

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes		
					Yes	No	Not Applicable			
Application & Interface Security <i>Application Security</i>	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 (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your <u>Systems/Software Development Lifecycle (SDLC)</u> ?		X		Modus sviluppa tenendo presenti le best practice di settore. Durante lo sviluppo effettua regolarmente test di sicurezza sulla base dei 10 top rischi come definiti da <u>OWASP (Open Web Application Security Project) top ten</u>		
		AIS-01.2		Do you use an automated source code analysis tool to detect <u>security defects in code prior to production</u> ?		X				
		AIS-01.3		Do you use manual source-code analysis to detect security defects <u>in code prior to production</u> ?	X				Usiamo gli strumenti integrati in Visual Studio (ambiente di sviluppo Microsoft)	
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) <u>security</u> ?	X					Il fornitore principale di SW utilizzato da Modus + Microsoft, azienda certificata ISO 27001 e in molti altri <u>standard di settore</u>
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to <u>production</u> ?	X					
Application & Interface Security <i>Customer Access Requirements</i>	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 <u>shall be addressed</u> .	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and <u>information systems</u> ?	X			I clienti Modus possono accedere solo alle funzionalità dell'applicazione e l'applicazione stessa controlla le modalità di accesso. Il sistema soddisfa il GDPR. I profili di accesso sono definiti nella guida <u>dell'applicazione</u>		
		AIS-02.2		Are all requirements and trust levels for customers' access defined and <u>documented</u> ?	X					
Application & Interface Security <i>Data Integrity</i>	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	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			I dati inseriti dall'utente sono verificati prima del caricamento. Tutte le modifiche effettuate dagli utenti sono tracciate (con valore precedente, data e autore)		
Application & Interface Security <i>Data Security / Integrity</i>	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	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULTISAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			Microsoft controlla ogni aggiornamento del SW di infrastruttura contro modifiche non autorizzate e non coerenti con la propria SDL (Security Development Lifecycle). Inoltre vengono eseguiti controlli automatici di integrità ogni ora sulla infrastruttura per verificare l'assenza di anomalie e di modifiche non autorizzate.		

Audit Assurance & Compliance <i>Audit Planning</i>	AAC-01	Microsoft's cloud infrastructure, including ISO/IEC 27001:2013 certification, SSAE 16/ISAE 3402 SOC 1 Type 1 and Type 2 and AT Section 101 SOC 2 and 3 Type 1 and Type 2 attestations, as well as FedRAMP Certification and	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 produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?		X		L'infrastruttura Azure di Microsoft ha ottenuto svariate certificazioni: ISO/IEC 27001:2013, SSAE 16/ISAE 3402 SOC 1 Tipo 1 e Tipo 2, AT Section 101 SOC 2 e 3, Tipo 1 and Tipo 2, FedRAMP. Tutte questi standard prevedono un audit da parte dei certificatori.
Audit Assurance & Compliance <i>Independent Audits</i>	AAC-02	AAC-02.1 AAC-02.2 AAC-02.3 AAC-02.4 AAC-02.5 AAC-02.6	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? Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance? Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance? Do you conduct internal audits regularly as prescribed by industry best practices and guidance? Do you conduct external audits regularly as prescribed by industry best practices and guidance? Are the results of the penetration tests available to tenants at their request?	X X X X	 X	 X	I report sono disponibili nel trust center di Microsoft ed eventualmente possono essere integrati da maggiori informazioni previo accordo di confidenzialità. Microsoft esegue ogni trimestre test di penetrazione; in caso di problemi la fix viene applicata e nuovamente sottoposta al test. Microsoft esegue test di penetrazione basati su quanto indicato in NIST SP800-115, ETSI, OWASP, IETF e ISO 27000 e inoltre fornisce un sistema di protezione contro gli attacchi di tipo DoS (denial of Service). Modus esegue regolarmente test di penetrazione applicativa basati sui cicli identificati da OWASP. Modus, quali piccola impresa, non dispone di una funzione dedicata all'audit, le attività di audit vengono svolte in modo incrociato dai team di lavoro. Microsoft ha una funzione di audit interna. Microsoft è sottoposta agli audit dei certificatori dei vari standard che supporta. Per dettagli visitare il Microsoft Azure Trust Center. E' richiesto un accordo di confidenzialità

		AAC-02.7		Are the results of internal and external audits available to tenants at their request?			X	Microsoft pubblica i risultati degli audit estermi sul proprio Trust Center. Modus richiede un accordo di confidenzialità .
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?			X	Vedi punto AAC-02.4
Audit Assurance & Compliance <i>Information System Regulatory Mapping</i>	AAC-03	AAC-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 the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			I dati sono segmentati in modo tale che ogni tenant dell'applicazione ProcessFrame possa solo accedere alla propria porzione di dati. Microsoft garantisce che il contesto in cui opera ProcessFrame non sia accessibile da utenti di applicazioni diverse da ProcessFrame
		AAC-03.2		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			I dati sono backuppati giornalmente su strutture di storage ridondate
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			Tutta l'infrastruttura e i dati usati da Modus sono all'interno della UE
		AAC-03.4		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			Modus segue le normative Italiane e della UE
Business Continuity Management & Operational Resilience <i>Business Continuity Planning</i>	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	Do you provide tenants with geographically resilient hosting options?	X			E' possibile replicare l'applicazione e i dati su infrastrutture Azure di Microsoft in regioni diverse, pur rimandando sempre all'interno della UE
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?			X	La possibile di replicare in siti Microsoft geograficamente distinti ma comunque all'interno della UE, rende superflua questa funzionalità
Business Continuity Management & Operational Resilience <i>Business Continuity Testing</i>	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject 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	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Microsoft esegue test regolari del proprio piano di continuità.
Business Continuity Management & Operational Resilience <i>Power /</i>	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls)	Do you provide tenants with documentation showing the transport route of their data between your systems?			X	
		BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?			X	
Business Continuity Management & Operational Resilience <i>Documentation</i>	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: <ul style="list-style-type: none"> Configuring, installing, and operating the information system Effectively using the system's 	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	L'applicazione è utilizzata come servizio: configurazioni e operazioni gestionali sul sistema sono a carico di Modus Consulting. Tutte le operazioni che possono essere svolte dal utilizzatori, sia in termini funzionali che di configurazione, sono documentate dal manuale utente messo a disposizione degli utenti stessi.

Business Continuity Management & Operational Resilience <i>Environmental Risks</i>	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunamis, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	X			L'infrastruttura è distribuita su più sedi fisiche, operativa 24x7x365 e utilizza numerose misure per prevenire interruzioni di alimentazione, intrusioni fisiche e interruzioni della connettività. Tali misure sono certificate secondo lo standard ISO 27001.
Business Continuity Management & Operational Resilience <i>Equipment Location</i>	BCR-06	BCR-06.1	Vedd	Are 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		Vedi distribuzione geografica dei siti Microsoft. I siti sono comunque in Europa, in zone sicure rispetto a terremoti e alluvioni, e dotati di meccanismi di protezione contro incendi e altre calamità naturali
Business Continuity Management & Operational Resilience <i>Equipment Maintenance</i>	BCR-07	BCR-07.1	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.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			Lo storage è replicato localmente e su richiesta può essere replicato in località geograficamente distinte
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?			X	Possiamo riportare i dati del cliente indietro utilizzando i backup conservati. La estensione della durata della conservazione può essere concordata contrattualmente
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?			X	Possiamo migrare l'applicazione e i relativi dati sulla infrastruttura di un altro provider.
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?			X	Possiamo migrare l'applicazione e i relativi dati sulla infrastruttura on premise del cliente.
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?			X	La gestione dei backup è in carico a Modus Consulting, a meno di non concordare una diversa modalità
Business Continuity Management & Operational Resilience <i>Equipment Power Failures</i>	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			Le misure sono a carico di Microsoft: vedi la loro documentazione in materia
Business Continuity Management & Operational Resilience <i>Impact Analysis</i>	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:	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			Informazioni disponibili su richiesta
		BCR-09.2		Do you make standards-based information security metrics (CSA, CMM, etc.) available to your tenants?			X	
		BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			Informazioni disponibili su richiesta

Business Continuity Management & Operational Resilience Policy	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include <u>defined roles and responsibilities</u>	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			Il personale Modus è informato e aggiornato sui termini contrattuali e SLA definiti per ciascun cliente
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	Do you have technical control capabilities to enforce tenant data retention policies?	X			
		BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	X			
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			Quanto verrà garantito ai clienti sia in termini di frequenze di backup, numero e tempi di conservazione delle copie, ridondanza dei dati è esposto in tutti i contratti ed implicano in rispetto delle normative o condizioni più stringenti negoziate con il singolo cliente
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	X			
Change Control & Configuration Management New Development / Acquisition	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			
		CCC-01.2		Is documentation available that describes the installation, configuration, and use of products/services/features?	X			La documentazione tecnica è disponibile e prevalentemente ad uso interno, il manuale d'uso è disponibile per i clienti per ogni prodotto/servizio forniti
Change Control & Configuration Management Outsourced	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as	Do you have controls in place to ensure that standards of quality are being met for all software development?			X	non facciamo outsourcing di sviluppo
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?			X	non facciamo outsourcing di sviluppo
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 provide your tenants with documentation that describes your quality assurance process?		X		
		CCC-03.2		Is documentation describing known issues with certain products/services available?	X			i problemi funzionali noti sono documentati.
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			gli errori sono tracciati sul sistema Azur DevOps e le fix sono applicate su base mensile (i casi critici appena disponibili)
		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			

Change Control & Configuration Management <i>Unauthorized Software Installations</i>	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			L'accesso alla infrastruttura è limitato a persone autorizzate all'interno della sola Modus Consulting.
Change Control & Configuration Management <i>Production Changes</i>	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: <ul style="list-style-type: none"> • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	X			Le variazioni alla infrastruttura sono comunicate in anticipo ai clienti. Le fix applicate sono documentate ai clienti tramite release notes.
Data Security & Information Lifecycle Management <i>Classification</i>	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the <i>wrong country</i>)?			X	i clienti accedono al servizio, non conoscono la macchina
DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			X				
DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?			X				
DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	X			i dati sono all'interno della UE			
DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	X			i dati sono all'interno della UE			
DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?			X				
DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?				i dati sono all'interno della UE			
Data Security & Information Lifecycle Management	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?			X	i dati sono all'interno della UE

Data Inventory / Flows		DSI-02.2	measures implemented, to inventory, document, and maintain	Can you ensure that data does not migrate beyond a defined geographical residency?	X			i dati sono all'interno della UE
Data Security & Information Lifecycle Management E-commerce Transactions	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			Gli utenti accedono in HTTPS utilizzando TLS 1.2 con chiave a 256-bit.
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?		X		
Data Security & Information Lifecycle Management Handling / Labeling /	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?			X	
		DSI-04.2	which contain data. Mechanisms for	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	
Data Security & Information Lifecycle Management Nonproduction Data	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			Eeventuali repliche parziali a fini di test o demo sono anonimizzate
Data Security & Information Lifecycle Management Ownership / Stewardship	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
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	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Datacenter Security Asset Management	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	X			
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	X			
Datacenter Security Controlled Access Points	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?			X	Si, parte delle procedure di sicurezza implementate da Microsoft

Datacenter Security <i>Equipment Identification</i>	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	Y			Qualora richiesto, si può controllare l'accesso da parte di sistemi esterni utilizzando certificati per l'autenticazione
Datacenter Security <i>Offsite Authorization</i>	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, replication)?			X	
Datacenter Security <i>Offsite Equipment</i>	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?			X	
Datacenter Security <i>Policy</i>	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			Microsoft rende disponibili le sue procedure di sicurezza
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			Microsoft rende disponibili le sue procedure di sicurezza
Datacenter Security <i>Secure Area Authorization</i>	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?			X	Modus Consulting utilizza sono risorse Azure all'interno della UE
Datacenter Security <i>Unauthorized Persons Entry</i>	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption,	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)

Datacenter Security <i>User Access</i>	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Encryption & Key Management <i>Entitlement</i>	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management	Do you have key management policies binding keys to identifiable owners?	X			Le chiavi sono gestite da Microsoft con le sue procedure (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Encryption & Key Management <i>Key Generation</i>	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 algorithms used, access controls in	Do you have a capability to allow creation of unique encryption keys per tenant?		X		
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?			X	La crittografia dei dati è centralizzata a livello servizio e non per singolo tenant
		EKM-02.3		Do you maintain key management procedures?	X			Le chiavi sono gestite da Microsoft con le sue procedure (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			Le chiavi sono gestite da Microsoft con le sue procedure (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?		X		Le chiavi sono gestite da Microsoft con le sue procedure (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Encryption & Key Management <i>Encryption</i>	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 protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			L'applicazione usa lo storage della piattaforma Azure con i servizi Premium che gestisce l'encryption
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			E' utilizzato il protocollo HTTPS
		EKM-03.3		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?		X		
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			In generale la crittografia è gestita da Microsoft, che ha le sue procedure
Encryption & Key Management <i>Storage and Access</i>	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	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?				Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?				Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		EKM-04.3		Do you store encryption keys in the cloud?				Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		EKM-04.4		Do you have separate key management and key usage duties?				Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Governance and Risk Management <i>Baseline Requirements</i>	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 comply with applicable legal, statutory, and regulatory	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?				Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			tramite il security center di Azure
		GRM-01.3		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?			X	l'applicazione è fornita come servizio
Governance and Risk Management <i>Risk Assessments</i>	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?		X		
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X			

Governance and Risk Management <i>Management Oversight</i>	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			
Governance and Risk Management <i>Management Program</i>	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you provide tenants with documentation describing your Information Security Management Program (ISMP) ?	X			può essere fornita la relativa documentazione Microsoft
		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year ?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Governance and Risk Management <i>Management Support / Involvement</i>	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Governance and Risk Management <i>Policy</i>	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	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.) ?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies ?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards ?				Microsoft pubblica questi dati sul proprio Trust Center
		GRM-06.4		Do you disclose which controls, standards, certifications, and/or regulations you comply with ?	X			Microsoft pubblica questi dati sul proprio Trust Center
Governance and Risk Management <i>Policy Enforcement</i>	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			Il personale Modus è formato in merito alla sicurezza dei dati ed è consapevole delle conseguenze disciplinari nei confronti di chi le viola.
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			Il personale Modus è formato in merito alla sicurezza dei dati ed è consapevole delle conseguenze disciplinari nei confronti di chi le viola.
Governance and Risk Management <i>Business / Policy Change Impacts</i>	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective .	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			
Governance and Risk Management <i>Policy Reviews</i>	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security	Do you notify your tenants when you make material changes to your information security and/or privacy policies ?	X			
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies ?	X			
Governance and Risk Management <i>Assessments</i>	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all risks using qualitative and quantitative methods ?	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks using qualitative and quantitative methods ?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Governance and Risk Management	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels	Do you have a documented, organization-wide program in place to manage risk ?				Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)

Program		GRM-11.2	based on risk criteria shall be established and documented in	Do you make available documentation of your organization-wide risk management program?				Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Human Resources Asset Returns	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X			Gestito sia da Microsoft che da Modus
Human Resources Background Screening	HRS-02	HRS-01.2	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and	Is your Privacy Policy aligned with industry standards?	X			
		HRS-02.1		Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			
Human Resources Employment Agreements	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			
		HRS-03.2		Do you document employee acknowledgment of training they have completed?		X		
		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	X			Parte del contratto standard di lavoro
		HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	X			su base continuativa
Human Resources Employment Termination	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 place to govern change in employment and/or termination?	X			
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			
Human Resources Portable / Mobile Devices	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			i dati gestiti dalle applicazioni offerte in SaaS sono accessibili solo da desktop in sede

Human Resources <i>Non-Disclosure Agreements</i>	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?			X	
Human Resources <i>Roles / Responsibilities</i>	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			
Human Resources <i>Acceptable Use</i>	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned information technology resources.	Do you provide documentation regarding how you may access tenant data and metadata?	X			su richiesta
		HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)?		X		
		HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		X		
Human Resources <i>Training / Awareness</i>	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 information technology resources shall be required to complete the training.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?			X	
		HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			
Human Resources <i>User Responsibility</i>	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, regulatory, and contractual requirements.	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?			X	
		HRS-10.2		Are users made aware of their responsibilities for maintaining a safe and secure working environment?	X			
		HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	X			
Human Resources <i>Workspace</i>	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Do your data management policies and procedures address tenant and service level conflicts of interests?	X			
		HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	X			
		HRS-11.3		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Identity & Access Management <i>Audit Tools Access</i>	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise of the information systems.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			
Identity & Access Management <i>User Access Policy</i>	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 and access management.	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			
		IAM-02.2		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	X			

Identity & Access Management <i>Diagnostic / Configuration Ports Access</i>	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	X			utilizzo di VPN con MFA
Identity & Access Management <i>Policies and Procedures</i>	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			
Identity & Access Management <i>Segregation of Duties</i>	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?			X	
Identity & Access Management <i>Source Code Access Restriction</i>	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			
Identity & Access Management <i>Third Party Access</i>	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 minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall	Do you provide multi-failure disaster recovery capability?	X			funzionalità proposta come opzionale ai cliente ed attivabili grazie all'infrastruttura Azure
		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		IAM-07.3		Do you have more than one provider for each service you depend on?	X			L'applicazione è dipendente dall'infrastruttura Azure, che a sua volta utilizza strutture e provider ridondanti
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?				funzionalità opzionale basata su opzioni dell'infrastruttura Azure
		IAM-07.6		Do you provide a tenant-triggered failover option?		X		
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?			X	
Identity & Access Management <i>User Access Restriction / Authorization</i>	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities	Do you document how you grant and approve access to tenant data?	X			
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?		X		
Identity & Access Management <i>User Access Authorization</i>	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			

		IAM-09.2	(physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and	Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X				
Identity & Access Management <i>User Access Reviews</i>	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 at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	X				
		IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	X				
		IAM-10.3		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	X				
Identity & Access Management <i>User Access Revocation</i>	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X				
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X				
Identity & Access Management <i>User ID Credentials</i>	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:	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			Supporto nativo con SSO di Office 365, altre integrazioni su richiesta	
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	X			Su richiesta	
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?				Su richiesta	
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		X			
		IAM-12.5		• Identity trust verification and service-to-service application (API) and information processing	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X			
		IAM-12.6		interoperability (e.g., SSO and Federation)	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			Su richiesta
		IAM-12.7		• Account credential lifecycle management from instantiation through revocation	Do you allow tenants to use third-party identity assurance services?	X			Su richiesta
		IAM-12.8		• Account credential and/or identity store minimization or re-use when feasible	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X			Supporto standard
		IAM-12.9		• Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you allow tenants/customers to define password and account lockout policies for their accounts?		X		In linea di principio no. Nel caso un cliente lo chiedesse formalmente sarebbe possibile gestirlo in modo personalizzato
		IAM-12.10			Do you support the ability to force password changes upon first login?	X			
IAM-12.11			Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X					

Identity & Access Management <i>Utility Programs Access</i>	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored ?			X	
		IAM-13.2		Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	X			in carico a Microsoft: evidenziato nel Security Center di Azure
		IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls ?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Infrastructure & Virtualization Security <i>Audit Logging / Intrusion Detection</i>	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 behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents ?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel ?	X			
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done ?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		IVS-01.4		Are audit logs centrally stored and retained?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Infrastructure & Virtualization Security <i>Change Detection</i>	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 regardless of their running state	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running) ?			X	
		IVS-02.2		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?			X	
Infrastructure & Virtualization Security <i>Clock Synchronization</i>	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			
Infrastructure & Virtualization Security <i>Capacity / Resource Planning</i>	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 obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios ?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor ?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		IVS-04.3		Do your system capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants ?	X			Controlliamo periodicamente il profilo di utilizzo delle risorse e anticipiamo piani di crescita dell'utilizzo da parte dei clienti
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants ?	X			
Infrastructure & Virtualization Security <i>Management - Vulnerability Management</i>	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware)	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)

Infrastructure & Virtualization Security <i>Network Security</i>	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 supported by a documented justification for use for all allowed services, protocols,	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using <u>your virtualized solution</u> ?			X	
		IVS-06.2		Do you regularly update network architecture diagrams that include <u>data flows between security domains/zones</u> ?	X			
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security <u>domains/zones within the network</u> ?	X			
		IVS-06.4		Are all firewall access control lists documented with business <u>justification</u> ?	X			
Infrastructure & Virtualization Security <i>OS Hardening and Base Controls</i>	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			
Infrastructure & Virtualization Security <i>Production / Non-Production Environments</i>	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 include <u>stateful inspection firewalls</u> .	For your SaaS or PaaS offering, do you provide tenants with <u>separate environments for production and test processes</u> ?	X			su richiesta
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on <u>how to create suitable production and test environments</u> ?			X	
		IVS-08.3		Do you logically and physically segregate production and non- <u>production environments</u> ?	X			
Infrastructure & Virtualization Security <i>Segmentation</i>	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 other tenant users, based on the following considerations:	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security <u>requirements</u> ?	X			utilizziamo il WAF di Azure
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, <u>and contractual requirements</u> ?	X			utilizziamo il WAF di Azure
		IVS-09.3		Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non- <u>production environments</u> ?	X			
		IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive <u>data</u> ?	X			
Infrastructure & Virtualization Security <i>VM Security - Data Protection</i>	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to <u>virtualized servers and where</u>	Are secured and encrypted communication channels used when <u>migrating physical servers, applications, or data to virtual servers</u> ?	X			utilizzo di TLS
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual <u>servers</u> ?			X	

Infrastructure & Virtualization Security <i>VMM Security - Hypervisor Hardening</i>	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			
Infrastructure & Virtualization Security <i>Wireless Security</i>	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	
		IVS-12.2	• Perimeter firewalls implemented and configured to restrict unauthorized traffic	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X	
		IVS-12.3	• Security settings enabled with strong encryption for authentication and transmission, replacing vendor	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			X	
Infrastructure & Virtualization Security <i>Network Architecture</i>	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?			X	
		IVS-13.2	Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial of service (DDoS) attacks?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Interoperability & Portability <i>APIs</i>	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migration applications	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			Il sistema include due web services SOAP per inserire dati e documenti e cercarli/estrarli. Entrambi sono configurabili su misura per ogni tenant.
Interoperability & Portability <i>Data Request</i>	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., doc, xls, pdf, logs, and flat files)	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			i dati strutturati possono essere esportati in formati csv e xlsx direttamente dall'utente. I documenti (file di qualsiasi formato) caricati sul sistema possono essere estratti con i relativi metadati.
Interoperability & Portability <i>Policy & Legal</i>	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 (API	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	X			
		IPY-03.2	and information processing	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X			

Interoperability & Portability <i>Standardized Network Protocols</i>	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), <u>industry accepted standardized network protocols</u> ?	X			Https e autenticazione SOAP
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			
Interoperability & Portability <i>Virtualization</i>	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 custom changes made	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?			X	
		IPY-05.2		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			X	
Mobile Security <i>Anti-Malware</i>	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			X	L'applicazione può essere utilizzata da utenti tramite browser residente su device mobile. La sicurezza del device è in carico al cliente.
Mobile Security <i>Application Stores</i>	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			X	
Mobile Security <i>Approved Applications</i>	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			X	
Mobile Security <i>Approved Software for BYOD</i>	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			x	
Mobile Security <i>Awareness and Training</i>	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			X	
Mobile Security <i>Cloud Based Services</i>	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			x	

Mobile Security <i>Compatibility</i>	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			X	
Mobile Security <i>Device Eligibility</i>	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			X	
Mobile Security <i>Device Inventory</i>	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			X	
Mobile Security <i>Device Management</i>	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			X	
Mobile Security <i>Encryption</i>	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technical controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			X	
Mobile Security <i>Jailbreaking and Rooting</i>	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			X	
		MOS-12.2	and is enforced through detective and preventative controls on the	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			X	
Mobile Security <i>Legal</i>	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	
		MOS-13.2	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			X	
Mobile Security <i>Lockout Screen</i>	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	

Mobile Security <i>Operating Systems</i>	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			X	
Mobile Security <i>Passwords</i>	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 and shall prohibit the	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			X	
		MOS-16.2	technical controls on all company devices or devices approved for BYOD usage and shall prohibit the	Are your password policies enforced through technical controls (i.e. MDM)?			X	
		MOS-16.3	technical controls on all company devices or devices approved for BYOD usage and shall prohibit the	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X	
Mobile Security <i>Policy</i>	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-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	
		MOS-17.2	backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	
		MOS-17.3	backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X	
Mobile Security <i>Remote Wipe</i>	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	
		MOS-18.2	program or a company-assigned mobile device shall allow for remote	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			X	
Mobile Security <i>Security Patches</i>	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			X	
		MOS-19.2	version/patch validation. All mobile	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X	
Mobile Security <i>Users</i>	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 allowed for use or access on the BYOD-enabled device?			X	
		MOS-20.2	systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	
Security Incident <i>Management, E-Discovery, & Cloud Forensics</i> <i>Contact / Authority Maintenance</i>	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			
		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	Do you have a documented security incident response plan?	X			
		SEF-02.2	established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident	Do you integrate customized tenant requirements into your security incident response plans?		X		
Security Incident <i>Management, E-Discovery, & Cloud Forensics</i> <i>Incident Management</i>		SEF-02.3	established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		X		

		SEF-02.4	timely and thorough incident management, as per established IT	Have you tested your security incident response plans in the last year?	X				
Security Incident Management, E-Discovery, & Cloud Forensics	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	Does your security information and event management (SIEM) system merge data sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	X				
		SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	X				
Security Incident Management, E-Discovery, & Cloud Forensics <i>Incident Response Legal Preparation</i>	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, customers and/or other external business partners impacted by a	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X				
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X				
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X				
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X				
Security Incident Management, E-Discovery, & Cloud Forensics	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X				
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	X				
Supply Chain Management, Transparency, and Accountability <i>Data Quality and Integrity</i>	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	X				
		STA-01.2	Providers shall design and implement controls to mitigate and	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X				
Supply Chain Management, Transparency, and Accountability <i>Incident Reporting</i>	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			Saimo compliant con il regolamento GDPR per quanto riguarda i data breach	
Supply Chain Management, Transparency, and Accountability	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-	Do you collect capacity and use data for all relevant components of your cloud service offering?	X				
		STA-03.2		Do you provide tenants with capacity planning and use reports?		X			
Supply Chain Management, Transparency, and Accountability <i>Provider Internal Assessments</i>	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X				
Supply Chain Management, Transparency, and Accountability <i>Third Party Agreements</i>	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:	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)	
		STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?			X		
		STA-05.3	• Scope of business relationship	Does legal counsel review all third-party agreements?			X		
		STA-05.4	and services offered (e.g., customer (tenant) data collection, storage,	Do third-party agreements include provision for the security and protection of information and assets?	X				

		STA-05.5	(tenant) data acquisition, exchange and usage, feature sets and	Do you provide the client with a list and copies of all <u>subprocessing agreements and keep this updated?</u>	X			Info disponibili sui siti Microsoft
Supply Chain Management, Transparency, and Accountability <i>Supply Chain Governance Reviews</i>	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Supply Chain Management, Transparency, and Accountability <i>Supply Chain Metrics</i>	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	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between <u>providers and customers (tenants)?</u>	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (<u>upstream/downstream</u>)?	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting <u>from disparate supplier relationships?</u>	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		STA-07.4		Do you review all agreements, policies, and processes at least <u>annually?</u>	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Supply Chain Management, Transparency, and Accountability	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by <u>performing an annual review.</u> The	Do you assure reasonable information security across your <u>information supply chain by performing an annual review?</u>	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		STA-08.2		Does your annual review include all partners/third-party providers <u>upon which your information supply chain depends?</u>	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Supply Chain Management, Transparency, and Accountability <i>Third Party Audits</i>	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, <u>service definitions, and delivery</u>	Do you permit tenants to perform independent vulnerability <u>assessments?</u>	X			previo accordo preliminare
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and <u>networks?</u>	X			in carico a Microsoft per la parte infrastrutturale
Threat and Vulnerability Management <i>Antivirus / Malicious Software</i>	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting	Do you have anti-malware programs that support or connect to <u>your cloud service offerings installed on all of your systems?</u>	X			
		TVM-01.2	business processes and technical measures implemented, to prevent <u>the execution of malware on</u>	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all <u>infrastructure components within industry accepted time frames?</u>	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
Threat and Vulnerability Management <i>Vulnerability / Patch Management</i>	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting	Do you conduct network-layer vulnerability scans regularly as <u>prescribed by industry best practices?</u>	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		TVM-02.2	processes and technical measures implemented, for timely detection of vulnerabilities within	Do you conduct application-layer vulnerability scans regularly as <u>prescribed by industry best practices?</u>	X			
		TVM-02.3	organizational-owned or managed applications, infrastructure network	Do you conduct local operating system-layer vulnerability scans <u>regularly as prescribed by industry best practices?</u>	X			Gestito da Microsoft (vedi assessment CAIQ_3.0.1 pubblicato da Microsoft)
		TVM-02.4	and system components (e.g., network vulnerability assessment,	Will you make the results of vulnerability scans available to <u>tenants at their request?</u>		X		
		TVM-02.5	penetration testing) to ensure the efficiency of implemented security	Do you have a capability to rapidly patch vulnerabilities across all <u>of your computing devices, applications, and systems?</u>	X			in carico a Microsoft per la parte infrastrutturale. In carico a Modus per la parte applicativa.
		TVM-02.6		Will you provide your risk-based systems patching time frames to <u>your tenants upon request?</u>	X			
Threat and Vulnerability Management <i>Mobile Code</i>	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile <u>code operates according to a clearly defined security policy?</u>			X	
		TVM-03.2	measures implemented, to prevent	Is all unauthorized mobile code prevented from executing?			X	

