CSA STAR

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers: Yes	No	Not Applicable	Notes
Application & Interface Security Application Security	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g. OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO-27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			Composition setting through OWASP and Attack Prevention
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			Security code review as a tool Static analysis
		AIS-01.3		Do you use manual source code analysis to detect security defects in code prior to production?	X			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			
Application & Interface Security Customer Access Requirements	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			
		AIS-02.2		Are all requirements and test results for customers' assets defined and documented?		X		
Application & Interface Security Data Integrity	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Does your data management policies and procedures require audits to verify data input and output integrity routines?		X		
		AIS-03.2		Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?		X		
Application & Interface Security Data Security / Integrity	AIS-04	AIS-04.1	Policies 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.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULTILAYR, Clip Trusted Cloud Architecture Standard, FedRAMP, CAESARS)?			X	
Audit Assurance & Compliance Audit Planning	AUD-01	AUD-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources, etc.) for reviewing the efficiency and effectiveness of implemented security controls?		X		Service/activities implemented by our Cloud Service Provider Microsoft Azure
		AUD-01.2		Does your audit program take into account effectiveness of implementation of security operations?		X		Service/activities implemented by our Cloud Service Provider Microsoft Azure
Audit Assurance & Compliance Independent Audits	AUD-02	AUD-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?		X		Service/activities implemented by our Cloud Service Provider Microsoft Azure
		AUD-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?		X		Service/activities implemented by our Cloud Service Provider Microsoft Azure
		AUD-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?		X		Service/activities implemented by our Cloud Service Provider Microsoft Azure
		AUD-02.4		Do you conduct internal audits at least annually?		X		Service/activities implemented by our Cloud Service Provider Microsoft Azure
		AUD-02.5		Do you conduct independent audits at least annually?		X		Service/activities implemented by our Cloud Service Provider Microsoft Azure
		AUD-02.6		Are the results of the penetration tests available to tenants at their request?		X		Service/activities implemented by our Cloud Service Provider Microsoft Azure
		AUD-02.7		Are the results of internal and external audits available to tenants at their request?		X		Service/activities implemented by our Cloud Service Provider Microsoft Azure
Audit Assurance & Compliance Information System Regulatory Mapping	AUD-03	AUD-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	BCR-01.1	A business continuity framework for business continuity planning and the management of operational resilience shall be established in ensure of business interruptions are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined roles, responsibilities, roles, and responsibilities • Detailed recovery procedures, manual work around, and reference information • Method for plan invocation	Does your organization have a plan or framework for business continuity management or disaster recovery management?		X		
		BCR-01.2		Do you have more than one provider for each critical service you depend on?		X		
		BCR-01.3		Do you provide a disaster recovery capability?	X			
		BCR-01.4		Do you monitor service continuity with upstream providers in the event of provider failure?	X			
		BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?		X		
		BCR-01.6		Do you provide a mean-time-to-service-recovery?		X		
		BCR-01.7		Do you share your business continuity and redundancy plans with your tenants?		X		
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subjected to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			
Business Continuity Management & Operational Resilience Power / Telecommunications	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continued effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed according to applicable laws or other redundancies in the event of planned or unplanned disruptions.	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?			X	Service/activities implemented by our Cloud Service Provider Microsoft Azure
		BCR-03.2		Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?		X		
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) shall be made available to authorized personnel to ensure configuration, installation and operation of the information system: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			
Business Continuity Management & Operational Resilience Equipment Location	BCR-05	BCR-05.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance	Is any of your data centers located in places that have a high probability/occurrence of high impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?			X	Service/activities implemented by our Cloud Service Provider Microsoft Azure
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-06	BCR-06.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	Do you have documentation, procedures and supporting business processes for equipment and datacenter maintenance?			X	Service/activities implemented by our Cloud Service Provider Microsoft Azure
		BCR-06.2		Do you have an equipment and datacenter maintenance routine or plan?			X	Service/activities implemented by our Cloud Service Provider Microsoft Azure
Business Continuity Management & Operational Resilience Impact Analysis	BCR-07	BCR-07.1	Configuration management shall be performed prior to hardware and man-made threats based upon a geographically specific business impact assessment.	Do you provide a configuration management plan (one time or term) for hardware and man-made threats based upon a geographically specific business impact assessment?			X	Service/activities implemented by our Cloud Service Provider Microsoft Azure
		BCR-07.2		Do security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc)?			X	Service/activities implemented by our Cloud Service Provider Microsoft Azure

| CCM v3.0.1 | | |

| | | |

| | | |

| | | |

| | | |

| | | |

| | | |