ICA S.R.L.

CSA Consensus Assessments Initiative Questionnaire

ICA S.R.L.
23/05/2019

CSA Consensus Assessments Initiative Questionnaire

Control Domain	Question ID	Consensus Assessment Questions	ICA
Application & Interface Security ***Application Security***	AIS-01.1	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 Systems/Software Development Lifecycle (SDLC)?	ICA sviluppa il proprio software internamente e attraverso partner ai quali viene richiesta contrattualmente l'implementazione delle più attuali best-practices. Vengono periodicamente svolti controlli e, dove possibile, usati strumenti di verifica automatica del software prima della messa in produzione. Il software SaaS viene verificato con strumenti per la verifica di vulnerabilità prima della distribuzione.
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	
Application & Interface Security ***Customer Access Requirements***	AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	I clienti ICA utilizzano il software secondo le modalità indicate dalla legge e utilizzando le funzionalità indicate nei bandi di gara pubblici a cui ICA partecipa. ICA compie sempre un periodo di formazione sugli operatori a cui fornisce in utilizzo il proprio software e mette a disposizione la necessaria documentazione.
	AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Application & Interface Security ***Data Integrity***	AIS-03.1	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?	Le procedure di caricamento ed elaborazione dei dati prevedono, ove possibile, controlli incrociati per minimizzare eventuali errori di inserimento manuale dei dati. Le routine di caricamento massivo di dati evitano l'accesso diretto ai database e attraversano sempre procedure collaudate e non manipolabili da operatori.
Application & Interface Security ***Data Security / Integrity***	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	L'infrastruttura è collocata completamente su datacenter AWS e ne sfrutta il più possibile le modalità di protezione. L'accesso pubblico agli applicativi non è consentito e viene sempre concordata con l'utilizzatore la modalità di accesso al datacenter.
Audit Assurance & Compliance ***Audit Planning***	AAC-01.1	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.)?	ICA monitora l'utilizzo dei sistemi attraverso strumenti disponibili sul mercato e, in accordo con i clienti, può fornire reportistica standardizzata sull'utilizzo dei sistemi.

Control Domain	Question ID	Consensus Assessment Questions	ICA
Audit Assurance & Compliance*Independent Audits*	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	ICA sfrutta i sistemi di protezione del sistema AWS per mantenere chiuso il proprio datacenter rispetto al mondo Internet. Il sistema AWS svolge autonomamente continui controlli di sicurezza e la reportistica pubblica viene periodicamente verificata. Sugli indirizzi abilitati a ricevere connessioni dall'esterno, e comunque sempre dai soli clienti, vengono regolarmente svolti test di sicurezza attraverso strumenti standard e di terze parti. Ai clienti che ne fanno richiesta viene fornita la documentazione riguardante i test di sicurezza.
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	
	AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	
	AAC-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	
	AAC-02.8	Do you have an internal audit program that allows for cross-functional audit of assessments?	
Audit Assurance & Compliance *Information System*	AAC-03.1	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?	I clienti hanno la proprietà dei dati e l'accesso agli stessi è rigorosamente isolato. Per i clienti che ne fanno richiesta è possibile attivare sistemi di crittografia a vari livelli. I file

Control Domain	Question ID	Consensus Assessment Questions	ICA
Regulatory Mapping	AAC-03.2	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	documentali sono mantenuti in aree separate per ogni cliente e classificati opportunamente attraverso il supporto di specifici database o sistemi documentali avanzati. Sfruttando le possibilità fornite dal datacenter è possibile limitare geograficamente l'accesso alle risorse nelle aree previste dal sistema AWS. L'ipotesi di *data loss* è ridotta al minimo appoggiandosi alle politiche di sicurezza del datacenter e creando ulteriori copie di backup. I termini di ripristino in caso di *data loss* sono regolati contrattualmente con i singoli clienti. ICA dispone di un ufficio legale interno e utilizza consulenti esterni per monitorare le variazioni normative.
	AAC-03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	
	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?	
Business Continuity Management & Operational Resilience ***Business Continuity Planning***	BCR-01.1	Do you provide tenants with geographically resilient hosting options?	I datacenter usati da ICA sono costruiti in cluster in modo da fornire nativamente sia la certezza della localizzazione territoriale sia le capacità di "*service failover*" verso altre aree del cluster.
	BCR-01.2	Do you provide tenants with infrastructure service failover capability to other providers?	
Business Continuity Management & Operational Resilience*Business Continuity Testing*	BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Le procedure previste da AWS nelle proprie certificazioni garantiscono la ragionevole continuità operativa del datacenter. Le procedure per mantenere in funzione i programmi sono garantite attraverso contratti di assistenza fra ICA e i propri

Control Domain	Question ID	Consensus Assessment Questions	ICA
			fornitori di software e servizi sistemici in grado di coprire tutte le ore di disponibilità del servizio.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	ICA può fornire ai propri clienti documentazione riguardante la localizzazione geografica dei datacenter e dei propri uffici nei quali vengano eventualmente svolte attività di supporto a richiesta. ICA è sempre in grado di fornire il percorso dei dati attraverso i propri sistemi e determinare con il cliente eventuali modalità di interfacciamento con sistemi esterni (Poste, Banche, ecc.)
	BCR-03.2	Can tenants define how their data is transported and through which legal jurisdictions?	
Business Continuity Management & Operational Resilience Documentation	BCR-04.1	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?	I soggetti tecnici interessati all'interno dell'infrastruttura ICA hanno a disposizione tutta la necessaria documentazione per la manutenzione del datacenter.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	I datacenter utilizzati da ICA dispongono di protezioni fisiche verso i rischi ambientali certificate da auditor esterni.
Business Continuity Management & Operational Resilience	BCR-06.1	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.)?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Equipment Location			
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	ICA sfrutta le possibilità offerte dall'infrastruttura di servizi AWS per offrire, a richiesta del cliente, punti di ripristino particolari o snapshot delle informazioni. Il cliente deve sempre concordare preventivamente con ICA la possibilità di disporre di snapshot periodici. Per la natura del servizio fornito, ICA non consente di scaricare le macchine virtuali sulle quali i propri sistemi vengono forniti. Su richiesta vengono tuttavia forniti i contenuti delle macchine virtuali sotto forma di file e tabelle.
	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?	
	BCR-07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud 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?	
	BCR-07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	
Business Continuity Management & Operational Resilience*Equipment Power Failures*	BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	ICA sfrutta tutte le protezioni del datacenter AWS, che rispecchiano i più alti standard di sicurezza. La documentazione relativa è disponibile pubblicamente.
Business Continuity Management & Operational	BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	ICA può fornire ai propri clienti tutte le statistiche di utilizzo dei propri sistemi in datacenter e in aggiunta

Control Domain	Question ID	Consensus Assessment Questions	ICA
Resilience ***Impact Analysis***	BCR-09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	comunica tempestivamente ai propri clienti eventuali interruzioni nel regolare funzionamento dei software o interventi programmati. Gli SLA sono sempre stabiliti contrattualmente con il cliente, il quale ne richiede visibilità secondo quanto contrattualmente concordato caso per caso.
	BCR-09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	
Business Continuity Management & Operational Resilience ***Policy***	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	ICA dispone di procedure interne per la regolamentazione dei ruoli e dei compiti degli incaricati interni ed esterni alla manutenzione dei software. Attraverso una intranet aziendale, regolamentata secondo quanto descritto nelle proiprie certificazioni ISO, ICA diffonde al personale incaricato le istruzioni e le modalità di comportamento. ICA tiene inoltre regolarmente corsi specifici al personale.
Business Continuity Management & Operational Resilience ***Retention Policy***	BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	Le modalità di tenuta dei dati e le possibilità di cancellazione sono regolamentate, vista la specificità della materia trattata, da specifiche norme. I clienti, di conseguenza, hanno solo limitate possibilità di cancellazione completa dei dati e il software garantisce che eventuali cancellazioni avvengano secondo la normativa. È responsabilità
	BCR-11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	
	BCR-11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
	BCR-11.5	Do you test your backup or redundancy mechanisms at least annually?	del cliente gestire correttamente i propri dati ed evitare perdite dovute ad un utilizzo non corretto del software. In casi specifici in cui sia richiesto il recupero di informazioni, ICA è in grado di ripristinare situazioni passate secondo periodicità predefinite. Le procedure di backup vengono regolarmente testate e i risultati annotati in appositi registri.
Change Control & Configuration Management ***New Development / Acquisition***	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Ogni aggiornamento o integrazione ai sistemi deve essere approvato da diversi team di sviluppo e supporto sistemistico, sia interni che esterni e deve essere compliant con gli standard del data center AWS. ICA traccia dettagliatamente gli aggiornamenti attraverso un workflow di documentazione e approvazione interno. L'approvazione finale delle modifiche è sempre demandata ad un comitato che include responsabili con competenze nelle aree interessate dalla modifica stessa (area contabile, area legale, area organizzativa).
	CCC-01.2	Is documentation available that describes the installation, configuration, and use of products/services/features?	
Change Control & Configuration Management ***Outsourced Development***	CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	Gli standard qualitativi vengono valutati periodicamente, in particolare verificando la compliance rispetto alle normative e alle indicazioni emanate dagli enti preposti. Le richieste di variazioni finalizzate a
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
			miglioramenti qualitativi sono documentate e motivate in apposita documentazione interna che deve essere approvata dai settori aziendali coinvolti. ICA dispone di un apposito ufficio interno che svolge continui controlli sulle procedure, lavorando anche in contatto diretto con i clienti. Ogni problematica individuata viene tracciata in un apposito sistema di database e la risoluzione viene documentata.
Change Control & Configuration *ManagementQuality Testing*	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	Tutta la documentazione tecnica è disponibile per i clienti. In aggiunta i clienti hanno accesso diretto all'ufficio interno preposto alla risoluzione dei problemi informatici e hanno la possibilità di segnalare e monitorare eventuali difetti.
	CCC-03.2	Is documentation describing known issues with certain products/services available?	
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	ICA dispone di un apposito ufficio interno, differente dalle unità di sviluppo, con il compito di verificare il software prodotto prima e dopo il rilascio. Lo stesso ufficio si occupa di tracciare i bug segnalati su un apposito sistema e di fornire al cliente il tracciamento della risoluzione. Su richiesta è possibile fornire al cliente accesso diretto al tracking della risoluzione problemi.
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Change Control & Configuration Management ***Unauthorized Software Installations***	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	I sistemi messi a disposizione dei clienti sono installati su macchine virtuali controllate da politiche di dominio restrittive e sulle quali sono installati sia sistemi antivirus che sistemi di audit degli accessi di terze parti. In aggiunta l'accesso a queste macchine in ambiente di produzione è limitato ad un numero molto ristretto di tecnici e sempre attraverso canali criptati. Ove possibile la connessione delle macchine è limitata al minimo e gli ambienti di datacenter non sono pubblicati all'esterno.
Change Control & Configuration Management ***Production Changes***	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	Tutte le modifiche apportate ai sistemi devono attraversare un processo di approvazione regolamentato da uno specifico software di tracciamento. Solo le modifiche che superano l'iter vengono sviluppate e arrivano in produzione. L'iter di approvazione include anche personale specializzato nelle aree di competenza sulle quali la modifica impatta (area contabile, area legale, area amministrativa, area tecnica). La documentazione di ogni modifica è disponibile ai clienti sotto forma di documentazione d'uso che descrive le corrette modalità di utilizzo.

Control Domain	Question ID	Consensus Assessment Questions	ICA
Data Security & Information Lifecycle Management ***Classification***	DSI-01.1	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 wrong country)?	Sfruttando le capacità del datacenter vengono assegnati TAG sia alle virtual machines che ai repository documentali, che ai singoli documenti in modo da poterli identificare e associare ai clienti. È possibile, se richiesto, limitare l'accesso geografico ai servizi secondo le possibilità fornite dal datacenter AWS. La localizzazione fisica delle risorse è sempre disponibile.
	DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	
	DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?	
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	
	DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	
	DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	
Data Security & Information Lifecycle Management ***Data Inventory / Flows***	DSI-02.1	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?	I dati sono residenti su datacenter in specifiche aree geografiche e non vengono spostati da quelle aree. Nel caso in cui, per ragioni di manutenzione o di organizzazione dei datacenter, dovesse rendersi necessario spostare i dati, ICA procederebbe a informare i
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
			propri clienti sulla nuova collocazione dei datacenter e sulle procedure eseguite.
Data Security & Information Lifecycle Management ***E-commerce Transactions***	DSI-03.1	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)?	L'accesso ai datacenter è consentito solamente attraverso connessioni criptate che utilizzano standard aperti. I clienti possono richiedere differenti modalità di collegamento a seconda dei servizi e delle proprie infrastrutture. ICA consente e garantisce solamente comunicazioni su reti pubbliche che avvengano attraverso protocolli crittografati.
	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)?	
Data Security & Information Lifecycle Management ***Handling / Labeling / Security Policy***	DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	Tutte le macchine virtuali, i database e i repository di documenti sono taggati e riconducibili ai clienti che li hanno in utilizzo.
	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	
Data Security & Information Lifecycle Management ***Nonproduction Data***	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	I contratti di fornitura e manutenzione che ICA stipula con i propri partner prevedono rigide regole riguardo la protezione dei dati. Gli ambienti di sviluppo e test non sono ricavati da database di produzione e non contengono i dati relativi a clienti reali. ICA verifica, attraverso l'ufficio interno preposto, che opera indipendentemente dai gruppi di sviluppo, che le regole

Control Domain	Question ID	Consensus Assessment Questions	ICA
			contrattualizzate riguardanti la privacy vengano rispettate.
Data Security & Information Lifecycle Management ***Ownership / Stewardship***	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	ICA comunica ai propri clienti le modalità di trattamento interno dei dati. I clienti che utilizzano sistemi ICA in modalità SaaS sono i proprietari dei dati e concordano con ICA le modalità di verifica delle procedure.
Data Security & Information Lifecycle Management ***Secure Disposal***	DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	ICA utilizza sistemi hardware acquisiti attraverso il datacenter AWS. Il datacenter AWS utilizza e certifica le tecniche dettagliate nella specifica NIST 800-88. La relativa documentazione è disponibile sul sito del fornitore AWS. Le macchine virtuali utilizzati sono installate su volumi criptati.
	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?	
Datacenter Security ***Asset Management***	DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	ICA mantiene elenchi degli asset impiegati in tutto il ciclo di fornitura del sistema SaaS, incluse le risorse software.
	DCS-01.2	Do you maintain a complete inventory of all of your critical supplier relationships?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Datacenter Security ***Controlled Access Points***	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?	L'intero trattamento dei dati utilizzati da ICA avviene all'interno del datacenter AWS, che implementa le necessarie misure di sicurezza fisica.
Datacenter Security ***Equipment Identification***	DCS-03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	AWS gestisce la procedura in accordo alla propria conformità ISO 27001.
Datacenter Security ***Offsite Authorization***	DCS-04.1	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)?	Nel caso in cui i dati dovessero essere spostati attraverso differenti areee fisiche, ICA provvede ad informare i clienti delle modalità e del nuovo posizionamento.
Datacenter Security ***Offsite Equipment***	DCS-05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	ICA utilizza, in remoto, sistemi fisici nel datacenter AWS per lo svolgimento delle attività. Per i terminali locali, viene applicata una politica di classificazione e dismissione degli apparati aderente alla politica parte della certificazione 27001 dell'azienda.
Datacenter Security ***Policy***	DCS-06.1	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?	ICA dispone di un sistema interno di diffusione delle indicazioni comportamentali e delle politiche nei confronti del personale. ICA svolge periodicamente corsi di aggiornamento del personale in accordo alle proprie certificazioni ISO.
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Datacenter Security ***Secure Area Authorization***	DCS-07.1	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)?	ICA mantiene i dati in un'unica area geografica, rispettando le attuali normative riguardanti il posizionamento dei dati per la Pubblica Amministrazione.
Datacenter Security*Unauthorized Persons Entry*	DCS-08.1	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?	L'accesso agli uffici ICA è rigorosamente controllato e monitorato con l'utilizzo di badge e telecamere. Eventuale personale esterno può accedere ai locali solo se accompagnato da un operatore ICA che lo accompagna per tutta la durata dell'intervento.
Datacenter Security ***User Access***	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	
Encryption & Key Management ***Entitlement***	EKM-01.1	Do you have key management policies binding keys to identifiable owners?	Nei casi in cui vengono utilizzate chiavi di crittografia specifiche per cliente, le chiavi vengono fornite al cliente stesso.
Encryption & Key Management ***Key Generation***	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	Per quanto riguarda tutta l'area documentale, per ogni cliente possono essere create su richiesta chiavi di crittografie distinte. Per quanto riguarda i database, su richiesta del cliente può essere creata una specifica istanza con crittografia riservata. Le chiavi di crittografia vengono gestite attraverso l'infrastruttura resa disponibile da AWS.
	EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	
	EKM-02.3	Do you maintain key management procedures?	
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Encryption & Key Management ***Encryption***	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Tutte le comunicazioni che trasportino dati dei clienti avvengono su canali criptati. Vengono utilizzate tecnologie che implementano protocolli IPSec oppure comunicazioni su canali in VPN (L2TP/IPSec) verso i clienti. Il cliente può richiedere l'accesso ai sistemi indicando il proprio IP pubblico e utilizzando protocolli HTTPS o RDP protetto con SSL/TLS. ICA classifica i propri clienti secondo le modalità di accesso e conserva documentazione riguardanti le specifiche di connettività per ognuno. ICA non consente l'accesso ai sistemi da reti pubbliche senza i requisiti di crittografia necessari.
	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	
	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)?	
	EKM-03.4	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	
Encryption & Key Management ***Storage and Access***	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	I canali crittografati stabiliti con i clienti si basano su tecnologie rese disponibili sul datacenter AWS. A seconda dei casi, le chiavi di crittografia sono disponibili sui gestori di chiavi predisposti da AWS, oppure nelle macchine virtuali che gestiscono gli accessi in VPN. Queste non sono accessibili dai clienti e sono a loro volta residenti su filesystem crittografati. ICA non può ricostruire le chiavi di crittografia consegnate ai clienti.
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	
	EKM-04.3	Do you store encryption keys in the cloud?	
	EKM-04.4	Do you have separate key management and key usage duties?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Governance and Risk Management*Baseline Requirements*	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	L'infrastruttura è documentata e monitorata sia attraverso strumenti resi disponibili da AWS, sia attraverso strumenti interni, sia proprietari che commerciali. Ai clienti non è consentita l'installazione di nulla sul datacenter.
	GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	
	GRM-01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	
Governance and Risk Management *Risk Assessments*	GRM-02.1	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)?	Ai clienti può essere reso disponibile un pannello di monitoraggio indicante lo stato di funzionamento dei servizi. Il pannello riporta informazioni riguardanti l'efficienza complessiva del sistema, noni dettagli delle cause di eventuali interruzioni.
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	I controlli di vulnerabilità vengono condotti con frequenza mensile da strutture interne e annualmente da strutture esterne all'azienda.
Governance and Risk Management *Management Oversight*	GRM-03.1	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?	L'azienda provvede alla formazione del proprio personale e mantiene una struttura interna dedicata alla verifica della compliance alle politiche di sicurezza. L'azienda si avvale inoltre di aziende esterne per la verifica delle aree di responsabilità.

Control Domain	Question ID	Consensus Assessment Questions	ICA
Governance and Risk Management ***Management Program***	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	L'azienda dispone di certificazione ISO 27001 e provvede alla revisione periodica delle proprie politiche di sicurezza. Su richiesta dei clienti, questi possono essere messi a conoscenza delle politiche in vigore e richiedere specifiche verifiche.
	GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	
Governance and Risk Management ***Management Support / Involvement***	GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	I rapporti con i fornitori sono regolamentati attraverso gli standard previsti dalla normativa ISO 27001. I contratti prevedono specifiche clausole riguardanti il rispetto delle normative sulla privacy. ICA compie direttamente controlli, attraverso uno specifico ufficio interno, sulle attività dei fornitori.
Governance and Risk Management ***Policy***	GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	I rapporti con i fornitori sono regolamentati attraverso gli standard previsti dalla normativa ISO 27001. I contratti prevedono specifiche clausole riguardanti il rispetto delle normative sulla privacy. ICA compie direttamente controlli, attraverso uno specifico ufficio interno, sulle attività dei fornitori. Su richiesta dei clienti ICA può rendere disponibili le proprie modalità di verifica di aderenza agli standard.
	GRM-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	
	GRM-06.3	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	
	GRM-06.4	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Governance and Risk Management *Policy Enforcement*	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Ai dipendenti ed ai fornitori vengono comunicate le politiche di sicurezza e i contratti prevedono specifiche clausole. I dipendenti e i fornitori sono soggetti a sanzioni secondo quanto regolamentato dalle normative vigenti e dagli accordi contrattuali.
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	Il documento di valutazione dei rischi viene rinnovato annualmente e rivalutato al fine di rimanere valido.
Governance and Risk Management *Policy Reviews*	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Le politiche vengono revisionate ogni anno al fine di garantire standard di sicurezza sempre maggiori. I clienti vengono informati nel caso in cui vengano apportate modifiche che coinvolgano la loro specifica operatività sui sistemi oppure che comportino lo spostamento di dati su differenti sistemi al di fuori del datacenter.
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	
Governance and Risk Management *Assessments*	GRM-10.1	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?	Il piano di gestione dei rischi è sviluppato da un'azienda esterna, la quale individua le minacce residue dopo il piano di mitigazione annuale. Il rischio residuo è determinato internamente valutando le

Control Domain	Question ID	Consensus Assessment Questions	ICA
	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)?	probabilità di accadimento e la gravità della minaccia.
Governance and Risk Management ***Program***	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	Il programma per la gestione dei rischi prevede l'utilizzo di documentazione interna, resa disponibile ai soggetti interessati dai piani di contromisure.
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	
Human Resources ***Asset Returns***	HRS-01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	ICA utilizza strumenti sul mercato per l'identificazione di comportamenti anomali, per loggare l'accesso ai dati e ai file e per tracciare anomalie nei comportamenti degli operatori.
	HRS-01.2	Is your Privacy Policy aligned with industry standards?	
Human Resources*Background Screening*	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?	ICA svolge, nei limiti consentiti dalle normative, controlli sui propri fornitori e dipendenti.
Human Resources ***Employment Agreements***	HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	ICA svolge corsi interni docuementati riguardanti le politiche di sicurezza adottate. L'esito dei corsi è tracciato attraverso sistemi automatici. I dipendenti ed i fornitori sono tenuti a firmare specifici accordi di riservatezza.
	HRS-03.2	Do you document employee acknowledgment of training they have completed?	
	HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
	HRS-03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	
	HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	
Human Resources ***Employment Termination***	HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	ICA implementa procedure per il cambio di mansione, l'interruzione della collaborazione e per eventuali sospensioni degli incarichi. Le procedure prevedono l'utilizzo di software di workflow e documentazione interna per l'approvazione, il tracciamento e la verifica delle corrette riassegnazioni dei privilegi sui sistemi.
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	
Human Resources ***Portable / Mobile Devices***	HRS-05.1	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)?	I dati specifici dei clienti non sono disponibili localmente su sistemi mobili. I sistemi mobili possono accedere al datacenter solamente tramite VPN le cui credenziali sono specifiche per utente. Sui dispositivi portatili, dove possibile, sono implementati meccanismi di crittografia dei dischi rigidi.
Human Resources ***Non-Disclosure Agreements***	HRS-06.1	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?	ICA dispone di un ufficio legale interno e di consulenti esterni che rivedono periodicamente la conformità delle politiche implementate con le normative.

Control Domain	Question ID	Consensus Assessment Questions	ICA
Human Resources ***Roles / Responsibilities***	HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	In fase di contrattualizzazione con il cliente vengono forniti documenti riguardanti la struttura interna e le responsabilità delle varie funzioni.
Human Resources*Acceptable Use*	HRS-08.1	Do you provide documentation regarding how you may access tenant data and metadata?	Le modalità di accesso ai dati del cliente da parte di ICA sono esplicate nei documenti allegati al contratto e concordate con il cliente. ICA accede ai dati del cliente solamente per svolgere funzioni necessarie a svolgere la propria attività e nel rispetto degli accordi di riservatezza stipulati con il cliente.
	HRS-08.2	Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)?	
	HRS-08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	
Human Resources ***Training / Awareness***	HRS-09.1	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?	Durante la fase di attivazione dei servizi, ICA svolge specifiche sessioni di istruzioni riguardanti le modalità di accesso ai dati ed ai sistemi. Gli utenti, che tuttavia rimangono i proprietari d i dati, vengono istruiti riguardo le proprie responsabilità dovute ad un utilizzo non corretto dei sistemi.
	HRS-09.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	
Human Resources ***User Responsibility***	HRS-10.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	Durante la fase di attivazione dei servizi, ICA svolge specifiche sessioni di istruzioni riguardanti le modalità di accesso ai dati ed ai sistemi. Gli utenti, che tuttavia

Control Domain	Question ID	Consensus Assessment Questions	ICA
	HRS-10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	rimangono i proprietari d i dati, vengono istruiti riguardo le proprie responsabilità dovute ad un utilizzo non corretto dei sistemi. ICA fornisce al cliente ogni informazione di cui viene in possesso riguardo utilizzi impropri degli strumenti messi a disposizione.
	HRS-10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	
Human Resources ***Workspace***	HRS-11.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	ICA utilizza sistemi di audit di terze parti per individuare tentativi di accessi non consentiti ai dati al di fuori delle procedure standard. I sistemi ICA sono protetti da componenti software di terze parti che verificano eventuali compromissioni degli applicativi.
	HRS-11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	
	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?	
Identity & Access Management*Audit Tools Access*	IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	Gli accessi al sistema sono loggati e mantenuti riservati. Uno specifico software analizza anomalie negli accessi e vengono eseguiti controlli a campione su specifici eventi. Sono definite specifiche categorie di eventi che producono allarmi automatici. Gli accessi amministrativi sono suddivisi per specifiche aree e funzioni in modo da limitare compromissioni solamente ad aree ridotte del sistema
	IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Identity & Access Management ***User Access Policy***	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	La gestione degli accessi al sistema è automaticamente legata alla durata dei contratti cliente per quanto riguarda i loro accessi, ed è legata alla durata degli incarichi interni per quanto riguarda gli accessi operatore. ICA implementa una procedura automatizzata che segue uno specifico workflow legato al cambio di mansione/ruolo interno. La gestione delle credenziali di accesso è parte integrante di gestione del workflow. Periodicamente viene effettuata una verifica su tutti gli account attivi sui sistemi al fine di verificare la corrispondenza fra i ruoli e le mansioni assegnate.
	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?	
Identity & Access Management ***Diagnostic / Configuration Ports Access***	IAM-03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Gli accessi all'infrastruttura cloud avvengono attraverso canali criptati verso il datacenter attestati su reti separate rispetto agli accessi cliente.
Identity & Access Management ***Policies and Procedures***	IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Tutto il personale che ha la possibilità di accedere all'infrastruttura IT è individuato e le credenziali di accesso sono personali e legate al livello specifico di accesso.
	IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Identity & Access Management ***Segregation of Duties***	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Su richiesta dei clienti, è possibile comunicare documentazione riguardo la struttura dei dati gestiti nel datacenter e sulla separazione dei ruoli. Il datacenter è progettato per separare gli accessi amministrativi alle varie aree funzionali. I responsabili delle differenti aree operano, dove necessario, come amministratori di sistema limitatamente alle aree necessarie per i propri scopi.
Identity & Access Management ***Source Code Access Restriction***	IAM-06.1	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?	Il codice sorgente degli applicativi è mantenuto su server dedicati allo sviluppo accessibili solamente dal personale autorizzato. Il codice sorgente, anche quando sviluppato da fornitori esterni, non viene replicato all'esterno dei server aziendali. L'ufficio informatica interno sovrintende sempre al controllo dei server di sviluppo e alle corrette modalità operative dei fornitori.
	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?	
Identity & Access Management ***Third Party Access***	IAM-07.1	Do you provide multi-failure disaster recovery capability?	L'accesso ai sistemi avviene attraverso i meccanismi messi a disposizione dai datacenter AWS. AWS mette a disposizione automaticamente meccanismi di *disaster recovery* all'interno della stessa zona di disponibilità.
	IAM-07.2	Do you monitor service continuity with upstream providers in the event of provider failure?	
	IAM-07.3	Do you have more than one provider for each service you depend on?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
	IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	Nel caso di guasti alla componente software proprietaria, ICA interviene seguendo il proprio piano di recovery che può arrivare a comportare il ripristino di una condizione precedente del sistema.
	IAM-07.5	Do you provide the tenant the ability to declare a disaster?	
	IAM-07.6	Do you provide a tenant-triggered failover option?	
	IAM-07.7	Do you share your business continuity and redundancy plans with your tenants?	
Identity & Access Management ***User Access Restriction / Authorization***	IAM-08.1	Do you document how you grant and approve access to tenant data?	Il cliente gestisce autonomamente le proprie politiche di accesso ai dati e configura autonomamente i ruoli dei propri operatori. L'eventuale assegnazione di ruoli non corretti agli operatori abilitati sul sistema è responsabilità del cliente. ICA può supportare nella definizione dei ruoli per gli operatori in fase di attivazione del sistema oppure in caso di variazioni da apportare su richiesta dei clienti.
	IAM-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	
Identity & Access Management ***User Access Authorization***	IAM-09.1	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?	Le credenziali di accesso e i ruoli vengono forniti su richiesta del cliente e secondo i ruoli richiesti e per i limiti di tempo richiesti. Il workflow interno di gestione delle risorse determina i ruoli per gli utenti collegandoli ai contratti e alle funzioni in azienda. Su

Control Domain	Question ID	Consensus Assessment Questions	ICA
	IAM-09.2	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?	richiesta del cliente e se preventivamente concordato, ICA può fornire accesso controllato a specifici utenti e a risorse riguardanti specifici clienti.
Identity & Access Management ***User Access Reviews***	IAM-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Tutti gli accessi interni hanno durata massima preimpostata e vengono riattivati durante la fase di revisione prevista dalla procedura ISO 27001. Tutti gli accessi sono collegati al software di gestione del personale e vengono automaticamente disabilitati in caso di interruzione del rapporto di lavoro. La gestione degli accessi da parte di fornitori esterni è legata alla durata dei contratti e in fase di abilitazione dell'utente la scadenza viene preimpostata
	IAM-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	
	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?	
Identity & Access Management ***User Access Revocation***	IAM-11.1	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?	Tutti gli accessi interni hanno durata massima preimpostata e vengono riattivati durante la fase di revisione prevista dalla procedura ISO 27001. Tutti gli accessi sono collegati al software di gestione del personale e vengono automaticamente disabilitati in caso di interruzione del rapporto di lavoro. La gestione degli accessi da parte di fornitori esterni è legata alla durata dei contratti e in fase di abilitazione dell'utente la scadenza viene preimpostata.
	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?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Identity & Access Management ***User ID Credentials***	IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	I sistemi ICA non consentono l'integrazione con sistemi SSO del cliente. Le politiche di gestione della password sono specificate nei documenti del GDPR ICA e possono variare nel tempo per adeguarsi alle normative. In particolare, i requisiti minimi di complessità, durata e ripetibilità delle password sono documentati internamente e comunicati ai clienti. I clienti possono disporre di account di livello superiore che consentono la disabilitazione o la sospensione dei propri account nel sistema.
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	
	IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	
	IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	
	IAM-12.5	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?	
	IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	
	IAM-12.7	Do you allow tenants to use third-party identity assurance services?	
	IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	
	IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
	IAM-12.10	Do you support the ability to force password changes upon first logon?	
	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)?	
Identity & Access Management ***Utility Programs Access***	IAM-13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	L'accesso all'infrastruttura virtualizzata è gestito da AWS e non è accessibile direttamente a ICA. AWS rende disponibili le proprie politiche di protezione dell'infrastruttura di virtualizzazione. I sistemi forniti all'utente sono adeguatamente protetti da politiche restrittive che non consentono l'installazione di software
	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.)?	
	IAM-13.3	Are attacks that target the virtual infrastructure prevented with technical controls?	
Infrastructure & Virtualization Security ***Audit Logging / Intrusion Detection***	IVS-01.1	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?	Tutta l'infrastruttura virtuale su cui si appoggiano i servizi SaaS è mantenuta su sistemi AWS e di conseguenza ne vengono ereditate le politiche. L'accesso ai sistemi utenti è monitorato tramite firewall. I log degli accessi agli applicativi vengono manutenuti in database separati e quotidianamente esportati su sistemi indipendenti non accessibili agli utenti e non raggiungibili direttamente dalle macchine accessibili ai clienti. I log dei web server vengono trasferiti su macchine esterne. I log
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	
	IVS-01.4	Are audit logs centrally stored and retained?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	vengono riversati periodicamente su sistemi fuori linea accessibili solamente da personale specifico. Sul sistema operano procedure di terze parti in grado di segnalare anomalie.
Infrastructure & Virtualization Security ***Change Detection***	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	ICA non utilizza immagini predefinite di virtual machines per fornire il servizio ai clienti.
	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)?	
Infrastructure & Virtualization Security ***Clock Synchronization***	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	ICA utilizza il sistema NTP su tutti i propri sistemi per sincronizzarne l'orario
Infrastructure & Virtualization Security ***Capacity / Resource Planning***	IVS-04.1	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?	ICA monitora attraverso sistemi automatici l'utilizzo di risorse sui propri sistemi e dispone di un'infrastruttura scalabile in grado di adeguarsi alle richieste dei clienti. I sistemi di monitoraggio prevedono allarmi in grado di segnalare il raggiungimento di soglie di utilizzo delle risorse.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	
	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?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
	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?	
Infrastructure & Virtualization Security ***Management - Vulnerability Management***	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	ICA utilizza il sistema di virtualizzazione di AWS, altamente monitorato e controllato. Si rimanda ai meccanismi di sicurezza del sistema di virtualizzazione di AWS.
Infrastructure & Virtualization Security ***Network Security***	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	ICA non fornisce servizi di tipo IaaS.
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	
	IVS-06.4	Are all firewall access control lists documented with business justification?	
Infrastructure & Virtualization Security ***OS Hardening and Base Controls***	IVS-07.1	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?	Le politiche di dominio di ICA e i software di supporto di terze parti utilizzati dal settore informatica automatizzano la configurazione. I sistemi antivirus e di firewalling locale sono centralizzati e monitorati tramite una console dedicata. I firewall perimetrali di AWS

Control Domain	Question ID	Consensus Assessment Questions	ICA
			sono configurati per supportare nella riduzione al minimo dei protocolli e delle porte aperte verso l'esterno. I sistemi ICA non sono pubblicamente raggiungibili se non dai clienti abilitati esplicitamente.
Infrastructure & Virtualization Security ***Production / Non-Production Environments***	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Generalmente i servizi offerti da ICA includono procedure di simulazione specifiche. I clienti non hanno accesso ad ambienti di test del software.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	ICA non fornisce servizi di tipo IaaS.
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	Gli ambienti di produzione, sviluppo e test sono separati sia logicamente che fisicamente.
Infrastructure & Virtualization Security ***Segmentation***	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	Tutti gli ambiente di produzione e di sviluppo sono separati utilizzando diverse VPC all'interno del sistema AWS. Tutti gli accessi ai sistemi transitano attraverso firewall e sono rigorosamente limitati agli indirizzi, alle VPN o ai tunnel IPSec autorizzati.
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, and contractual requirements?	
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
	IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	
Infrastructure & Virtualization Security ***VM Security - Data Protection***	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	Non vengono eseguiti servizi di migrazione di server fisici.
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	
Infrastructure & Virtualization Security ***VMM Security - Hypervisor Hardening***	IVS-11.1	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)?	L'accesso alle funzioni di gestione dell'ambiente di virtualizzazione EC2 di AWS è limitato ai soli amministratori incaricati e avviene attraverso i meccanismi di sicurezza delle comunicazioni e degli accessi resi disponibili da AWS.
Infrastructure & Virtualization Security ***Wireless Security***	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Non sono disponibili accessi wireless interni all'area datacenter. Eventuali connessioni wireless da parte di clienti autorizzati oppure operatori possono avvenire solamente tramite VPN

Control Domain	Question ID	Consensus Assessment Questions	ICA
	IVS-12.2	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)?	criptate IPSec direttamente dal dispositivo. E' responsabilità del cliente la protezione dei propri sistemi wireless al di fuori del perimetro datacenter ICA. L'accesso ai servizi datacenter, tuttavia, può avvenire solamente attraverso protocolli criptati.
	IVS-12.3	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?	
Infrastructure & Virtualization Security*Network Architecture*	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	I diagrammi di rete del datacenter AWS e le specifiche di costruzione dei software proprietari individuano chiaramente il posizionamento dei dati e il transito dei dati stessi fra le diverse macchine virtuali. Vengono inoltre individuati i punti di ingresso e di uscita di tutti i flussi dal datacenter.
	IVS-13.2	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?	ICA utilizza software per il firewalling di terze parti per il monitoraggio e la segnalazione di allarmi. I software vengono automaticamente aggiornati dai fornitori.

Control Domain	Question ID	Consensus Assessment Questions	ICA
Interoperability & Portability ***APIs***	IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	ICA non fornisce API per l'integrazione con sistemi esterni. I servizi di interscambio dati con Enti pubblici avvengono secondo le modalità concordate con gli stessi (VPN oppure tunnel IPSec) oppure tramite passaggio su rete SPC nazionale.
Interoperability & Portability ***Data Request***	IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	Su richiesta ICA fornisce ai clienti i propri dati in formati non strutturati. I documenti in formato PDF e i dati in file XML.
Interoperability & Portability ***Policy & Legal***	IPY-03.1	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?	Le migrazioni dati possono essere eseguite solamente con l'intervento diretto del personale ICA, che provvede a validarli su sistemi di test. Superato il controllo formale, la responsabilità del contenuto informativo dei dati è del cliente. Tutto il processo di migrazione è concordato con il cliente che viene messo a conoscenza di tutti gli step eseguiti.
	IPY-03.2	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	
Interoperability & Portability ***Standardized Network Protocols***	IPY-04.1	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Interoperability & Portability ***Virtualization***	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	Il sistema di virtualizzazione utilizzato è quello di AWS e il datacenter consente - su richiesta- l'esportazione delle macchine virtuali in formati standard.
	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?	
Mobile Security***Anti-Malware***	MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	ICA informa periodicamente il proprio personale ed i clienti tramite comunicazioni diffuse via e-mail oppure pubblicate in specifiche aree utente di nuove minacce e della necessità di adeguamenti nei comportamenti per minimizzare i rischi.
Mobile Security ***Application Stores***	MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	La responsabilità dei dispositivi utilizzati dai clienti per accedere ai dati è dei clienti stessi. ICA garantisce l'utilizzo di protocolli di comunicazione considerati sicuri secondo gli standard di sicurezza più elevati.
Mobile Security ***Approved Applications***	MOS-03.1	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?	
Mobile Security ***Approved Software for BYOD***	MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Mobile Security ***Awareness and Training***	MOS-05.1	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?	L'uso dei dispositivi mobili all'interno dell'organizzazione è limitato. I dispositivi autorizzati all'accesso al datacenter sono configurati internamente forniti agli utilizzatori senza la possibilità di installare altre applicazioni. Tutti i dispositivi possono accedere solamente tramite VPN criptata preconfigurata. Al momento della fornitura del dispositivo all'operatore, questo viene informato sulle responsabilità e i limiti di utilizzo. Gli accessi alle VPN del datacenter sono loggati e monitorati. Viene mantenuta una lista dei dispositivi forniti e dell'operatore che ne è responsabile in modo da poter associare gli accessi all'operatore.
Mobile Security ***Cloud Based Services***	MOS-06.1	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?	
Mobile Security ***Compatibility***	MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?	
Mobile Security ***Device Eligibility***	MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	
Mobile Security ***Device Inventory***	MOS-09.1	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)?	
Mobile Security ***Device Management***	MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	
Mobile Security***Encryption***	MOS-11.1	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?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Mobile Security ***Jailbreaking and Rooting***	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	
	MOS-12.2	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?	
Mobile Security ***Legal***	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	
	MOS-13.2	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?	
Mobile Security ***Lockout Screen***	MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	
Mobile Security ***Operating Systems***	MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	
Mobile Security ***Passwords***	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	
	MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	
Mobile Security *Policy*	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	
	MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	
	MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	
Mobile Security*Remote Wipe*	MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	
Mobile Security *Security Patches*	MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	I dispositivi forniti agli utenti vengono periodicamente controllati per regolare manutenzione. Considerati gli altri livelli di sicurezza previsti e il livello di affidabilità del personale a cui vengono forniti i dispositivi mobili, non sono applicati livelli di controllo ulteriori sul software installato. I tecnici tuttavia verificano l'aggiornamento del sistema e provvedono agli aggiornamenti necessari.
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
Mobile Security ***Users***	MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	L'accesso via dispositivi BYOD non è consentito e non vengono fornite credenziali che consentano l'accesso attraverso dispositivi non controllati.
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	
Security Incident Management, E-Discovery, & Cloud Forensics ***Contact / Authority Maintenance***	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	
Security Incident Management, E-Discovery, & Cloud Forensics ***Incident Management***	SEF-02.1	Do you have a documented security incident response plan?	ICA dispone di un *response plan* in caso di incidente che viene condiviso su richiesta con i clienti. Eventuali necessità dei clienti possono essere integrate per venire incontro a specifiche esigenze. Il piano viene verificato in occasione della revisione annuale della certificazione ISO27001 e in fase di revisione dei documenti relativi al GDPR
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	
	SEF-02.4	Have you tested your security incident response plans in the last year?	
Security Incident Management, E-Discovery, & Cloud Forensics ***Incident Reporting***	SEF-03.1	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?	Il sistema raccogli informazioni provenienti da differenti fonti e sonde nel sistema al fine di individuare situazioni di allarme causate da combinazioni particolari di attività.

Control Domain	Question ID	Consensus Assessment Questions	ICA
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	Nella maggioranza dei casi il sistema di log consente di isolare a specifici clienti il perimetro dell'incidente. In alcune circostanze ciò non è tecnicamente possibile al momento.
Security Incident Management, E-Discovery, & Cloud Forensics ***Incident Response Legal Preparation***	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	
	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?	In casi molto particolari esiste una procedura per separare i dati di uno specifico cliente in un ambiente isolato in modo da non interferire con quelli degli altri e poter essere congelato attraverso diversi snapshot nel tempo.
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	
Security Incident Management, E-Discovery, & Cloud Forensics ***Incident Response Metrics***	SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	Le procedure interne prevedono il tracciamento degli incidenti. I dettagli degli incidenti non vengono condivisi con i clienti, tuttavia possono essere fornite informazioni statistiche aggregate su richiesta.
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	
Supply Chain Management, Transparency, and	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	La qualità dei dati è responsabilità dei clienti. Le procedure ICA forniscono meccanismi per mitigare

Control Domain	Question ID	Consensus Assessment Questions	ICA
Accountability ***Data Quality and Integrity***	STA-01.2	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?	errori dovuti alla bassa qualità dei dati cliente, tuttavia le decisioni sull'utilizzo dei dati sono sempre prese dai clienti. L'accesso ai dati da parte di ICA è sempre limitato alle specifiche aree di competenza degli operatori. Nessun operatore ICA ha accesso diretto all'intero sistema.
Supply Chain Management, Transparency, and Accountability ***Incident Reporting***	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	In caso di incidente tutte le informazioni vengono condivise con i clienti tramite contatto diretto con i responsabili.
Supply Chain Management, Transparency, and Accountability ***Network / Infrastructure Services***	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	L'utilizzo delle risorse viene monitorato da sistemi automatici. ICA si occupa di mantenere in efficienza i sistemi. Nel caso in cui i clienti richiedano specifiche informazioni sulle capacità dei sistemi, queste possono essere fornite.
	STA-03.2	Do you provide tenants with capacity planning and use reports?	
Supply Chain Management, Transparency, and Accountability ***Provider Internal Assessments***	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	In occasioni delle revisioni per le certificazioni ISO27001 e per la documentazione GDPR vengono riprese in esame tutte le politiche del sistema.
Supply Chain Management, Transparency, and Accountability	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	ICA condivide con i propri clienti le informazioni riguardanti i propri fornitori di sistemi quando ciò è previsto dai contratti o dalle gare di

Control Domain	Question ID	Consensus Assessment Questions	ICA
Third Party Agreements	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	appalto. L'ufficio legale interno di ICA, con il supporto di consulenti esterni, valuta gli accordi contrattuali e la loro conformità agli standard e alle normative in vigore.
	STA-05.3	Does legal counsel review all third-party agreements?	
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	
	STA-05.5	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	
Supply Chain Management, Transparency, and Accountability ***Supply Chain Governance Reviews***	STA-06.1	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	I fornitori di ICA sono contrattualmente vincolati a fornire tutte le informazioni riguardanti la catena di fornitura coinvolta nell'esecuzione dei propri processi. ICA richiede le opportune certificazioni per ridurre il rischio connesso all'esternalizzazione di specifiche funzioni.
Supply Chain Management, Transparency, and Accountability ***Supply Chain Metrics***	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	ICA dispone di un apposito ufficio con la funzione di verificare il corretto svolgimento delle forniture dei servizi e dei beni da parte di fornitori esterni. L'ufficio classifica i contratti e monitora con continuità la qualità dei servizi forniti, affrontando direttamente eventuali problematiche con il fornitore. Laddove siano previsti livelli di servizio che si
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	

Control Domain	Question ID	Consensus Assessment Questions	ICA
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	ripercuotano direttamente sugli SLA cliente, l'ufficio ricollega direttamente la fornitura al cliente e si accerta del rispetto dei vincoli contrattuali.
	STA-07.4	Do you review all agreements, policies, and processes at least annually?	
Supply Chain Management, Transparency, and Accountability *Third Party Assessment*	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	ICA ha continui rapporti con i propri fornitori e mantiene costantemente condivise le informazioni necessarie allo svolgimento dei servizi nelle massime condizioni di sicurezza.
	STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	
Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	Ogni cliente abilitato all'accesso può compiere i propri *vulnerability assessment* se lo ritiene opportuno. Periodicamente anche ICA svolge questo tipo di test sui propri sistemi.
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	
Threat and Vulnerability Management*Antivirus / Malicious Software*	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	ICA utilizza i sistemi antivirus/antimalware forniti dalle più quotate aziende del settore. Tutti i sistemi sono centralizzati e monitorati tramite una console che rileva eventuali problemi con gli aggiornamenti delle definizioni o con attività di rilevazione di virus/malware positive.
	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	
Threat and Vulnerability Management *Vulnerability /*	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Periodicamente vengono condotti test di vulnerabilità secondo standard consolidati sia a livello di rete che di

Control Domain	Question ID	Consensus Assessment Questions	ICA
Patch Management	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	sistemi e applicazioni. I risultati dei test vengono utilizzati per ottimizzare il sistema e garantire la massima sicurezza. Le patch sui sistemi possono generalmente essere installate immediatamente dopo la rilevazione della vulnerabilità se messe a disposizione dal fornitore. I tempi di patch possono essere condivisi con i clienti su richiesta.
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	
	TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	
	TVM-02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	
Threat and Vulnerability Management ***Mobile Code***	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	L'esecuzione di *mobile code* non è consentita
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	