA-11.1 Are the policies and procedures that apply to the IaaS environment updated and implemented annually? Yes Shown CISP and CSCI

The InterSystems and the IaaS Provider incident response processes are defined, documented, and updated to address gaps, vulnerabilities, and impact on security incidents. These include guidance for responding to and managing security incidents including but not limited to: incident identification, isolation, containment, recovery, documentation, and reporting in a manner in accordance with Customer agreements, industry standards, and other information security policies.

Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.
| STA-08.1 | Are risk factors associated with all organizations in the supply chain periodically reviewed by CSP? | Yes | CSP-owned | The Third Party Risk Management process reviews risk factors associated with all organizations in the supply chain. Policies for identifying and evaluating risk factors for the protection of privacy and safeguards for access to maintain confidentiality, integrity, and availability of information assets. Customer, tenant, and third-party linkages to the IaaS Provider’s service. CSPs periodically review risk factors associated with all organizations in the supply chain. CSPs periodically review risk factors associated with all organizations in the supply chain. | Supply Chain Risk Management |
| STA-09.1 | Do agreements between CSPs and CSCs (tenants) incorporate at least the following security requirements? (Based on the identified risk)? | Yes | CSP-owned | The Third Party Risk Management process reviews agreements between CSPs and CSCs (tenants). Policies for identifying and evaluating risk factors for the protection of privacy and safeguards for access to maintain confidentiality, integrity, and availability of information assets. Customer, tenant, and third-party linkages to the IaaS Provider’s service. CSPs periodically review agreements between CSPs and CSCs (tenants). | Supply Chain Risk Management |
| STA-10.1 | Are supply chain agreements between CSPs and CSCs reviewed at least annually? | Yes | CSP-owned | Through the use of established assessment procedures, CSPs periodically review agreements between CSPs and CSCs (tenants). | Supply Chain Agreement Review |
| STA-11.1 | Are policies and procedures to protect against malware on managed assets established, reviewed periodically, and adequately updated? | Yes | CSP-owned | Through the use of established assessment procedures, CSPs periodically review the organization’s supply chain partners’ IT governance policies and procedures. CSPs periodically review the organization’s supply chain partners’ IT governance policies and procedures. | Internal Compliance Testing |
| STA-12.1 | Are policies that require all supply chain CSPs and 3rd-party suppliers to comply with information security, confidentiality, access control, privacy, personal policy, and service level agreements to be standard? | Yes | CSP-owned | Through the use of established assessment procedures, CSPs periodically review the organization’s supply chain partners’ IT governance policies and procedures. CSPs periodically review the organization’s supply chain partners’ IT governance policies and procedures. | Information Security Requirements (including ISMS) |
| STA-13.1 | Are supply chain agreements between CSPs and CSCs reviewed at least annually? | Yes | CSP-owned | Through the use of established assessment procedures, CSPs periodically review agreements between CSPs and CSCs (tenants). | Supply Chain Agreement Review |
| STA-14.1 | Are policies and procedures established, documented, approved, communicated, applied, measured, maintained, and continually assessed? | Yes | CSP-owned | Through the use of established assessment procedures, CSPs periodically review agreements between CSPs and CSCs (tenants). | Supply Chain Service Management |
| TVM-01.1 | Are comprehensive vulnerability management policies and procedures reviewed and updated on at least an annual basis? | Yes | CSP-owned | Through the use of established assessment procedures, CSPs periodically review agreements between CSPs and CSCs (tenants). | Theme and Vulnerability Management Policy and Procedures |
| TVM-02.1 | Are vulnerability remediation management policies and procedures reviewed and updated on at least an annual basis? | Yes | CSP-owned | Through the use of established assessment procedures, CSPs periodically review agreements between CSPs and CSCs (tenants). | Theme and Vulnerability Management Policy and Procedures |
| TVM-05.1 | Are security assessments and reviews performed? | Yes | CSP-owned | Through the use of established assessment procedures, CSPs periodically review agreements between CSPs and CSCs (tenants). | Theme and Vulnerability Management Policy and Procedures |
| TVM-06.1 | Are security assessments and reviews performed? | Yes | CSP-owned | Through the use of established assessment procedures, CSPs periodically review agreements between CSPs and CSCs (tenants). | Theme and Vulnerability Management Policy and Procedures |
| TVM-07.1 | Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly? | Yes | CSC-owned | InterSystems Managed Services perform regular vulnerability scans on the Catalyst solution environment for the InterSystems cloud infrastructure using a variety of tools. | TVM-07 | Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least annually. | Vulnerability Identification |
| --- | --- | --- | --- | --- | --- | --- |
| TVM-08 | Is vulnerability remediation prioritized using a risk-based model using an industry-recognized framework? | Yes | Shared CSP and 3rd-party | The InterSystems and the IaaS Provider's vulnerability remediation management program, policies, and procedures include managing applications, assets, software, and vulnerabilities, in accordance with ISO 27001 standards. | TVM-08 | Define, implement and prioritize vulnerability remediation using an industry recognized framework. | Vulnerability Prioritization |
| TVM-09 | Is system-defined and implemented on a risk and impact vulnerability identification and remediation process that includes vulnerability classifications? | Yes | Shared CSP and 3rd-party | The InterSystems and the IaaS Provider's vulnerability remediation management program, policies, and procedures include managing applications, assets, software, and vulnerabilities, in accordance with ISO 27001 standards. | TVM-09 | Define and implement a process for training and reporting vulnerability identification and remediation controls that include vulnerability classifications. | Vulnerability Management Reporting |
| TVM-10 | Are metrics for vulnerability identification and remediation established, maintained, and reported as defined locally? | Yes | Shared CSP and 3rd-party | The InterSystems and the IaaS Provider's vulnerability remediation management program, policies, and procedures include managing applications, assets, software, and vulnerabilities, in accordance with ISO 27001 standards. | TVM-10 | Establish, maintain and report metrics for vulnerability identification and remediation as defined in the assessment. | Vulnerability Management Planning |
| UEM-01.1 | Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints? | Yes | CSC-owned | Customer must be responsible for any end user access to endpoint inventory. | UEM-01 | Define, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. | Endpoint Device Policy and Procedures |
| UEM-02.1 | Are universal endpoint management policies and procedures reviewed and updated at least annually? | Yes | CSC-owned | Customer must be responsible for any end user access to endpoint inventory. | UEM-02 | Define, implement and update universal endpoint management policies and procedures reviewed and updated at least annually. | Enduser/Device Management |
| UEM-02.1.1 | Is there a defined and documented, applicable and evaluated process for overseeing approved applications, services, and the source of applications (stores) acceptable for organization endpoints when accessing or storing organization managed data? | Yes | CSC-owned | Customer must be responsible for any end user access to endpoint inventory. | UEM-02.1 | Define, implement and evaluate processes, procedures and technical measures for organization endpoints when accessing or storing organization managed data. | Enduser/Device Management |
| UEM-04.1.1 | Are changes to endpoint operating systems, patch levels, and/or applications managed through the organization's change management process? | Yes | CSC-owned | Customer solution. | UEM-04.1 | Manage changes to endpoint operating systems, patch levels, and/or applications through the organization's change management process. | Operating System |
| UEM-05.1 | Is there an inventory of all endpoints used and maintained on site and across company sites? | Yes | CSC-owned | Customer must be responsible for any end user access to endpoint inventory. | UEM-05 | Create an inventory of all endpoints used and maintained on site and across company sites. | Endpoint Inventory |
| UEM-07.1 | Are processes, procedures, and technical measures defined, implemented, and evaluated for unauthorized access to endpoint devices whether on site, transient, or present organization data? | Yes | CSC-owned | Customer must be responsible for any end user access to endpoint inventory. | UEM-07 | Define, implement and evaluate processes, procedures and technical measures for unauthorized access to endpoint devices. | Universal/Endpoint Management |
| UEM-08.1 | Are all remote management and reporting mechanisms configured or required to connect with the system? | Yes | CSC-owned | Customer must be responsible for any end user access to endpoint inventory. | UEM-08 | Configure all remote management and reporting mechanisms configured or required to connect with the system. | Universal/Endpoint Management |
| UEM-09.1 | Are changes in endpoint operating systems, patch levels, and/or applications managed through the organization's change management process? | Yes | CSC-owned | Customer must be responsible for any end user access to endpoint inventory. | UEM-09 | Manage changes in endpoint operating systems, patch levels, and/or applications through the organization's change management process. | Operating System |
| UEM-10.1 | Are there any unauthorized access to organization assets? | Yes | CSC-owned | Customer solution. | UEM-10 | Provide information from uncontrolled disclosure on managed endpoints accessed with storage encryption. | Storage Encryption |
| UEM-11.1 | Are software firewalls configured on managed endpoints? | Yes | CSC-owned | Customer must be responsible for any end user access to endpoint inventory. | UEM-11 | Configure managed endpoints with anti-malware detection and prevention technologies and services. | AntiMalware Detection and Prevention |
| UEM-12.1 | Are remote geolocation capabilities enabled for all managed mobile endpoints? | Yes | CSC-owned | Customer must be responsible for any end user access to endpoint inventory. | UEM-12 | Enable remote geolocation capabilities for all managed mobile endpoints. | Remote Location |
| UEM-13.1 | Are processes, procedures, and technical measures defined, implemented, and evaluated to securely monitor any security of third-party endpoints, with access to organization assets? | Yes | Distinct CSP and CSC | InterSystems and IaaS Provider maintain appropriate policies and procedures for third-party endpoint access. Customer must maintain appropriate policies and procedures for third-party endpoint access. | UEM-13 | Define, implement and evaluate universal, policies, procedures and technical measures to securely monitor any security of third-party endpoints, with access to organization assets. | Third Party Endpoint Security Policies |