<table>
<thead>
<tr>
<th>Control Domain</th>
<th>Control ID</th>
<th>Question ID</th>
<th>Control Specification</th>
<th>CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application &amp; Interface Security</td>
<td>XE-09</td>
<td>AAC-03.1</td>
<td>Applications and programming interfaces (APIs) shall be designed, developed, deployed, and maintained in accordance with leading industry standards (e.g., CDIAP for web applications) and subject to application legal, regulatory, or compliance obligations.</td>
<td>• Do you use industry standards (e.g. OWASP, Software Assurance Maturity Model, CAESARS) to build in security for your Systems/Software/Development/Maintenance (S3D)?&lt;br&gt;• Do you use an automated source code analysis tool to detect security defects in code prior to production?</td>
</tr>
<tr>
<td>Application &amp; Interface Security</td>
<td>XE-09</td>
<td>AAC-03.2</td>
<td>Do you conduct application penetration tests of your cloud applications, business partners, and third party service infrastructure at least annually?</td>
<td>• Does your Data Security Architecture designed using an industry standard (e.g., CSA, NIST/ANSI, CIAB) Cloud Security Architecture Standard, FedRAMP, CAIGA?</td>
</tr>
<tr>
<td>Application &amp; Interface Security</td>
<td>XE-09</td>
<td>AAC-04.1</td>
<td>Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent improper disclosure, alteration, or destruction.</td>
<td>• Are data input and output integrity routines (i.e., MD5/SHA hashes) to detect potential file corruption to be implemented?</td>
</tr>
<tr>
<td>Application &amp; Interface Security</td>
<td>XE-09</td>
<td>AAC-04.2</td>
<td>Are business continuity plans subject to testing at planned intervals or upon significant organizational or operational changes?</td>
<td>• Do your business continuity plans include the services you rely on?</td>
</tr>
<tr>
<td>Application &amp; Interface Security</td>
<td>XE-09</td>
<td>AAC-04.3</td>
<td>Prior to granting customers access to data, assets, and applications, business partners, and third party service infrastructure regularly as prescribed by industry best practices and guidance?</td>
<td>• Are business continuity plans subject to testing at planned intervals or upon significant organizational or operational changes?</td>
</tr>
<tr>
<td>Application &amp; Interface Security</td>
<td>XE-09</td>
<td>AAC-04.4</td>
<td>Do you review your applications for security vulnerabilities and any impact to data, processes, and procedures shall be established and maintained in support of data security to include confidentiality, integrity, and availability across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.</td>
<td>• Does your Data Security Architecture designed using an industry standard (e.g., CDIAP, NIST/ANSI, CIAB) Cloud Security Architecture Standard, FedRAMP, CAIGA?</td>
</tr>
<tr>
<td>Audit Assurance &amp; Compliance</td>
<td>XE-09</td>
<td>AAC-06.1</td>
<td>Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on ensuring the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.</td>
<td>• Does your audit program take into account effectiveness of implementation of security operations?</td>
</tr>
<tr>
<td>Audit Assurance &amp; Compliance</td>
<td>XE-09</td>
<td>AAC-06.2</td>
<td>Does your independent review and assessment include the evaluation of cloud service infrastructure regularly as prescribed by industry best practices and guidance?</td>
<td>• Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power, water, temperatures and humidity controls)?</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>XE-09</td>
<td>AAC-07.1</td>
<td>Organizations shall create and maintain a business continuity and disaster recovery plan (BCP) that includes the following: • Define purpose and scope, aligned with relevant regulations&lt;br&gt;• Applicable to and understood by those who will use the plan&lt;br&gt;• Owned by a named person who is responsible for their review, update, and approval&lt;br&gt;• Defined lines of communication, roles, and responsibilities&lt;br&gt;• Information system documentation (e.g., administrator)&lt;br&gt;• Physical protection against damage from natural causes&lt;br&gt;• To include risks from environmental hazards, hazards&lt;br&gt;• Policies and procedures shall be established, and&lt;br&gt;• Supporting business processes and contractual arrangements&lt;br&gt;• Information system documentation (e.g., administrator)&lt;br&gt;• Policies and procedures shall be established, and&lt;br&gt;• Supporting business processes and contractual arrangements</td>
<td>• Does your organization's business continuity and crisis management plans include the services you rely on?</td>
</tr>
</tbody>
</table>

---

**Notes:**
- **Yes/No/Not Applicable**
- **No** implies that there is no plan or process in place to mitigate the identified risk.
- **Not Applicable** implies that the risk is not applicable to the organization.
- **X** indicates that the control was not applicable or not applicable at the time of the assessment.
Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?

- [ ] Yes
- [ ] No

**Business Continuity**

**BCS-02**  
Do you have a capability to use system geographic location information to detect source code assets located at all sites or geographical locations and their applications to access corporate resources?

- [ ] Yes
- [ ] No

**Human Resources Management & Access Control**

**BCS-03**  
Do risk assessments associated with data governance and data management be conducted at planned intervals and include residual risk determined independently, considering all risk mitigation strategies?

- [ ] Yes
- [ ] No

**Security**

**BCS-04**  
Do you maintain key management procedures?

- [ ] Yes
- [ ] No

**IT Lifecycle Management & Change Control**

**BCS-05**  
Do you have processes in place to ensure production data changes in production environments are registered, test code elements are removed from released software, and changes in production environments are registered, test code elements are removed from released software?

- [ ] Yes
- [ ] No

**Risk Management & Compliance**

**BCS-06**  
Do executive and line management take formal action to ensure that all information security policies and procedure changes in production environments are registered, test code elements are removed from released software, and changes in production environments are registered, test code elements are removed from released software?

- [ ] Yes
- [ ] No
IAM-03.1 Do you regularly update network architecture diagrams?

MOS-14 Do you have a policy that requires BYOD users to use anti-virus software?

MOS-08 Do you use an industry-recognized virtualization platform?

MOS-12 Do you have the ability to logically segment or encrypt virtual machines?
Do you inspect and account for data quality errors?

Do legal counsel review all third-party agreements?

Do you have anti-malware programs that support or

Do you provide the client with a list and copies of all

Do you ensure that security threat detection systems using

Do you allow tenants to define acceptable geographical

Is mobile code authorized before its installation and use,

Do you conduct network-layer vulnerability scans regularly

Do you conduct application-layer vulnerability scans

Do you provide tenants with ongoing visibility and

Do third-party agreements include provision for the security

Do you provide tenants with ongoing visibility and reporting

Do you have the capability to restrict the storage of

Do you ensure that security threat detection systems over a trusted or untrusted network and executed

Do you inform customers (tenant) of policies and procedures

Do you inform customers (tenant) of policies and procedures

Do you review the risk management and governance

Does legal counsel review all third-party agreements?

Do you conduct network-layer vulnerability scans as prescribed by industry best practices?

Do you determine the level of security that your data is classified?

Do you allow tenants to define acceptable geographical

Do you provide customers with ongoing visibility and

Do you select and monitor outsourced providers to ensure that

Do you make standards-based information security metrics

Do you have the capability to restrict the storage of

Do you ensure that security threat detection systems

Do you have anti-malware programs that support or

Do you allow tenants to define acceptable geographical

Do you have the capability to restrict the storage of

Do you provide customers with ongoing visibility and

Do you conduct application-layer vulnerability scans

Do you allow tenants to define acceptable geographical

Do you provide customers with ongoing visibility and

Do you ensure that security threat detection systems

Do you protection against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or

Do you allow tenants to define acceptable geographical

Do you provide tenants with capacity planning and use

Do you protect against unauthorized disclosure or