CAIQv3.1

CONSENSUS ASSESSMENTS
INITIATIVE QUESTIONNAIRE v3.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
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			
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			code quality tool su apposito docker
		AIS-01.3		Do you use manual source-code analysis to detect security	X			Merge request su GitLab
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development	X			
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment	X			
Application & Interface Security *Customer Access*	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	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed	X			
		AIS- 02.2		Are all requirements and trust levels for customers' access	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	X			
		AIS-03.2		Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and		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, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-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		
		AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?	X			
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-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			
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			VA/PT 2019
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			VA/PT 2019
		AAC-02.4		Do you conduct internal audits at least annually?	X			pianificazione controlli
		AAC-02.5		Do you conduct independent audits at least annually?	X			pianificazione controlli
		AAC-02.6		Are the results of the penetration tests available to tenants		X		documentazione tecnica
		AAC-02.7		Are the results of internal and external audits available to		X		documentazione tecnica
Audit Assurance &	AAC-03	AAC-03.1	Organizations shall create and maintain a control	Do you have a program in place that includes the ability to	X			
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans 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 lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			Service Provider
		BCR-01.2		Do you have more than one provider for each 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 tenant-triggered failover option?	X			
		BCR-01.7		Do you share your business continuity and redundancy plans with your tenants?		X		documentazione tecnica interna
Business Continuity	BCR-02	BCR-02.1	Business continuity and security incident response plans	Are business continuity plans subject to testing at planned	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 continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the	Does your organization adhere to any international or industry	X			Service Provider
		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	BCR-04	BCR-04.1	Information system documentation (e.g., administrator	Are information system documents (e.g., administrator and	X			solo a persone qualificate,
Business Continuity	BCR-05	BCR-05.1	Physical protection against damage from natural causes	Is physical damage anticipated and are countermeasures			X	IAAS
Business Continuity	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards,	Are any of your data centers located in places that have a		X		
Business Continuity Management &	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures	Do you have documented policies, procedures and supporting			X	IAAS
		BCR-07.2		Do you have an equipment and datacenter maintenance			X	IAAS
Business Continuity	BCR-08	BCR-08.1	Protection measures shall be put into place to react to	Are security mechanisms and redundancies implemented to			X	IAAS
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			In linea con quanto richiesto dai capitolati di gara

		BCR-09.2	providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?		X		
Business Continuity	BCR-10	BCR-10.1	Policies and procedures shall be established, and	Are policies and procedures established and made available	X			
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business	Do you have technical capabilities to enforce tenant data	X			
		BCR-11.2		Do you have documented policies and procedures		X		
		BCR-11.3		Have you implemented backup or recovery mechanisms to	X			
		BCR-11.4		If using virtual infrastructure, does your cloud solution	X			
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a	X			
		BCR-11.6		Does your cloud solution include software/provider	X			
		BCR-11.7		Do you test your backup or redundancy mechanisms at	X			Pianificazione dei controlli -
Change Control &	CCC-01	CCC-01.1	Policies and procedures shall be established, and	Are policies and procedures established for management	X			Processo di progettazione
Change Control & Configuration	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release,	Are policies and procedures for change management, release,	X			
		CCC-02.2		Are policies and procedures adequately enforced to ensure		X		Non esiste attualmente
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you have a defined quality change control and testing	X			
		CCC-03.2		Is documentation describing known issues with certain		X		
		CCC-03.3		Are there policies and procedures in place to triage and	X			Ticketing, Gitlab issue
		CCC-03.4		Do you have controls in place to ensure that standards of	X			Merge request, Hash della
		CCC-03.5		Do you have controls in place to detect source code	X			Merge request
		CCC-03.6		Are mechanisms in place to ensure that all debugging and	X			
Change Control &	CCC-04	CCC-04.1	Policies and procedures shall be established, and	Do you have controls in place to restrict and monitor the	X			Hash della release e relativo
Change Control & Configuration Management	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting	Do you provide tenants with documentation that describes		X		
		CCC-05.2		Do you have policies and procedures established for	X			Risk assessment 27001
		CCC-05.3		Do you have technical measures in place to ensure that	X			
Data Security & Information	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value,	Do you provide a capability to identify data and virtual	X			
		DSI-01.2		Do you provide a capability to identify data and hardware			X	
Data Security & Information	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures	Do you inventory, document, and maintain data flows for	X			
		DSI-02.2		Can you ensure that data does not migrate beyond a	X			
Data Security & Information	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified	Do you provide standardized (e.g. ISO/IEC) non-proprietary	X			protocollo https
		DSI-03.2		Do you utilize open encryption methodologies any time	X			VPN, HTTPS, autenticazione
Data Security & Information Lifecycle	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be	Are policies and procedures established for data labeling	X			ISO 27001
		DSI-04.2		Do you follow a structured data-labeling standard (e.g., ISO		X		
		DSI-04.3		Are mechanisms for label inheritance implemented for		X		
Data Security &	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-	Do you have procedures in place to ensure production data	X			ambienti separati previsti
Data Security &	DSI-06	DSI-06.1	All data shall be designated with stewardship, with	Are the responsibilities regarding data stewardship defined,	X			ISO 27001
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			
		DSI-07.2		Can you provide a published procedure for exiting the	X			ISO 27001, CAPITOLATI DI
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity	Do you classify your assets in terms of business criticality,			X	IAAS
		DCS-01.2		Do you maintain a complete inventory of all of your critical			X	IAAS
Datacenter Security	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers,	Are physical security perimeters (e.g., fences, walls, barriers,			X	IAAS
Datacenter Security *Equipment*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware	Do you have a capability to use system geographic location			X	IAAS
		DCS-03.2		Is automated equipment identification used as a method to			X	IAAS
Datacenter Security	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or	Is authorization obtained prior to relocation or transfer of			X	IAAS
Datacenter Security	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure	Can you provide tenants with your asset management			X	IAAS
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for	Can you provide evidence that policies, standards, and			X	IAAS
		DCS-06.2		Can you provide evidence that your personnel and involved			X	IAAS
Datacenter Security	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and	Are physical access control mechanisms (e.g. CCTV			X	IAAS
Datacenter Security	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other	Are ingress and egress points, such as service areas and			X	IAAS
Datacenter Security	DCS-09	DCS-09.1	Physical access to information assets and functions by	Do you restrict physical access to information assets and			X	IAAS
Encryption & Key	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to	Do you have key management policies binding keys to		X		
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and	Do you have a capability to allow creation of unique		X		
		EKM-02.2		Do you have a capability to manage encryption keys on		X		
		EKM-02.3		Do you maintain key management procedures?		X		
		EKM-02.4		Do you have documented ownership for each stage of the		X		
		EKM-02.5		Do you utilize any third party/open source/proprietary		X		
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for	Do you encrypt tenant data at rest (on disk/storage) within		X		
		EKM-03.2		Do you leverage encryption to protect data and virtual		X		
		EKM-03.3		Do you have documentation establishing and defining your		X		
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud	Do you have platform and data appropriate encryption that	X			
		EKM-04.2		Are your encryption keys maintained by the cloud		X		
		EKM-04.3		Do you store encryption keys in the cloud?	X			
		EKM-04.4		Do you have separate key management and key usage		X		
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that	Do you have documented information security baselines for	X			
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?		X		
Governance and Risk Management	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and	Does your organization's risk assessments take into account		X		
		GRM-02.2		Do you conduct risk assessments associated with data	X			
Governance and	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of,	Are your technical, business, and executive managers	X			
Governance and Risk Management	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and	Do you provide tenants with documentation describing		X		
		GRM-04.2		Do you review your Information Security Management	X			ISO 9001 E 27001
Governance and	GRM-05	GRM-05.1	Executive and line management shall take formal action to	Do executive and line management take formal action	X			
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable	Are your information security policies and procedures made	X			ISO 27001
		GRM-06.2		Are information security policies authorized by the	X			
		GRM-06.3		Do you have agreements to ensure your providers adhere	X			
		GRM-06.4		Can you provide evidence of due diligence mapping of your		X		
		GRM-06.5		Do you disclose which controls, standards, certifications,		X		
Governance and Risk Management	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and	Is a formal disciplinary or sanction policy established for		X		Informativa e gestione degli
		GRM-07.2		Are employees made aware of what actions could be taken	X			Informativa e gestione degli
Governance and	GRM-08	GRM-08.1	Risk assessment results shall include updates to security	Do risk assessment results include updates to security	X			
Governance and Risk Management	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the	Do you notify your tenants when you make material	X			
		GRM-09.2		Do you perform, at minimum, annual reviews to your	X			
Governance and Risk Management	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at	Are formal risk assessments aligned with the enterprise-	X			
		GRM-10.2		Is the likelihood and impact associated with inherent and	X			
Governance and Risk Management	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and	Do you have a documented, organization-wide program in	X			
		GRM-11.2		Do you make available documentation of your organization-		X		
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all	Upon termination of contract or business relationship, are	X			
		HRS-01.2		Do you have asset return procedures outlining how assets	X			
Human Resources	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual	Pursuant to local laws, regulations, ethics, and contractual	X			
Human Resources *Employment*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information	Do your employment agreements incorporate provisions and/or	X			
		HRS-03.2		Do you require that employment agreements are signed by	X			
Human Resources *Employment*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be	Are documented policies, procedures, and guidelines in	X			
		HRS-04.2		Do the above procedures and guidelines account for timely	X			
Human Resources	HRS-05	HRS-05.1	Policies and procedures shall be established, and	Are policies and procedures established and measures	X			
Human Resources	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality	Are requirements for non-disclosure or confidentiality	X			
Human Resources	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and	Do you provide tenants with a role definition document	X			
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures	Do you have policies and procedures in place to define		X		
		HRS-08.2		Do you define allowance and conditions for BYOD devices		X		
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating	Do you provide a formal, role-based, security awareness	X			FORMAZIONE
		HRS-09.2		Do you specifically train your employees regarding their	X			
		HRS-09.3		Do you document employee acknowledgment of training	X			
		HRS-09.4		Is successful and timed completion of the training	X			
		HRS-09.5		Are personnel trained and provided with awareness		X		
		HRS-09.6		Are administrators and data stewards properly educated on	X			
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established	Are personnel informed of their responsibilities for	X			
		HRS-10.2		Are personnel informed of their responsibilities for	X			
		HRS-10.3		Are personnel informed of their responsibilities for ensuring	X			
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on	Are all computers and laptops configured such that there is	X			
		HRS-11.2		Are there policies and procedures to ensure that	X			
Identity & Access Management	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately	Do you restrict, log, and monitor access to your information	X			
		IAM-01.2		Do you monitor and log privileged access (e.g.,	X			
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network	Do you have controls in place ensuring timely removal of	X			
		IAM-02.2		Do you have policies, procedures and technical measures in		X		
		IAM-02.3		Do you have procedures and technical measures in place	X			COMPETENZE
		IAM-02.4		Do you have procedures and technical measures in place	X			
		IAM-02.5		Do you enforce data access permissions based on the rules	X			
		IAM-02.6		Do your policies and procedures incorporate security	X			
		IAM-02.7		Do you provide metrics to track the speed with which you		X		

Identity & Access	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			
Identity & Access **Management**	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who	Do you manage and store the identity of all personnel who	X			COMPETENZE
		IAM-04.2		Do you manage and store the user identity of all personnel	X			COMPETENZE
Identity & Access	IAM-05	IAM-05.1	User access policies and procedures shall be established,	Do you provide tenants with documentation on how you		X		
Identity & Access **Management**	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of	Are controls in place to prevent unauthorized access to	X			
		IAM-06.2		Are controls in place to prevent unauthorized access to	X			
Identity & Access **Management** *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to	Does your organization conduct third-party unauthorized access risk assessments?	X			
		IAM-07.2		Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access?	X			
Identity & Access **Management** *User Access*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least	Do you document how you grant, approve and enforce	X			
		IAM-08.2		Based on the rules of least privilege, do you have policies	X			
		IAM-08.3		Do you limit identities' replication only to users explicitly	X			
Identity & Access **Management**	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier	Does your management provision the authorization and	X			
		IAM-09.2		Do you provide upon the request of users with legitimate	X			
Identity & Access **Management** *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to	Do you require a periodical authorization and validation	X			
		IAM-10.2		Do you collect evidence to demonstrate that the policy (see	X			gestione incidenti di
		IAM-10.3		follow user access policies?	X			
		IAM-10.4		Will you share user entitlement and remediation reports with	X			COMUNICAZIONE AL
Identity & Access **Management**	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed	Is timely deprovisioning, revocation, or modification of user	X			
		IAM-11.2		Is any change in user access status intended to include	X			
Identity & Access **Management** *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or	Do you support use of, or integration with, existing	X			
		IAM-12.2		Do you use open standards to delegate authentication	X			WS SOAP e REST
		IAM-12.3		Do you support identity federation standards (e.g., SAML,	X			IDENTITY PROVIDER IN
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g.,		X		
		IAM-12.5		Do you have an identity management system (enabling		X		
		IAM-12.6		Do you provide tenants with strong (multifactor)	X			TOKEN
		IAM-12.7		Do you allow tenants to use third-party identity assurance	X			LDAP, SSO AZIENDALI
		IAM-12.8		Do you support password (e.g., minimum length, age,	X			
		IAM-12.9		Do you allow tenants/customers to define password and	X			
		IAM-12.10		Do you support the ability to force password changes upon	X			
		IAM-12.11		Do you have mechanisms in place for unlocking accounts	X			
Identity & Access	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system,	Are access to utility programs used to manage virtualized	X			
Infrastructure & **Virtualization** **Security** *Audit Logging /* *Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network	Are file integrity (host) and network intrusion detection		X		
		IVS-01.2		Is physical and logical user access to audit logs restricted to	X			
		IVS-01.3		Can you provide evidence that due diligence mapping of		X		
		IVS-01.4		Are audit logs centrally stored and retained?	X			
		IVS-01.5		Are audit logs reviewed on a regular basis for security		X		
Infrastructure & **Virtualization** **Security**	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised	Do you log and alert any changes made to virtual machine		X		
		IVS-02.2		Does the virtual machine management infrastructure		X		
		IVS-02.3		Are changes made to virtual machines, or moving of an		X		
Infrastructure &	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source	Do you use a synchronized time-service protocol (e.g., NTP)	X			
Infrastructure & **Virtualization** **Security** *Capacity / Resource*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance	Do you provide documentation regarding what levels of			X	
		IVS-04.2		Do you restrict use of the memory oversubscription			X	
		IVS-04.3		Does your system's capacity requirements take into	X			
		IVS-04.4		Is system performance monitored and tuned in order to	X			SAR SUI SERVIZI (VM) E
Infrastructure &	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability	Do security vulnerability assessment tools or services			X	
Infrastructure & **Virtualization** **Security** *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and	For your IaaS offering, do you provide customers with			X	
		IVS-06.2		Do you regularly update network architecture diagrams			X	
		IVS-06.3		Do you regularly review for appropriateness the allowed			X	
		IVS-06.4		Are all firewall access control lists documented with			X	
Infrastructure &	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only	Are operating systems hardened to provide only the	X			
Infrastructure & **Virtualization** **Security**	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may	For your SaaS or PaaS offering, do you provide tenants with	X			
		IVS-08.2		For your IaaS offering, do you provide tenants with		X		
		IVS-08.3		Do you logically and physically segregate production and	X			
Infrastructure & **Virtualization** **Security** *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from	Are system and network environments protected by a	X			
		IVS-09.2		Are system and network environments protected by a firewall	X			
		IVS-09.3		Have you implemented the necessary measures for the	X			
		IVS-09.4		Do you have the ability to logically segment or encrypt	X			
		IVS-09.5		Are system and network environments protected by a	X			
Infrastructure & **Virtualization**	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data	Are secured and encrypted communication channels used	X			
		IVS-10.2		Do you use a network segregated from production-level	X			
Infrastructure &	IVS-11	IVS-11.1	Access to all hypervisor management functions or	Do you restrict personnel access to all hypervisor	X			
Infrastructure & **Virtualization** **Security**	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments,	Are policies and procedures established and mechanisms	X			
		IVS-12.2		Are policies and procedures established and mechanisms	X			
		IVS-12.3		Are policies and procedures established and mechanisms	X			
Infrastructure & **Virtualization**	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal	Do your network architecture diagrams clearly identify high-		X		
		IVS-13.2		Do you implement technical measures and apply defense-in-		X		
Interoperability &	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure	Do you publish a list of all APIs available in the service and	X			
Interoperability &	IPY-02	IPY-02.1	All structured and unstructured data shall be available to	Is unstructured customer data available on request in an	X			PDF, XLS, CSV
Interoperability & **Portability** *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application	Do you provide policies and procedures (i.e. service level	X			
		IPY-03.2		If using virtual infrastructure, do you allow virtual machine	X			
		IPY-03.3		Do you provide policies and procedures (i.e. service level	X			
Interoperability & **Portability**	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the	Is data import, data export, and service management be	X			
		IPY-04.2		Do you provide consumers (tenants) with documentation	X			
Interoperability & **Portability** *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented	Do you use an industry-recognized virtualization platform	X			
		IPY-05.2		If using virtual infrastructure, are machine images made		X		
		IPY-05.3		Do you have documented custom changes made to any	X			
Mobile Security	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile	Do you provide anti-malware training specific to mobile		X		
Mobile Security	MOS-02	MOS-02.1	A documented list of approved application stores has been	Do you document and make available lists of approved		X		
Mobile Security	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting	Do you have a policy enforcement capability (e.g., XACML)		X		
Mobile Security	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly	Does your BYOD policy and training clearly state which		X		
Mobile Security	MOS-05	MOS-05.1	The provider shall have a documented mobile device	Do you have a documented mobile device policy in your		X		
Mobile Security	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile	Do you have a documented list of pre-approved cloud		X		
Mobile Security	MOS-07	MOS-07.1	The company shall have a documented application	Do you have a documented application validation process		X		
Mobile Security	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility	Do you have a BYOD policy that defines the device(s) and		X		
Mobile Security	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access	Do you maintain an inventory of all mobile devices storing		X		
Mobile Security	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be	Do you have a centralized mobile device management		X		
Mobile Security	MOS-11	MOS-11.1	The mobile device policy shall require the use of	Does your mobile device policy require the use of	X			CRITTOGRAFATO
Mobile Security *Jailbreaking and*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g.,	Does your mobile device policy prohibit the circumvention		X		
		MOS-12.2		Do you have detective and preventative controls on the		X		
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-	Does your BYOD policy clearly define the expectation of		X		
		MOS-13.2		Does the BYOD policy clearly state the expectations over the		X		
Mobile Security	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to	Do you require and enforce via technical controls an	X			
Mobile Security	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels,	Do you manage all changes to mobile device operating	X			
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage,	Do you have password policies for enterprise issued mobile		X		
		MOS-16.2		Are your password policies enforced through technical		X		
		MOS-16.3		Do your password policies prohibit the changing of		X		
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-	Do you have a policy that requires BYOD users to perform		X		
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit		X		
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-		X		
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall	Does your IT provide remote wipe or corporate data wipe		X		
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe		X		
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for	Do your mobile devices have the latest available security-	X			
		MOS-19.2		Do your mobile devices allow for remote validation to		X		
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers		X		
		MOS-20.2		Does your BYOD policy specify the user roles that are		X		
Security Incident	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities,	Do you maintain liaisons and points of contact with local		X		
Security Incident **Management, E-** **Discovery, & Cloud** **Forensics**	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per	Do you have a documented security incident response plan?	X			
		SEF-02.2		Do you integrate customized tenant requirements into your		X		
		SEF-02.3		Do you publish a roles and responsibilities document		X		
		SEF-02.4		Have you tested your security incident response plans in the		X		
Security Incident **Management, E-** **Discovery, & Cloud** **Forensics** *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner	Are workforce personnel and external business relationships	X			
		SEF-03.2		Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			
Security Incident **Management, E-** **Discovery, & Cloud** **Forensics**	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification,	Does your incident response plan comply with industry		X		
		SEF-04.2		Does your incident response capability include the use of		X		
		SEF-04.3		Are you capable of supporting litigation holds (freeze of	X			
		SEF-04.4		Do you enforce and attest to tenant data separation when	X			
Security Incident **Management, E-**	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security	Do you monitor and quantify the types, volumes, and	X			
		SEF-05.2		Will you share statistical information for security incident	X			

Supply Chain Management,	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors	Do you inspect and account for data quality errors and		X		
		STA-01.2		Do you design and implement controls to mitigate and	X			
Supply Chain	STA-02	STA-02.1	The provider shall make security incident information	Do you make security incident information available to all	X			
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance	Do you collect capacity and use data for all relevant		X		
		STA-03.2		Do you provide tenants with capacity planning and use reports?		X		
Supply Chain	STA-04	STA-04.1	The provider shall perform annual internal assessments of	Do you perform annual internal assessments of	X			
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations)	Do you select and monitor outsourced providers in			X	
		STA-05.2		they are in compliance with applicable legislation?			X	
		STA-05.3		Does legal counsel review all third-party agreements?	X			
		STA-05.4		Do third-party agreements include provision for the security	X			IAAS
		STA-05.5		Do you have the capability to recover data for a specific		X		
		STA-05.6		Do you have the capability to restrict the storage of		X		
		STA-05.7		Can you provide the physical location/geography of storage		X		
		STA-05.8		Can you provide the physical location/geography of storage		X		
		STA-05.9		Do you allow tenants to define acceptable geographical		X		
		STA-05.10		Are systems in place to monitor for privacy breaches and		X		
		STA-05.11		Do you allow tenants to opt out of having their		X		
		STA-05.12		Do you provide the client with a list and copies of all		X		
Supply Chain	STA-06	STA-06.1	Providers shall review the risk management and	Do you review the risk management and governance	X			
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier	Are policies and procedures established, and supporting	X			
		STA-07.2		Do you have the ability to measure and address non-	X			
		STA-07.3		Can you manage service-level conflicts or inconsistencies	X			
		STA-07.4		Do you provide tenants with ongoing visibility and reporting	X			
		STA-07.5		Do you make standards-based information security metrics		X		
		STA-07.6		Do you provide customers with ongoing visibility and		X		
		STA-07.7		Do your data management policies and procedures address		X		
		STA-07.8		Do you review all service level agreements at least annually?	X			ISO 9001/27001
Supply Chain Management,	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an	Do you assure reasonable information security across your	X			
		STA-08.2		Does your annual review include all partners/third-party	X			
Supply Chain Management,	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality,	Do you mandate annual information security reviews and		X		
		STA-09.2		Do you have external third party services conduct		X		
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems	Do you have anti-malware programs that support or	X			
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X			
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies	Do you conduct network-layer vulnerability scans regularly	X			
		TVM-02.2		Do you conduct application-layer vulnerability scans	X			
		TVM-02.3		Do you conduct local operating system-layer vulnerability	X			
		TVM-02.4		Will you make the results of vulnerability scans available to		X		
		TVM-02.5		Do you have a capability to patch vulnerabilities across all of	X			
		TVM-02.6		Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	X			
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed	Is mobile code authorized before its installation and use,			X	
		TVM-03.2		Is all unauthorized mobile code prevented from executing?			X	