CSA Consensus

Assessments Initiative

Questionnaire

Febbraio 2018

Advanced Systems

Ver. 1.1

Revisioni

Versione	Data	Descrizione	Autore
1.0	20/12/2018	Versione iniziale	Leonello Calabresi
1.1	11/02/2019	Aggiunta sezione Termini e definizioni, in cui viene designato il CSP.	Leonello Calabresi

Avviso

Questo documento è disponibile esclusivamente a scopo informativo. Rappresenta lo stato attuale delle policy e delle procedure adottate alla data di questo documento da Advanced Systems, di seguito AS, in termini di sviluppo software e gestione del servizio di Software as a Service (SaaS).

Questo documento non costituisce alcuna garanzia, obbligazioni contrattuali, o assicurazioni verso i propri clienti. Le responsabilità di Advanced Systems verso i propri clienti sono regolate dai contratti di utilizzo dl software di cui questo documento non fa parte.

Sommario

Introduzione

La Cloud Security Alliance (CSA) è una organizzazione no-profit con la missione di introdurre best practices volte alla sicurezza delle infrastrutture di Cloud Computing. Per maggiori informazioni sull'argomento è possibile fare riferimento al seguente link https://cloudsecurityalliance.org/about/ .

Termini e definizioni

CSP: Cloud Service Provider

Ad oggi Advanced Systems ha designato Oracle Cloud come fornitore qualificato di servizi CSP. Pertanto, in questo documento tutti i riferimenti a CSP qualificati sono attribuiti ad Oracle Cloud. Oracle Cloud è stato censito nella lista dei fornitori qualificati di Advanced System in conformità con quanto previsto nel proprio manuale della qualità ISO 9001. Il sistema qualità di Advanced Systems è certificato secondo la norma UNI EN ISO 9001:2015.

Di seguito si evidenziano i principali requisiti (e relativi articoli) del GDPR che sono trattati nell'Oracle DPA (Data Processing Agreement).

Art. 28.3 GDPR - Documentare il contesto e la durata delle operazioni di data processing: La Sezione 1 del DPA descrive come si applica il nostro DPA durante l'intero periodo di esecuzione del servizio (contratto) ai dati personali che il cliente fornisce;

Art. 28.3 GDPR - Documentare le categorie di dati personali e di dati trattati dal fornitore cloud: La Sezione 4 del DPA elenca le categorie di dati personali che i clienti possono condividere con Oracle come parte della nostra vasta gamma di servizi Cloud.

Art. 28.3 GDPR - Documentare la natura e lo scopo delle operazioni di trattamento: Le sezioni 3, 5 e 13 descrivono come gestiamo i dati del cliente per fornire i servizi Cloud ordinati;

Art. 37.1 GDPR - Designazione di un responsabile della protezione dei dati: La sezione 14 del DPA fornisce le informazioni di contatto per il responsabile della protezione dei dati designato da Oracle.

Art. 28.3, 28.3.f, & 35 – 36 GDPR - Descrivere i diritti e gli obblighi del responsabile del trattamento: Le sezioni 3.1, 5.2 e 5.4 forniscono dettagli su come si mantiene il controllo dei propri dati, se si desidera che i dati vengano restituiti all'utente o cancellati in seguito alla cessazione dei servizi, per verificare ciò che Oracle sta facendo con i dati, da notificare in merito a violazioni dei dati personali o per assistere il cliente con i propri DPIA (Data Protection Impact Assessments);

Art. 28.3.b GDPR - Assicurarsi che il proprio fornitore cloud gestisca i tuoi dati in modo confidenziale: La sezione 9.3 descrive in che modo il personale che può avere accesso ai tuoi dati è soggetto a un obbligo di riservatezza.

Art. 32 e 28.3 GDPR - Assicurarsi che il proprio o fornitore cloud abbia un buon livello di sicurezza e possa anche aiutarti a soddisfare i tuoi obblighi GDPR relativi alla sicurezza: Oltre agli impegni di sicurezza descritti nella sezione 9 del nostro DPA, Oracle mette a disposizione le Hosting & Delivery Policies e le Cloud

Services Specifcations che forniscono ulteriori dettagli sui controlli di sicurezza applicabili o disponibili per i servizi Cloud.

Art. 28.3.f e 33 – 34 GDPR - Assicurarsi che il proprio fornitore di servizi cloud disponga di un programma di notifica di violazione dei dati personali e possa anche aiutarti a soddisfare i tuoi obblighi di notifica, in caso di violazione dei dati, verso le autorità di regolamentazione e gli individui coinvolti: La Sezione 11 fornisce informazioni sui controlli implementati per rilevare e rispondere agli incidenti di sicurezza che coinvolgono dati personali nel proprio ambiente cloud. Questa sezione ti informa anche sulle procedure di notifica nella misura in cui un incidente si configura come una violazione dei dati personali.

Art. 28.3.g GDPR – Assicurarsi che il proprio fornitore cloud possa eliminare o restituire i tuoi dati alla fine della fornitura dei servizi cloud: Le sezioni 12.1 e 12.2 descrivono come rendere disponibili i dati per il recupero al termine dei servizi Cloud, seguiti da una cancellazione dei dati.

Art. 28.3.g, 30.2 e 31 GDPR - Aiutarti con audit e ispezioni e fornirti tutte le informazioni necessarie a dimostrare la conformità con GDPR, compresi i registri di elaborazione: Le sezioni da 10.1 a 10.8 descrivono il processo di verifica della conformità con il DPA e impegnano la nostra assistenza per altre esigenze di conformità, quali la condivisione dei registri o la fornitura di rapporti di controllo indipendenti di terze parti che potrebbero essere disponibili per i servizi ordinati come ad esempio SOC 1Type 2, SOC 2Type 2, ISO 27001 o PCI DSS.

CSA Consensus Assessments Initiative Questionnaire

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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)?	Il ciclo dello sviluppo del software di AS incorpora le best practices del settore, include verifiche formali della sicurezza del software in tutte le fasi di progettazione. Di tali verifiche è responsabile un team specifico (Security Team). AS pone in essere nei propri processi procedure in linea con gli standard ISO 9001 e ISO 27001 la cui compliance è certificata da organismi esterni di audit. Per ulteriori dettagli sui controlli in essere si rimanda alla matrice di applicabilità del ISMS di AS.
	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?	L'accesso ai dati, agli asset, e alle soluzioni applicative viene fornito ai clienti in linea con quanto previsto dalla compliance con il GDPR 679/2016.
	AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	I controlli di integrità dei dati vengono gestiti in tutte le fasi di processamento del dato incluse quelle computazionali, di trasmissione e memorizzazione su archivi di massa. In aggiunta è possibile fare riferimento ai verbali degli audit ISO 9001 e ISO 27001.
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'architettura per la sicurezza dei dati di AS è progettata incorporando i migliori standard e best practices del settore. Per ulteriori dettagli è possibile fare riferimento alle certificazioni ISO 9001 e ISO 27001 di AS.
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.)?	AS è soggetta ad audit di terze parti che sono in grado di attestare la validità delle proprie certificazioni.
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?	AS è in grado di fornire attestazioni di terze parti a riguardo delle proprie certificazioni. I verbali di audit possono essere visionati dai clienti su richiesta. Il certificato relativo alla ISO 27001 può essere scaricato dal sito di AS. AS effettua la scansione delle vulnerabilità di tutti gli endpoint collegati ad Internet ad intervalli regolari. Il team addetto alla sicurezza di AS è in grado di notificare i propri clienti e fornitori riguardo a possibili
	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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	vulnerabilità in essere e ai relativi rimedi da applicare. In aggiunta, vengono effettuati da terze parti assessment esterni riguardo alla sicurezza delle infrastrutture, volti a scoprire possibili vulnerabilità. I report e le raccomandazioni che risultano da questi assessment vengono recepiti da AS e comunicati al management aziendale. L'infrastruttura dei servizi di AS è soggetta anche ad audit interni e risk assessment periodici.
	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 Regulatory Mapping*	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?	Tutti i dati gestiti negli applicativi offerti in modalità SaaS prevedono un alto livello di isolamento e sicurezza delle istanze tra i diversi clienti. Ciò viene garantito dai CSP qualificati a cui AS fa riferimento per il servizio di IaaS e PaaS. AS utilizza meccanismi di crittografia dei dati sia in fase di trasmissione (Tunnel IPSec, VPN, https) che di memorizzazione messi a disposizione dai propri CSP qualificati. AS effettua backup giornalieri dei dati gestiti all'interno dei propri applicativi.
	AAC-03.2	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	
	AAC-03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	AS utilizza fornitori CSP i cui data center sono localizzati in Italia o in altri paesi della Comunità Europea.
	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?	AS effettua un monitoraggio costante delle leggi vigenti e dei regolamenti in materia di sicurezza delle informazioni. Per ulteriori dettagli è possibile fare riferimento ai manuali ISO 9001 e ISO 27001. AS opera in linea con il vigente GDPR ed è allineata agli standard ISO 9001 e 27001 come attestato dagli organismi di certificazione indipendenti.
Business Continuity	BCR-01.1	Do you provide tenants with	AS installa le proprie applicazioni

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
Management & Operational Resilience *Business Continuity Planning*		geographically resilient hosting options?	presso CSP qualificati i cui servizi hanno le caratteristiche di resilienza e failover previsti dalla qualifica.
	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 policy e le procedure di Business Continuity di AS sono state sviluppare e verificate in linea con gli standard ISO 27001.
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?	I data center dei CSP fornitori di AS sono fisicamente collocati in Italia o in Paesi dell'Unione Europea. AS installa le proprie applicazioni presso CSP qualificati i cui servizi hanno le caratteristiche previste dalla qualifica.
	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?	La documentazione tecnica dei sistemi informativi e dei servizi messi a disposizione dai CSP qualificati a cui AS fa riferimento è disponibile internamente al personale di AS in linea con quanto previsto dalla propria certificazione ISO 27001.
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 data center dei CSP su cui AS installa i propri applicativi incorporano le necessarie misure di resilienza previste dalla qualifica.
Business Continuity Management & Operational Resilience *Equipment Location*	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.)?	I data center dei CSP su cui AS installa i propri applicativi incorporano le necessarie misure di resilienza previste dalla qualifica.

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	I data center dei CSP su cui AS installa i propri applicativi incorporano le necessarie misure di resilienza previste dalla qualifica.
	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.)?	I data center dei CSP su cui AS installa i propri applicativi incorporano le necessarie misure di resilienza previste dalla qualifica.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	I data center dei CSP su cui AS installa i propri applicativi incorporano le necessarie misure di resilienza previste dalla qualifica.
	BCR-09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	
	BCR-09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	AS è in grado di fornire su richiesta ai propri clienti i report relativi alle prestazioni delle SLA dei CSP su sono installati gli applicativi in SaaS.
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?	AS ha definito le proprie policy e procedure basandosi sugli standard ISO 27001, ISO 27017, ISO 27018, ISO.

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	Per motivi di sicurezza AS non consente ai propri clienti di intervenire direttamente sui database utilizzati dalle applicazioni fornite in SaaS. Tuttavia, su richiesta del cliente, delle autorità o di terze parti, esistono procedure documentate per mettere a disposizione i dati presenti nei propri archivi, nonché la cancellazione degli stessi.
	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?	I CSP qualificati presso i quali AS installa i propri applicativi mettono a disposizione meccanismi di backup e ridondanza in linea con i requisiti previsti dalla qualifica.
	BCR-11.5	Do you test your backup or redundancy mechanisms at least annually?	
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?	AS ha definito opportune policy e procedure basandosi sugli standard ISO 27001, ISO 27017, ISO 27018, ISO 9001.
	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?	AS non affida a società esterne lo sviluppo di software. AS incorpora standard di qualità e sicurezza come parte integrante del proprio processo di sviluppo del software (SDLC). Per ulteriori dettagli consultare i manuali delle certificazioni ISO 9001 e ISO 27001.
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	
Change Control & Configuration *Management Quality Testing*	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	AS detiene la certificazione ISO 9001. Tale certificazione è di fatto una validazione di terzi dei processi di sviluppo del software in ottemperanza con lo standard ISO 9001.
	CCC-03.2	Is documentation describing known issues with certain products/services available?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	AS ha in essere opportune procedure per comunicare ai propri clienti problemi riguardanti la sicurezza dei dati ed eventuali vulnerabilità dei propri applicativi. Il processo di sviluppo del software (SDLC) di AS incorpora le best practice del settore e prevede riesami formali da parte di un team dedicato alla sicurezza e all'analisi del rischio. Per maggiori dettagli consultare i manuali delle certificazioni ISO 9001 e ISO 27001.
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	
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?	AS ha definito procedure specifiche per controllare l'installazione del software ed individuare software malevolo in linea con gli standard ISO 27001. La compliance di AS agli standard ISO 27001 è stata certifica e validata da organismi indipendenti riconosciuti a livello internazionale.
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?	Su richiesta è possibile avere informazioni descrittive sulla procedura di change management adottata da AS.
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)?	AS utilizza data center di CSP qualificati presso i quali è possibile configurare le risorse da utilizzare.
	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?	AS utilizza CSP qualificati in grado di fornire l'accesso ai servizi SaaS in base all'indirizzo IP. Ai clienti viene messo a disposizione l'autenticazione mediante utente e password su trasporto SSL.

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	AS utilizza CSP qualificati in grado di fornire flessibilità in merito alle istanze degli applicativi ed alla collocazione dei database in più regioni geografiche all'interno dell'Unione Europea.
	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)?	AS prevede un Sistema di etichettatura/classificazione dei dati all'interno delle proprie procedure ISO 27001.
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	AS utilizza CSP qualificati in grado di fornire flessibilità in merito alle regioni fisiche in cui sono localizzati i server su cui vengono installati gli applicativi in SaaS. I clienti verranno informati delle regioni in cui sono situati i server e dell'eventuale spostamento degli stessi in altre aree geografiche
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?	AS utilizza CSP qualificati in grado di fornire informazioni sulla collocazione fisica delle risorse e sul loro eventuale spostamento in ottemperanza a quanto previsto dalla qualifica di CSP.
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	
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)?	AS utilizza CSP qualificati in grado di consentire l'accesso alle infrastrutture cloud in modalità sicura (SSH, VPN).
	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	DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	AS utilizza CSP qualificati in grado di consentire il controllo e ownership dei dati nonché la loro classificazione secondo proprie procedure che

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
Handling / Labeling / Security Policy	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	soddisfano i requisiti previsti dalla ISO 27001.
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?	AS utilizza CSP qualificati in grado di consentire il controllo e la separazione dei dati di produzione da quelli di test.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	Come SaaS e processore dei dati si rimanda ai contratti stipulati con i clienti.
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?	AS utilizza CSP qualificati in grado di assicurare la cancellazione sicura dei dati di backup in caso di dismissione del servizio o sostituzione dello storage.
	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?	AS utilizza CSP qualificati i cui data center sono gestiti in linea con i criteri di sicurezza previsti dagli standard ISO 27001.
	DCS-01.2	Do you maintain a complete inventory of all of your critical supplier relationships?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	
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?	
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)?	
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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	
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)?	
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?	
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?	AS consente ai propri clienti di utilizzare in autonomia i propri certificati digitali per stabilire connessioni sicure in modalità https o mediante VPN. AS è in grado di fornire ai propri clienti le proprie chiavi pubbliche per trasferire in maniera sicura chiavi di crittografia simmetriche nell'utilizzo dei servizi su connessioni https e VPN. Internamente AS gestisce chiavi crittografiche per i dipendenti che
Encryption & Key Management *Key Generation*	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	
	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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	hanno accesso ai servizi presso i CSP. All'interno di AS è definita una CA per distribuire le chiavi dei certificati X.509. I processi di rilascio dei certificati vengono riesaminati periodicamente in conformità con la certificazione ISO 27001.
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	
Encryption & Key Management *Encryption*	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	AS utilizza CSP qualificati in grado di fornire servizi di crittografia dei dati presenti nei database e sul file system.
	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?	AS utilizza CSP qualificati in grado di fornire servizi di crittografia e gestione delle chiavi simmetriche e asimmetriche. I processi di gestione dei certificati vengono riesaminati periodicamente in conformità con la certificazione ISO 27001.
	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	Risposta di Advanced Systems
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.)?	In linea con gli standard ISO 27001, AS gestisce delle baseline per i componenti critici dei propri sistemi. AS è stata validata e certificata da un ente accreditato indipendente allineato allo standard ISO 27001. AS non prevede che i propri clienti forniscano delle macchine virtuali proprie da importare sulle infrastrutture dei CSP su cui vengono installi gli applicativi AS.
	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)?	AS utilizza CSP qualificati in grado di fornire report ed altre informazioni riguardanti i processi, le policy, ed i controlli in essere nella fornitura della infrastruttura cloud.
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	In linea con lo standard ISO 27001, AS prevede un programma di gestione del rischio e sua mitigazione. La certificazione ISO 27001 include controlli estesi previsti nelle linee guida ISO 27018.
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?	Il controllo delle risorse in AS comincia al più alto livello del management. Tutti i ruoli all'interno dell'azienda prevedono formazione continua e condivisione delle politiche relative alla sicurezza a cadenza annuale.
Governance and Risk Management *Management Program*	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	AS rende disponibile per la visione sul il proprio sito il certificato ISO 27001. Il manuale del sistema ISMS è disponibile su richiesta.

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	La certificazione ISO 27001 è rilasciata da un ente indipendente accreditato. Annualmente AS conduce un audit interno ed un audit esterno eseguito da parte dell'ente certificatore. Ogni anno AS conduce un riesame della direzione che include lo stato del sistema ISMS.
Governance and Risk Management *Management Support / Involvement*	GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	AS gestisce una lista dei fornitori qualificati che include i CSP di riferimento per le infrastrutture che ospitano gli applicativi forniti in SaaS. I CSP qualificati devono prendere visione delle policy di AS in merito alla sicurezza delle informazioni ed alla privacy.
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.)?	AS ha definito un sistema per la sicurezza delle informazioni (ISMS) e delle opportune policy che sono state integrate nel manuale ISO 27001 con annessi i controlli previsti dalle linee guida ISO 27002. AS gestisce i rapporti con le terze parti in linea con gli standard ISO 27001.
	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?	
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?	AS distribuisce le proprie policy relative alla sicurezza a tutto il personale e provvede al loro addestramento in materia in funzione dei ruoli e delle responsabilità. I dipendenti che violano gli standard e i protocolli di sicurezza di AS possono essere soggetti ad azioni disciplinari e sanzioni. La certificazione ISO 27001 di AS è stata validata e certificata da un ente accreditato indipendente.
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	Aggiornamenti alle politiche di sicurezza, alle procedure, agli standard e controlli avvengono su base annuale in conformità con lo standard ISO 27001.
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?	I client vengono informati attraverso il sito istituzionale di AS ed a mezzo mail in relazione a modifiche che riguardano le policy sulla sicurezza delle informazioni e la privacy.
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	Le policy sulla sicurezza delle informazioni e sulla privacy vengono riesaminate annualmente a seguito degli audit interni ed esterni.
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?	In linea con lo standard ISO 27001 AS ha sviluppato un programma di gestione e mitigazione del rischio. Tale programma è illustrato nel manuale ISO 27001 disponibile su richiesta del cliente.
	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)?	
Governance and Risk Management *Program*	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	In linea con lo standard ISO 27001 AS ha sviluppato un programma di gestione e mitigazione del rischio. Tale programma è illustrato nel manuale ISO 27001 disponibile su richiesta del cliente.
	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?	I clienti di AS hanno la responsabilità di monitorare i propri sistemi in merito alla privacy. AS monitora le risorse sotto il proprio controllo e produce dei report periodici che possono essere richiesti dai propri clienti.
	HRS-01.2	Is your Privacy Policy aligned with industry standards?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	AS effettua dei controlli pre-assunzione nei termini consentiti dalla legge.
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?	In linea con lo standard ISO 27001, tutto il personale di AS deve completare un addestramento periodico di tipo role-based che include la sicurezza delle informazioni e prevede una verifica finale. Audit di compliance vengono effettuati internamente e periodicamente per verificare l'applicazione delle policy. Tutto il personale di AS deve firmare un accordo di riservatezza prima di ricevere l'accesso alle risorse. In aggiunta, prima dell'assunzione il personale deve leggere e firmare l'accettazione di una Acceptable Use Policy e di un Codice di Condotta.
	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?	
	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?	Il processo di gestione delle risorse umane prevede procedure di chiusura delle utenze dei dipendenti e di adeguamento delle autorizzazioni a secondo dei ruoli.
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	L'accesso alle risorse viene revocato quando un dipendente termina la propria posizione contrattuale. Quando le funzioni o il ruolo di un dipendente vengono modificate l'accesso alle risorse deve essere esplicitamente approvato.

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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 clienti hanno la responsabilità di controllare la sicurezza dei propri dispositivi mobile.
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?	Le politiche ed i termini contrattuali di non divulgazione e confidenzialità vengono periodicamente riesaminati dall'ufficio legale.
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?	Ai clienti viene fornita la documentazione di compliance al GDPR in vigore.
Human Resources *Acceptable Use*	HRS-08.1	Do you provide documentation regarding how you may access tenant data and metadata?	AS adotta una politica di controllo formale in merito a scopi, ruoli e responsabilità nell'acceso ai dati e metadati degli applicativi forniti in SaaS in conformità con il GDPR e alla ISO 27001 ed alle linee guida introdotte nella ISO 27018.
	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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	In linea con lo standard ISO 27001, tutti i dipendenti di AS devono completare un addestramento periodico in relazione alla sicurezza delle informazioni alla fine del quale è prevista una verifica. Audit di sorveglianza interni ed esterni sono previsti periodicamente per verificare che i dipendenti abbiano compreso i propri ruoli e responsabilità.
	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?	AS ha implementato vari metodi di comunicazione interna per aiutare i dipendenti a comprendere i propri ruoli e responsabilità ed a comunicare gli eventi in tempi rapidi. Questi metodi includono programmi di orientamento e addestramento per i nuovi assunti, e messaggi di posta elettronica con aggiornamenti periodici a tutti i dipendenti. Tutto ciò in linea con quanto previsto dallo standard ISO 27001.
	HRS-10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	
	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?	Le politiche di gestione dei dati di AS sono in linea con lo standard ISO 27001. AS è stata certificata e validata da un ente accreditato indipendente. AS utilizza CSP qualificati in grado di fornire registrazioni di audit contenenti le informazioni necessarie a condurre analisi dei dati in risposta ad eventi riguardanti la sicurezza.
	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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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.)?	In linea con gli standard ISO 27001, AS ha stabilito delle policy e procedure per delineare gli standard minimi di accesso logico alle risorse. Queste informazioni sono disponibili nei manuali del sistema di gestione della Sicurezza delle Informazioni (ISMS) definito per la ISO 27001.
	IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	Gli applicativi forniti in modalità SaaS prevedono il log di tutte le operazioni sui dati effettuate dagli utenti. Sono previsti anche meccanismi di alert per gli eventi scaturiti da operazioni effettuate dagli utenti amministratori. Il monitoraggio dei processi e l'accesso ai log viene regolato in conformità con gli standard della ISO 27001.
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?	I dettagli relativi alle modalità di revoca degli accessi agli utenti sono specificati all'interno del manuale ISMS relativo alla ISO 27001.
	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?	AS ha in essere specifici controlli per limitare l'accesso ai sistemi e ai dati e per garantire che l'accesso ai sistemi e ai dati è monitorato. I dati dei clienti residenti sulle infrastrutture dei CSP sono tenuti logicamente isolati gli uni dagli altri, così come le istanze dei server a loro dedicati.
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?	
	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	Risposta di Advanced Systems
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?	AS utilizza CSP qualificati che consentono di gestire la segregazione delle risorse.
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?	In linea con gli standard ISO 27001, AS ha stabilito policy e procedure per delineare gli standard minimi per l'accesso alle risorse.
	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?	AS utilizza CSP qualificati in grado di offrire flessibilità, continuità del servizio e ridondanza utilizzando data center in diverse zone dell'Unione Europea. Le politiche di backup e disaster recovery sono definite all'interno del manuale ISO 27001 disponibile su richiesta dei clienti.
	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?	
	IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	
	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?	I CSP qualificati utilizzati da AS consentono il controllo e l'ownership dei dati e prevedono che le istanze dei server su cui sono installati gli applicativi in SaaS siano logicamente isolate.
	IAM-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	Vengono definiti identificativi utenti univoci per l'accesso agli applicativi. La creazione degli account utente, l'abilitazione dei dispositivi e degli IP utilizzati per l'accesso alle piattaforme applicative è soggetta a processo di approvazione.
	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?	AS non consente l'accesso diretto alle infrastrutture cloud che ospitano i propri applicativi in SaaS.
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)?	In linea con lo standard ISO 27001, tutti i diritti di accesso vengono riesaminati periodicamente; l'accesso alle risorse viene revocato automaticamente in mancanza del rinnovo dell'approvazione. I report di audit delle ispezioni relative alla ISO 27001 possono essere resi disponibili ai clienti su richiesta.
	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?	L'accesso ai sistemi che ospitano gli applicativi in SaaS viene automaticamente revocato quando un dipendente termina il proprio rapporto di lavoro e avvengono delle modifiche alla posizione contrattuale e ai ruoli di quest'ultimo.

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	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?	
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?	L'accesso alle infrastrutture che ospitano gli applicativi in SaaS viene controllato attraverso i meccanismi gestiti dai CSP qualificati a cui AS fa riferimento.
	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?	AS utilizza CSP qualificati in grado di fornire meccanismi di accesso sicuro ai sistemi che ospitano gli applicativi in SaaS.
	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	Risposta di Advanced Systems
	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?	AS utilizza CSP qualificati che sono in linea con gli standard ISO 27001, le utilità di sistema operanti sul cloud vengono opportunamente monitorate e controllate.
	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?	AS utilizza CSP qualificati che in ottemperanza agli standard della ISO 27001 sono in grado fornire programmi adeguati di risposta agli incidenti che riguardano la sicurezza delle informazioni sulle proprie infrastrutture di virtualizzazione.
	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?	
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	
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)?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	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?	
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?	
	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?	
	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)?	
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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	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?	
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?	
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	
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?	
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, and contractual requirements?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	
	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?	
	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)?	
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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	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)?	
	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?	
	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?	
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?	I dettagli riguardanti le API di interoperabilità sono reperibili sul sito istituzionale di AS http://www.advancedsystems.it

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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)?	In linea con gli standard ISO 27001, AS ha stabilito delle policy formali e procedure per delineare gli standard minimi di accesso alle API dei propri applicativi.
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?	
	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?	I clienti possono accedere, su richiesta, alle proprie banche dati all'interno di specifiche aree destinate alla migrazione delle stesse.
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?	Gli applicativi in SaaS prevedono anche l'utilizzo di utility per l'importazione ed esportazione dei dati. Tali utility sono disponibili in conformità con gli standard ISO 27001.
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	
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?	AS utilizza CSP qualificati in linea con gli standard di interoperabilità e portabilità relativi alla virtualizzazione.
	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?	AS utilizza procedure e processi per la gestione del malware in linea con gli standard ISO 27001.

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	AS ha definito un proprio sistema per la sicurezza delle informazioni e delle policy che sono identificabili all'interno dei controlli delle linee guida ISO 27002 all'interno del proprio sistema di gestione della sicurezza delle informazioni certificato con lo standard ISO 27001.
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?	
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?	
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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	
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?	I client hanno il controllo e la responsabilità dei dati associati ai loro asset personali. È responsabilità dei clienti gestire la sicurezza dei propri dispositivi mobile e del loro contenuto.
	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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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)?	
	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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	
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?	
	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?	In termini di sicurezza delle informazioni, AS è in contatto con le organizzazioni e le autorità necessarie come previsto dalla compliance allo standard ISO 27001.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02.1	Do you have a documented security incident response plan?	Il program di risposta agli incidenti di AS, i piani e le procedure, sono stati sviluppati in conformità con lo standard ISO 27001. AS è stata validata e certificata in linea con lo standard ISO 27001 da un ente accreditato indipendente.
	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?	
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	
	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 metriche di sicurezza sono monitorate e analizzate da AS in conformità con lo standard ISO 27001.
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	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 processati da AS è controllata mediante opportune routine di validazione degli input nei propri applicativi. I dati migrati da forniture esterne devono essere preventivamente validati dal fornitore. L'accesso alle forniture esterne di dati da migrare viene preventivamente autorizzato e controllato secondo le procedure definite e le policy definite nell'ambito del proprio sistema per la gestione della sicurezza delle informazioni per il quale AS è certificata in conformità con la ISO 27001.
	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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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)?	Il sistema di risposta agli incidenti di AS, i piani e le procedure sono stati sviluppati in linea con lo standard ISO 27001.
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?	AS utilizza CSP qualificati in grado di fornire informazioni in linea con lo standard ISO 27001.
	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?	Il settore approvigionamenti di AS gestisce le relazioni con i fornitori. In linea con lo standard ISO 27001, AS ha validato e certificato i propri fornitori. Tra As ed i fornitori di servizi cloud (CSP) vengono firmati accordi reciproci di non divulgazione.
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	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?	
	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	
	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?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	AS definisce accordi formali con fornitori di servizi Cloud e terze parti e gestisce meccanismi di comunicazione appropriati in linea con lo standard ISO 27001.
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)?	
	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)?	
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	
	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?	
	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?	AS non consente di effettuare vulnerability assessment indipendenti sulle infrastrutture dei CSP che ospitano i propri applicativi in SaaS.
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	

Control Domain	Question ID	Consensus Assessment Questions	Risposta di Advanced Systems
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?	I processi e le procedure di AS per la gestione dei software anti malware sono in linea con gli standard ISO 27001.
	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 / Patch Management*	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	AS controlla periodicamente i sistemi operativi e software applicativi installati sulle infrastrutture cloud dei CSP utilizzati. Vengono effettuate scansioni periodiche delle vulnerabilità e applicate le necessarie patch, nonché gli aggiornamenti di sistema. Tutto ciò in linea con quanto previsto dallo standard ISO 27001 e annessi controlli. Nel caso determinate vulnerabilità coinvolgano anche i propri clienti AS darà pronta notifica delle stesse e dei relativi rimedi da utilizzare.
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	
	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?	AS non prevede l'installazione di applicazioni mobile di terze parti sulle infrastrutture che ospitano i propri applicativi in SaaS.
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	