ZUCCHETTI SPA

ultimo aggiornamento gennaio 2019

CAIQv3.1 ZUCCHETTI

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			La progettazione, sviluppo, commercializzazione, installazione, erogazione, formazione, assistenza e manutenzione di prodotti SW e servizi saas sono attività realizzate seguendo le linee guida della certificazione ISO9001 e ogni sviluppo viene realizzato previa analisi progettuale di privacy by design in conformità allo standard BS10012.
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			Zucchetti segue un processo di sviluppo e rilascio di prodotti SW strutturato. Come parte di questo processo il codice viene revisionato prima del rilascio. Zucchetti mette a disposizione all'interno della propria suite strumenti di analisi del codice appositamente sviluppati sulla base delle best practice del settore. Inoltre Zucchetti esegue test VAPT post-rilascio su ambienti appositamente predisposti.
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	X			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?			X	Zucchetti non affida a partner lo sviluppo della Suite Zucchetti Infinity.
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Zucchetti segue un processo di sviluppo e rilascio di prodotti SW strutturato. Come parte di questo processo il codice viene revisionato prima del rilascio. Zucchetti mette a disposizione all'interno della propria suite strumenti di analisi del codice appositamente sviluppati sulla base delle best practice del settore. Inoltre Zucchetti esegue test VAPT post-rilascio su ambienti appositamente predisposti. Inoltre c'è un processo di controllo qualità definito in procedure Iso9001 che definisce che le modifiche realizzate siano efficaci rispetto alle analisi e agli sviluppi effettuati.
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			I clienti accettano le regole contrattuali con gli sla definiti. I clienti possono in ogni momento accedere ai loro dati e Zucchetti, in qualità di responsabile del trattamento dati, aiuta il Titolare nell'accesso alle proprie informazioni.
		AIS-02.2		Are all requirements and trust levels for customers' access defined and documented?	X			I diritti di accesso ai dati degli utenti e le configurazioni di accesso sono definite a livello software e salvate in tabelle dedicate il cui contenuto può essere estratto in formato .csv. L'utente amministratore non vede nulla di default e deve essere attivato il relativo profilo di autorizzazione
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			Tutte le operazioni sono in transazione e quindi l'integrità è garantita dal fatto che la transazione vada a buon fine
		AIS-03.2		Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			Il Datacenter Zucchetti effettua controlli di integrità sui dati salvati sui propri sistemi di backup per garantire la disponibilità e il ripristino dei dati, ove previsti in contratto, come parte dei processi Zucchetti in standard ISO 27001. La garanzia dell'integrità dei dati viene garantita anche dal software stesso che esegue le elaborazioni secondo standard normativi verificati e testati.

Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			L'architettura è stata progettata con l'intenzione di dimostrare la rispondenza agli standard di sicurezza sulla gestione delle informazioni della certificazione ISO 27001 e BS10012. In particolare rispetto al CSA Trusted Cloud Architectural Standard sono state sviluppate le seguenti procedure, finalizzate: alla gestione del rischio e alla determinazione della conformità legislativa; alla gestione sicura dei dati; alla gestione degli accessi privilegiati all'infrastruttura e alle applicazioni; all'implementazione di procedure di verifica delle vulnerabilità e a test di violazione, alla sicurezza dell'infrastruttura che eroga i servizi, alla protezione dei dati; alla gestione delle politiche e degli standard di processo. I processi di gestione sono definiti secondo le logiche Iso27002, in particolare sono definite le competenze di coloro che erogano il servizio e le caratteristiche per l'erogazione e la continuità dello stesso. E' prevista una struttura che eroga servizi e assiste i clienti nel risolvere i problemi che dovessero presentarsi. Sono sviluppate procedure per la gestione degli incidenti, per la gestione e sviluppo delle competenza, per la formazione delle persone affinchè l'incidente non si verifichi più. Ci sono procedure per la gestione dei cambiamenti e per la gestione delle release e delle patch applicative. Nei confronti dei fornitori terzi ci sono procedure di qualifica, audit e di assunzioni di obbligazioni contrattuali e di responsabilità applicati. I dati personali sono controllati sia nell'input che nell'output e chi può importare o esportare è censito con appositi profili di autorizzazione. Sono sviluppate procedure per incrementare la competenza delle persone e per la loro formazione. Ci sono uffici dedicati, quali l'ufficio sicurezza it, l'ufficio legale e l'ufficio privacy e qualità che operano in modo indipendente per portare i processi tra gli sviluppatori e ne controllano l'implementazione. Al fine di facilitare i clienti nella valutazione del prodotto sono sviluppati ambienti di prova in cui possono testare le procedure e le sicurezze. Ci sono cicli di vita del software applicati che sono finalizzati al termine con politiche di migrazione a strumenti nuovi e aggiornati. Per quanto riguarda le interfacce di integrazione
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	X			Per il Datacenter Zucchetti sono pianificati, ad intervalli regolari, audit (interni ed esterni) per verificare l'efficacia e l'efficienza dei controlli di sicurezza implementati
		AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?	X			In Zucchetti è stato predisposto un sistema di audit interno in interazione tra i vari sistemi, regolato dalle disposizioni della ISO 27001 9001 e BS10012.
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			Zucchetti mette a disposizione dei clienti i report delle certificazioni ISO 9001, BS10012 scaricabili da proprio sito http://www.zucchetti.it/website/cms/be-zucchetti/6497-certificazioni.html
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			Zucchetti effettua annualmente scansioni regolari di tutti gli indirizzi IP degli endpoint gestiti sulle reti private e connesse a internet in Datacenter per individuare e gestire le eventuali vulnerabilità come parte dei processi della ISO27001.
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Zucchetti commissiona a società indipendenti, operanti nel settore della cybersecurity, attività di WAPT su ambienti appositamente predisposti in Datacenter.
		AAC-02.4		Do you conduct internal audits at least annually?	X			Gli audit sono effettuati internamente con cadenza annuale
		AAC-02.5		Do you conduct independent audits at least annually?	X			Sì, sono effettuati audit annualmente su ambienti di test e macchine dedicate da un ente esterno ed indipendente
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	X			Zucchetti ottiene le certificazioni sulla gestione della sicurezza delle informazioni da strutture di terze parti indipendenti. A richiesta può fornire il public report executive e l'elenco dei controlli di sicurezza delle attività di WAPT
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	X			

Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			Tutte le modifiche normative che possono influire su particolari funzionalità degli applicativi sono monitorate dai team di gestione delle compliance normative. Questi interegiscono all'interno di Zucchetti per garantire la conformità con le leggi in vigore italiane e delle comunità europea. L'ambito di aggiornamento è definito contrattualmente.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			Il BC ed il DR plan sono stati redatti in linea con le direttive ISO27001
		BCR-01.2		Do you have more than one provider for each service you depend on?	X			Il datacenter Zucchetti è configurato in un'ottica di disaster recovery dividendosi su siti differenti di erogazione in modo da poter reagire agli eventuali eventi inattesi. Le diverse situazioni sono valutate e gestite direttamente dal personale tecnico Zucchetti che metterà in atto le relative procedure atte alla minimizzazione del disagio. Il disaster recovery viene attivato qualora il contratto lo preveda ed insieme al cliente è possibile configurare diversi livelli di recovery con sisti di ripristino ubicati a diverse distanze rispetto a quello di produzione. Il piano di DR viene condiviso con i clienti a richiesta degli stessi.
		BCR-01.3		Do you provide a disaster recovery capability?	X			
		BCR-01.4		Do you monitor service continuity with upstream providers in the event of provider failure?	X			
		BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?	X			
		BCR-01.6		Do you provide a tenant-triggered failover option?	X			
		BCR-01.7		Do you share your business continuity and redundancy plans with your tenants?	X			
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Il Datacenter Zucchetti effettua annualmente i test di disaster recovery simulando scenari di discontinuità operativa. A livello applicativo Zucchetti opera su tutto il territorio nazionale con figure di backup per ogni sviluppo e funzione applicativa. Almeno ogni anno sono effettuate prove di ripristino di sistemi applicativi. Le prove sono effettuate in ambiente di test
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	X			Nel Datacenter Zucchetti sono state adottate diverse misure per il monitoraggio e la sicurezza dell'infrastruttura, in linea con quanto stabilito dalla certificazione ISO27001
		BCR-03.2		Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	X			Zucchetti rende dispobili, a richiesta del Cliente, diversi livelli di recovery con siti di ripristino a distanze diverse rispetto al sito di produzione
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			La documentazione viene fornita ai tecnici e addetti che hanno necessità di accedere alle informazioni per lo svolgimento delle loro attività professionali. La pertinenza del trattamento è valutata su un'apposita lettera di incarico.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical damage anticipated and are countermeasures included in the design of physical protections?	X			I siti di data center gestiti da Zucchetti sono costruiti in base alle norme nazionali e locali. Tutte le contromisure sono state messe in atto al fine di limitare gli effetti di eventuali danni.
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		X		i luoghi in cui sono ubicati i data center sono rischio sismico 3 e sono lontani da corsi di fiumi o mari. Sono costruiti secondo le regole costruttive del luogo in cui si trovano.
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	X			Tutte le procedure relative alle attività di gestione e manutenzione dell'infrastruttura di Datacenter sono documentate all'interno di procedure specifiche certificate ISO27001
		BCR-07.2		Do you have an equipment and datacenter maintenance routine or plan?	X			
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			Il Datacenter Zucchetti si appoggia a differenti provider di connettività internet per limitare i rischi di "network disruptions". I sistemi relativi all'erogazione del servizio SAAS sono progettati e realizzati in modalità ridondante, inoltre, sono state realizzate le best practice del settore al fine di prevenire possibili malfunzionamenti.

Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			Per ogni implementazione, Zucchetti esegue un'analisi di impatto (BIA) come da standard ISO27001 al fine di prevenire eventuali interruzioni ai servizi di Datacenter
		BCR-09.2		Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			Tutte le policy e le procedure sono rese disponibili al personale in base ai singoli ruoli, le regole seguono gli standard relativi all'ISO 9001 e BS10012.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical capabilities to enforce tenant data retention policies?		X		Zucchetti come parte del processo BS10012 effettua controlli sulla data retention. La data retention del servizio è standard e definita contrattualmente.
		BCR-11.2		Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	X			Le policy e le procedure che riguardano il periodo di conservazione dei dati sono descritte sia a livello contrattuale che all'interno del registro dei trattamenti, disponibile a richiesta per ogni Cliente
		BCR-11.3		Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			Zucchetti assicura l'aderenza alle normative vigenti tramite l'implementazione di procedure di backup e meccanismi di recovery
		BCR-11.4		If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?		X		La gestione dell'infrastruttura relativa all'erogazione del servizio SaaS è interamente in carico a Zucchetti
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?		X		
		BCR-11.6		Does your cloud solution include software/provider independent restore and recovery capabilities?		X		
		BCR-11.7		Do you test your backup or redundancy mechanisms at least annually?	X			Zucchetti verifica regolarmente l'efficacia del proprio processo di backup
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			Zucchetti ha messo in atto procedure di change per la gestione di nuovi sviluppi relativi alle risorse. Zucchetti ha messo in atto procedure per verificare la privacy by design delle nuove applicazioni/servizi secondo lo standard BS10012. Per ogni applicativo saas è disponibile il manuale di utilizzo e installazione in lingua italiana
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?			X	Tutte le modifiche relative all'erogazione del servizio o alle versioni implementate degli applicativi in uso sono comunicate tramite apposita documentazione pubblicata sul sito Zucchetti. Non vengono utilizzati partner per lo sviluppo degli applicativi o per l'erogazione dei servizi di Datacenter
		CCC-02.2		Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?			X	
Change Control & Configuration Management *Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			Tutti i processi di controllo e test dei cambiamenti sono definiti al fine di garantire integrità, confidenzialità e disponibilità dei dati come da standard ISO27001
		CCC-03.2		Is documentation describing known issues with certain products/services available?	X			Zucchetti adotta processi e procedure in ambito ISO 9001, ISO 27001, BS10012 e ulteriori linee guida per la gestione delle componenti dei servizi erogati. C'è un ufficio che si occupa delle comunicazioni verso i clienti in modo che siano aggiornati rispetto ai nuovi problemi di sicurezza e ai contenuti degli aggiornamenti. Ogni nuova versione è testata da addetti al controllo qualità che verificano che non vi siano bug applicativi o che non vi siano dati di test inseriti nella release. Qualora vi sia un bug di procedura la segnalazione arriva in assistenza che verifica la non conformità e passa l'informazione alla programmazione che risolve il problema, lo passa al controllo qualità che verifica l'impatto prima di rilasciare la release ai clienti. La release viene installata su tutti i clienti.
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			

		CCC-03.4		Do you have controls in place to ensure that standards of quality are being met for all software development?	X			Gli standard di qualità sono assicurati dalle procedure riportate nella certificazione ISO 9001 e BS10012.
		CCC-03.5		Do you have controls in place to detect source code security defects for any outsourced software development activities?			X	Zucchetti non affida a terzi la realizzazione di codice per i propri prodotti.
		CCC-03.6		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			Ogni nuova versione è testata da addetti al controllo qualità che verificano che non vi siano bug applicativi o che non vi siano dati di test inseriti nella release. Qualora vi sia un bug di procedura la segnalazione arriva in assistenza che verifica la non conformità e passa l'informazione alla programmazione che risolve il problema, lo passa al controllo qualità che verifica l'impatto prima di rilasciare la release ai clienti. La release viene installata su tutti i clienti.
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			Zucchetti ha messo a punto procedure e processi per monitorare ed evitare l'installazione di SW non autorizzato sui sistemi gestiti dai Sistemi IT interni. Ogni software deve essere autorizzato con la sua valutazione e inserimento nella white list.
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	X			Zucchetti adotta per i servizi erogati in regime di Saas procedure e processi per la gestione del Change Management. Tali procedure sono consegnate ai clienti solo su richiesta.
		CCC-05.2		Do you have policies and procedures established for managing risks with respect to change management in production environments?	X			Zucchetti adotta per i servizi erogati in regime di Saas procedure e processi per la gestione del Change Management. I change sono effettuati nel rispetto degli SLA contrattualizzati, analizzando i possibili rischi derivanti dall'operazione
		CCC-05.3		Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	X			
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify data and 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)?			X	I servizi SAAS non prevedono l'interazione diretta dei clienti con le funzioni amministrative dei server. Tutta la gestione delle macchine virtuali è gestita dagli ADS Zucchetti e tutti i servizi sono erogati dai data center siti in Europa
		DSI-01.2		Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			X	
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	X			I dati gestiti nelle applicazioni saas sono quelli previsti dall'adempimento normativo a cui il sw si riferisce e che prevede quali dati debbano essere raccolti. Ci sono campi aggiuntivi custom i cui dati sono classificabili solo dal cliente
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	X			I dati memorizzati nei data center non possono essere migrati in sedi differenti a quelle che compongono le sedi di erogazione del servizio che si trovano tutte in Europa. Prima della migrazione i clienti sono avvisati
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			Tutte le funzioni del servizio SAAS relative alle connessioni da e verso l'esterno possono essere gestite tramite metodologie di crypting con certificato: HTTPS per la fruizione degli applicativi, SFTP per eventuali flussi di scambio dati, PGP per la protezione dei singoli file, adeguandosi al livello di protezione richiesto dai Clienti.
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?		X		Il Cliente detiene il controllo e la proprietà dei propri dati, le policy di etichettatura e gestione rimangono in carico alla sua struttura. Zucchetti come previsto dalla certificazione BS10012 effettua la classificazione del dato in base alla natura del servizio erogato e sono determinati nei registri del

		DSI-04.2		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		X		trattamento gli applicativi a cui i dati sono passati per ulteriori elaborazioni.
		DSI-04.3		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			Zucchetti ha predisposto e mantiene politiche e procedure in linea con la certificazione 9001 e BS10012 per assicurare che i dati di produzione non vengano replicati in ambienti di test. Sono state applicate modalità di Segregation of Duty per assicurare che l'accesso agli ambiti di produzione e test siano limitati ai soli utenti autorizzati. Vi sono procedure di assistenza che non consentono l'utilizzo dei dati dei clienti da parte degli operatori senza la previa autorizzazione del cliente.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			Ogni amministratore di sistema è identificato e valutato. Nella lettera di incarico sono definiti obblighi e responsabilità. le attività/accessi degli ads sono loggati con uno specifico strumento dove è garantita l'integrità dei log. I log registrati sono di log in, log out, log in failed. Nel contratto sono chiarite tutte le responsabilità
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			Quando un dispositivo di storage raggiunge la fine del suo ciclo di vita, le procedure Zucchetti includono un processo di disattivazione progettato per impedire che i dati del cliente siano accessibili a persone non autorizzate secondo le procedure definite dalla BS10012.
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			Zucchetti può fornire la documentazione riportante le procedure di pulizia (sanitize) a richiesta. I dati dei clienti sono cancellati con formattazione invasiva o i dischi sono distrutti.
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			Gli asset hardware in Datacenter Zucchetti sono tracciati e monitorati dal personale Zucchetti mediante lo strumento di gestione inventario proprietario. Tale attività viene eseguita per tutti i siti di erogazione del Datacenter Zucchetti
		DCS-01.2		Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X			
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	X			I data center adottano misure di sicurezza fisica. A titolo esemplificativo vengono riportati alcuni di questi: misure di sicurezza a tutela del perimetro fisico e logico dei dati, personale addetto alla sicurezza h 24, video sorveglianza, sistemi di rilevamento dell'intrusione, sistema di controllo accessi, etc.
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Do you have a capability to use system geographic location as an authentication factor?			X	Zucchetti fornisce la possibilità di configurare delle ACL in base all'indirizzo IP chiamante fornito per iscritto dal Cliente
		DCS-03.2		Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			Sono gestite procedure per i flussi di networking tramite ACL.
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			Zucchetti documenta tutte le informazioni relative ad un eventuale spostamento dei dati tra i vari siti del data center in conformità agli standard ISO 27001.
Datacenter Security *Offsite Equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment	Can you provide tenants with your asset management policies and procedures?		X		Zucchetti fornisce solo informazioni in merito agli Hard Disk e ai supporti magnetici di memorizzazione relativi ai backup in adesione alle procedure BS10012 e ISO27001 per il Datacenter
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			Zucchetti ha messo in opera procedure e processi per il mantenimento di un posto di lavoro sicuro e protetto in tutti gli ambienti. Ogni accesso alle aree aziendali è controllato. Ci sono profili di autorizzazione che non consentono alle persone non autorizzate di accedere ad aree considerate sensibili o ad alto rischio.

		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			Tutti i dipendenti che prestono servizi presso i DC Zucchetti periodicamente effettuano formazione sulla gestione della sicurezza delle informazioni. I piani di formazione sono definiti nelle procedure BS10012 e ISO 27001. Le attività sono svolte da solo personale interno. Qualora ci siano fornitori esterni vengono consegnate agli stessi le procedure specifiche in relazione alle attività che dovranno svolgere come definite dal contratto. Inoltre viene attivata una procedura di qualifica dei fornitori anche indirizzata a verificare lo stato di maturità rispetto alle misure di sicurezza adottate.
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	x			Sono presenti meccanismi di controllo accessi (badge) e videocamere in tutta la zona del Datacenter. E' presente un presidio di guardia armata 24/7
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			Sono applicate adeguate misure di sicurezza per l'accesso ai locali data center atte ad impedire l'accesso a personale non autorizzato. Gli esterni che accedono ai locali in cui si trattano dati riservati sono sempre accompagnati. Gli esterni non possono accedere alla rete interna.
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X			L'accesso ai server viene rigorosamente controllato e consentito solo al personale autorizzato. Sono messe in atto diverse misure a protezione in modo da impedire l'accesso alle macchine a personale non autorizzato.
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	X			I processi di crittografia riguardano diversi aspetti: è applicata agli strumenti di backup; viene applicata ai db sql con la TDE qualora il cliente lo richieda. Tale procedura è facilitata dal fatto che ogni cliente ha un proprio db separato dagli altri. Viene applicata la crittografia nella fase di comunicazione utilizzando l'HTTPS. Viene applicata la crittografia nello storage documentale applicandola, qualora il cliente lo richieda, al DMS con l'attivazione di AES 256. Le chiavi sono gestite dagli applicativi e non conosciute dal cliente. Senza il prodotto software il cliente non può accedere ai documenti o al db. Per questo la gestione delle chiavi è gestite o in apposite tabelle a loro volta crittografate o in codici sorgenti.
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?	X			
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	X			
		EKM-02.3		Do you maintain key management procedures?	X			
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X			
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			A seconda della tipologia del dato e della relativa dislocazione sui server in Datacenter sono implementate diverse misure di crypting. Certificati HTTPS Pubblici • Certificati HTTPS nostra CA • Certificati WIFI nostra CA • Certificati TDE (database) • Certificati per TAPE • Certificati per Encryption Portatili gestiti dai sistemi informativi interni • Certificati per Encryption Applicativa gestiti dai sistemisti applicativi
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?		X		La migrazione delle immagini avviene in un'area segregata e protetta, che non può venire a contatto con dispositivi connessi con altri segmenti di rete.
		EKM-03.3		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			Zucchetti su richiesta installa le chiavi generate e fornite dal cliente. La Gestione delle chiavi del cliente segue regole e procedure che possono essere definite in maniera specifica a livello contrattuale. L'utilizzo di chiavi fornite dal cliente è previsto previa implementazione di una specifica configurazione da definire a livello progettuale.
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			Per la crittografia delle chiavi vengono utilizzati "open formats " e algoritmi standard. • I certificati HTTPS utilizzano algoritmi di cifratura SHA256 o superiore • I certificati TDE utilizzano algoritmi di cifratura SHA1 o superiore . • I certificati per encryption su TAPE usano AES 256-bit encryption • I certificati per encryption sullo storage Netapp (copie primarie backup) usano AES 256-bit encryption

		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?			X	La gestione, mantenimento e conservazione delle chiavi di Zucchetti sono definiti in apposita procedura del sistema Iso27001.
		EKM-04.3		Do you store encryption keys in the cloud?		X		
		EKM-04.4		Do you have separate key management and key usage duties?		X		
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			Zucchetti gestisce baseline di sistema per i componenti critici in linea con gli standard ISO 27001, ISO 9001 e BS10012. Sono messe in atto misure e controlli per mantenere l'infrastruttura in linea con quanto definito dalle informazioni delle baseline di sicurezza. Zucchetti consente la sola importazione dei dati secondo i propri standard. Se il cliente vuole delle configurazioni personalizzate può acquistare una macchina e assumerne la gestione. In tal caso può implementare gli standard che ritiene necessari
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X			Tutti i requisiti legali e normativi vengono presi in considerazione nelle procedure di gestione dei rischi
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X			Zucchetti ha predisposto un programma di gestione del rischio con una valutazione annuale in linea con le disposizione ISO 27001 e BS10012.
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			In Zucchetti l'azione di controllo sulle conformità alle policy, procedure e standard di sicurezza inizia al più alto livello dell'azienda. Sono proprio i manager e l'alta dirigenza che definiscono i principi e i valori seguiti dall'azienda. Ogni dipendente riceve il codice di condotta aziendale ed etico ed è tenuto a completare una formazione periodica. Vengono effettuati controlli in materia di conformità affinché i dipendenti comprendano e seguano le policy definite. I singoli responsabili di reparto verificano che le persone coordinate prestino la dovuta attenzione nei processi che sviluppano. Se rilevano delle criticità ne danno comunicazione agli uffici preposti affinche provvedano ad effettuare formazioni in aula o on the job
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		X		Il documento viene redatto dal personale Zucchetti e usato internamente, è un documento riservato non distribuibile ai clienti. Può essere distribuito solo il PIMS dello standard BS10012 relativo al trattamento dei dati personali. Inoltre è comunicato ai clienti il Registro dei trattamenti relativo al servizio saas che ha acquistato e qualora lo richieda la valutazione del rischio e di impatto relativa.
		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?	X			Il programma di gestione della sicurezza delle informazioni viene valutato annualmente da un ente esterno in conformità con gli standard ISO 27001 e BS10012.
Governance and Risk Management *Management Support /Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X			Tutte le azioni da intraprendere sono documentate nel remdiation plan del sistema di gestione BS10012 e Iso 27001. Le azioni da intraprendere sono formalizzatte con verbale del Comitato sicurezza redatto al termine delle riunioni mensili
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X			Tutta la documentazione relativa alle procedure di sicurezza è disponibile a richiesta per gli interessati
		GRM-06.2		Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	X			Tutte le procedure di sicurezza vengono discusse e riviste con il management aziendale. Esiste un apposito comitato che gestisce le tematiche aziendali relative alla sicurezza

		GRM-06.3		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			Zucchetti adotta procedure e processi in conformità a quanto descritto nella certificazione BS10012, ISO 27001 e ISO 9001. Vengono effettuate verifiche sui fornitori Zucchetti per l'adesione alle politiche privacy/sicurezza. Inoltre i fornitori sono qualificati attraverso la compilazione di appositi questionari finalizzati a valutare il grado di maturità delle loro strutture rispetto alla sicurezza dei dati e delle informazioni
		GRM-06.4		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?		X		
		GRM-06.5		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			Zucchetti rende disponibili le informazioni dei controlli, gli standard, le certificazioni e i regolamenti a cui si conforma. A seconda del contenuto alcuni potranno essere solo visionabili, altri richiederanno l'accettazione di un accordo di non divulgazione (NDA).
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			Zucchetti ha stabilito policy di sicurezza e fornisce formazione sulla sicurezza ai propri dipendenti per educarli sul loro ruolo e sulle responsabilità in relazione alla sicurezza delle informazioni. I dipendenti che violano gli standard o i protocolli definiti sono soggetti a indagini. In caso di violazione accertata vengono adottati gli opportuni provvedimenti disciplinari (ad esempio avvertimento, piano di prestazioni, sospensione e/o cessazione del rapporto di lavoro). Le sanzioni sono pubblicate sulle lettere di incarico consegnate ai dipendenti in relazione al ruolo ricoperto, sul disciplinare interno per l'utilizzo degli strumenti aziendali e sul codice etico.
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			In conformità allo standard ISO 27001 e BS10012, Zucchetti effettua una volta l'anno la revisione delle policy, delle procedure, degli standard e dei controlli di sicurezza in base alle baseline di sicurezza.
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			Zucchetti informa i clienti tramite i canali standard al momento in cui ci sono variazioni in merito alla sicurezza e alla privacy secondo le procedure presenti nello standard BS10012. Inoltre Zucchetti pubblica il presente CAIQ sul proprio sito internet e lo aggiorna con cadenza almeno annuale
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	X			In conformità allo standard ISO 27001 e BS10012, Zucchetti effettua una volta l'anno la revisione delle policy di sicurezza e privacy e del presente CAIQ.
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			In linea con lo standard ISO 27001 e BS10012, Zucchetti ha sviluppato un programma di gestione e riduzione dei rischi. Tali controlli sono stati estesi anche alle certificazioni ISO 27017 e ISO 27018
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X			
Governance and Risk Management *Program*	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Do you have a documented, organization-wide program in place to manage risk?	X			Zucchetti fornisce la documentazione riguardante processi e procedure per il sistema di gestione per la sicurezza delle informazioni solo in merito alla struttura di Data Center certificata ISO 27001 subordinata ad un accordo di riservatezza (NDA). Per il resto della struttura fornisce procedure secondo lo standard BS10012 e Iso 9001. A richiesta può essere fornito ai clienti il piano di audit BS10012 ed è pubblicato sul sito aziendale il presente CAIQ
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	X			
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			Zucchetti ha definito delle regole precise per la restituzione degli asset affidati ai singoli dipendenti. Tutte le policy sono consultabili sul sito aziendale da parte del personale interno
		HRS-01.2		Do you have asset return procedures outlining how assets should be returned within an established period?	X			
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?		X		Zucchetti effettua tali verifiche con questionari e valutazioni effettuate in sede di colloquio, con le valutazioni sul lavoro svolto dai collaboratori e con valutazione in sede di qualifica fornitori se esterni.

Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			Zucchetti ha definito procedure e regole per la gestione delle informazioni. Tutti i dipendenti ricevono tali procedure e sono tenuti a firmarle
		HRS-03.2		Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	X			
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			Zucchetti adotta procedure e controlli in merito alla procedura di employee management. Quando un collaboratore lascia l'azienda o cambia mansione tutti gli uffici ne sono informati tramite una comunicazione e ogni ufficio provvede a disabilitare la parte di competenza. L'ufficio privacy controlla che le utenze siano state disabilitate.
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			
Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			Nessun dispositivo mobile o portabile può essere interfacciato al sistema che ospita i dati dei clienti, sono state approntate regole, procedure e processi al fine di evitare tale possibilità. Può capitare che qualora il cliente lo richieda nello specifico l'addetto all'attività di assistenza salvi sul pc laptop i dati del cliente per effettuare test o prove di malfunzionamento. Tali dati, che in questo caso sono crittografati, sono trattati solo per il tempo strettamente necessario all'esecuzione di attività di assistenza e poi cancellati.
Human Resources *Non-Disclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			I requisiti per gli accordi di non divulgazione o di riservatezza in merito alla protezione dei dati e i dettagli operativi per la loro gestione sono identificati, documentati e riesaminati a intervalli pianificati. E' gestito il versioning degli NDA sviluppati nei rispettivi ambiti.
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			Zucchetti, come da accordi contrattuali che il cliente sottoscrive, fornisce tutti i dettagli sulle responsabilità e ruoli nei rapporti con lo stesso per il trattamento dei dati nella nomina a responsabile del trattamento dati. Zucchetti per i servizi saas trasmette ai clienti, a richiesta, l'elenco aggiornato degli amministratori di sistema
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			L'utilizzo degli strumenti aziendali viene regolato da un'apposita procedura, fornita e siglata da tutti i dipendenti. Non è consentito l'utilizzo di apparati BYOD
		HRS-08.2		Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?			X	
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			Tutti i dipendenti Zucchetti sono tenuti a completare una formazione su base periodica, relativa a propri ruoli, sulla sicurezza. Tutto il personale tecnico adibito alla funzione di ADS è tenuto a firmare un accordo di non divulgazione prima di essere autorizzato ad accedere ai sistemi. Il processo di formazione è definito secondo lo standard BS10012, ISO 27001 e ISO 9001. Tutti i lavoratori dell'area programmazione, analisi e controllo qualità dei prodotti venduti in modalità saas e i consulenti applicativi ed help desker che fanno assistenza ai clienti sul corretto uso delle procedure hanno fatto una formazione specifica sui requisiti da rispettare in relazione al GDPR e sui rischi. Rispetto a questi eventi sono registrate la presenza del collaboratore ed il contenuto del corso svolto. Tale formazione è ripetuta in occasione di ogni disfunzione rispetto agli standard aziendali che comporta un rischio per il trattamento dei dati
		HRS-09.2		Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			
		HRS-09.3		Do you document employee acknowledgment of training they have completed?	X			
		HRS-09.4		Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			
		HRS-09.5		Are personnel trained and provided with awareness programs at least once a year?	X			
		HRS-09.6		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			

Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			Zucchetti facilita con diversi strumenti la comunicazione tra dipendenti ed il diffondersi delle corrette informazioni per la comprensione del proprio ruolo e delle proprie responsabilità. Questi strumenti annoverano corsi per neoassunti, pubblicazioni a livello di Intranet e messaggi di posta puntuali su determinati argomenti. I coordinatori e responsabili dei diversi settori si assicurano che tutti gli argomenti siano ben compresi e che le procedure vengano messe in pratica nel rispetto degli standard definiti a livello aziendale. Zucchetti monitora il comportamento dei suoi collaboratori ed effettua interventi formativi indirizzati a modificare abitudini consolidate che possono generare un rischio per il trattamento dei dati interno o di clienti
		HRS-10.2		Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			
		HRS-10.3		Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			E' previsto, come da regolamento interno, che tutti i dispositivi siano configurati per attivare il lockout dopo un periodo di tempo definito
		HRS-11.2		Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X			Il regolamento interno stabilisce come tutti i documenti riservati non debbano essere conservati sulle scrivanie
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			Nel datacenter Zucchetti sono state adottate diverse misure di controllo, logging e di sicurezza. Gli accessi privilegiati (amministratori di sistema) sono tracciati, controllati in un sistema di logging e sono limitati al perimetro della control room.
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			E' previsto un processo di variazione e rimozione dei profili autorizzativi degli incaricati ad ADS.
		IAM-02.2		Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	X			L'accesso agli asset è regolato come da certificazione ISO27001. L'accesso ai dati è limitato come previsto dal regolamento GDPR e dalla certificazione BS10012
		IAM-02.3		Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	X			I profili degli amminsitratori di sistema sono gestiti da diversi uffici che monitorano continuamente gli account attivi al fine di individuare eventuali profili da disattivare
		IAM-02.4		Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?			X	L'installazione degli ambienti, nel servizio SaaS, è realizzata in maniera tale da riservare l'accesso ai singoli utenti del Cliente
		IAM-02.5		Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X			Le regole di accesso prevedono un meccanismo di autenticazione del singolo utente a cui si aggiunge una successiva assegnazione dei ruoli e dei permessi in base al gruppo di appartenenza configurato a sistema
		IAM-02.6		Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	x			Aziendalmente non vi è l'esigenza di avere fattori di autenticazione a due fattori se non nelle procedure amministrative istituzionali per le quali gli operatori accedono con lo SPID. Le attività svolte sui clienti prevedono l'adozione del processo scelto dal cliente.
		IAM-02.7		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		X		Vengono tracciate tramite trouble ticketing le richieste di variazione del profilo d'accesso.
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			L'accesso alle porte di diagnostica e configurazione è riservato solo agli amministratori di sistema
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			Zucchetti ha implementato la gestione e l'archiviazione dell'identità di tutto il personale che ha accesso ai sistemi e alla rete per necessità di gestione dei sistemi. Ci sono procedure per la gestione delle identità dei collaboratori e dei clienti. Sono registrate tutte le deleghe ad operare sui sistemi dei clienti
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			

Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			Zucchetti è responsabile per la gestione dell'infrastruttura. Il Cliente è responsabile per quanto riguarda le credenziali rilasciate dal proprio ufficio del personale per l'accesso al servizio SAAS. Tali accordi sono definiti a livello contrattuale. Ci sono documenti tecnici che informano il cliente sulle misure di sicurezza adottate.
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Zucchetti ha definito procedure e processi per garantire l'accesso ai sistemi ai soli utenti autorizzati. Gli ambienti di sviluppo degli applicativi contenenti i sorgenti del codice sono fisicamente dislocati in un ambito differente rispetto a quello di erogazione dei servizi. I test sono effettuati su dati di fantasia e mai su db di produzione a meno ce non vi sia una richiesta espressa in tal senso del cliente da definirsi a livello progettuale. Ci sono firewall , IDS e IPS a difesa del perimetro esterno. I collaboratori sono stati formati sulla sensibilità delle informazioni e sulla riservatezza che devono mantenere. Gli accessi agli uffici sono controllati e sono individuali gli accessi logici alle aree in cui quelle informazioni sono gestite e conservate
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Does your organization conduct third-party unauthorized access risk assessments?	X			Le attività di web application penetration test prevedono verifiche di "Authentication Testing".
		IAM-07.2		Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access?	X			Le web application infinity prevedono l'abilitazione dei seguenti controlli in fase di accesso: -ciclicità della Password impostabile; -scadenza automatica della password dopo un numero desiderato di giorni impostabile; -scadenza dell'utenza dopo un'inattività superiore a 180gg; -complessità della password e lunghezza minima della password di 8 caratteri impostabile; -abilitazione del codice Captcha; -numero massimo di tentativi di accesso impostabile; -abilitazione reset della password protetto da invio mail; -abilitazione al caricamento di un dizionario personalizzato di password non complesse; -abilitazione funzionalità per evitare l'enumerazione degli account utenti.
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?			X	Le credenziali sono gestite in autonomia dai Clienti. Le credenziali inoltre sono criptate all'interno del database Per i servizi SaaS non è previsto l'accesso ai dati da parte degli AdS Zucchetti se non formalmente autorizzato dal Cliente o in casi di emergenza.
		IAM-08.2		Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?			X	
		IAM-08.3		Do you limit identities' replication only to users explicitly defined as business necessary?			X	Le procedure in essere garantiscono l'univocità dell'assegnazione delle credenziali di accesso ad ogni singolo individuo. Non è consentita la replica delle utenze
Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			Esiste un processo di rilascio delle credenziali amministrative di accesso al servizio SAAS che garantisce al cliente la loro assegnazione univoca.
		IAM-09.2		Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?		X		Il servizio SAAS permette il solo accesso agli applicativi pubblicati.
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			In linea con lo standard ISO 27001, periodicamente vengono effettuati controlli sulle autorizzazioni concesse agli ADS Zucchetti; per ognuna di esse viene richiesta l'approvazione specifica, pena la revoca immediata dell'accesso

		IAM-10.2		Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			alle risorse di DC Zucchetti. Vengono raccolte le opportune evidenze a supporto del processo. Lo standard di cui sopra definisce gli specifici controlli delle analisi degli accessi delle utenze di Zucchetti. I rapporti di correzione dei diritti di accesso verranno condivisi con i clienti solo in caso di violazione dei rapporti. Qualora persone non autorizzate accedano ai dati dei clienti sarà attivata la procedura di comunicazione presunto data breach prevista dalla BS10012 attraverso la quale sarà fornita al cliente l'analisi dell'accaduto in modo che lo stesso sia messo nella posizione di poter decidere se comunicare l'accaduto alle Autorità
		IAM-10.3		Do you ensure that remediation actions for access violations follow user access policies?	X			
		IAM-10.4		Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	X			
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			Zucchetti per i propri dipendenti e partner commerciali ha messo in opera procedure e processi che coinvolgono diversi uffici con differenti competenze al fine di variare e revocare gli accessi delle utenze. E' demandato il controllo delle utenze del servizio SAAS direttamente al cliente.
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			Il servizio SAAS permette l'implementazione di soluzioni di Single Sign On (SSO) con l'ausilio di standard aperti e standard di federazione delle identità basate su SAML 2.0.
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	X			
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X			
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?			X	Non vengono integrate nelle modalità di autenticazione funzionalità di Policy Enforcement Point.
		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?			X	I servizi erogati dal DC Zucchetti permettono al cliente di definire la configurazione della profilazione degli utenti in base ai ruoli.
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			Sono disponibili diverse modalità di autenticazione per aumentare la complessità dell'operazione, a titolo esemplificativo sono compresi: captcha, pin code, multi-factor authentication. Fa eccezione la control room del Datacenter.
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?	X			La configurazione è permessa con la sola implementazione della modalità di SSO.
		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?	X			Le modalità di gestione degli utenti nel servizio SAAS permettono l'applicazione di policy relative alla complessità della password e del blocco degli account che consentono ai clienti di definirli secondo i propri standard. Sono attive procedure per la forzatura della password al primo collegamento e meccanismi per lo sblocco degli account in modalità manuale.
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			
		IAM-12.10		Do you support the ability to force password changes upon first logon?	X			
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			Zucchetti garantisce l'utilizzo di opportune limitazioni e di sistemi di monitoraggio in linea agli standard ISO 27001.
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			Solo gli utenti autorizzati possono accedere ai locali e agli ambienti dove sono trattati i dati dei clienti in data center. L'elenco dei collaboratori autorizzati è presente nei processi di gestione e viene gestito in relazione ai cambiamenti che possono nel tempo avvenire. La verifica degli accessi è demandata a sistemi elettronici di controllo accessi e di profili logici di autorizzazione per accedere agli ambienti. Il processo viene verificato con specifiche attività di audit sia da parte di auditor interni che di società esterne. Ci sono 2 sistemi di log: 1 su tabella in cui l'amministratore applicativo può verificare gli accessi - log in e log out (i log vengono cancellati dopo un tempo configurabile dal cliente), altro sistema su file. La gestione del log applicativo è demandato al cliente.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X			
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	X			
		IVS-01.4		Are audit logs centrally stored and retained?	X			Il collettore dei Log di sistema è configurato in modalità centralizzata, sia per la raccolta che per la conservazione. La collezione e analisi dei log degli ADS applicativi è in carico al cliente. L'estrazione dei log e la conservazione è in

		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			carico al cliente
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			Sono in uso strumenti che permettono il monitoring ed i relativi avvisi in tempo reale sulle condizioni operative delle macchine.
		IVS-02.2		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X			Sono predisposti meccanismi per l'individuazione di modifiche alla configurazione delle macchine virtuali
		IVS-02.3		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?		X		Al cliente che sottoscrive un contratto per un servizio in modalità condivisa viene garantita la disponibilità del servizio, in base agli SLA, indipendentemente dagli interventi di manutenzione all'infrastruttura.
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			I sistemi informatici di Zucchetti utilizzano clock di sistema interni sincronizzati tramite NTP (Network Time Protocol).
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?		X		L'erogazione del Servizio SAAS avviene in una modalità operativa che garantisce le migliori prestazioni a ogni ambiente dei clienti. Le risorse sono distribuite e condivise dalle varie macchine al fine di poter supportare l'intero carico richiesto. Sono presenti sistemi di monitoraggio al fine di ottimizzare le prestazioni del sistema per soddisfare in maniera continuativa i requisiti normativi e contrattuali per tutti i sistemi che erogano il servizio.
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			X	
		IVS-04.3		Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			Zucchetti mette in atto processi e procedure per la valutazione delle vulnerabilità di sicurezza in linea con le tecnologie di virtualizzazione impiegate per l'erogazione del servizio.
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			X	Zucchetti non prevede l'erogazione di servizi di questo tipo.
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X			Come parte dei processi di miglioramento tecnologico e della sicurezza, l'architettura di rete di base viene costantemente rivista, migliorata e implementata. Ogni modifica viene documentata come previsto dai processi ISO 27001.
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X			
		IVS-06.4		Are all firewall access control lists documented with business justification?	X			
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			Zucchetti , in linea con la privacy by default, ha adottato le policy di privilegio minimo ai componenti dell'infrastruttura al fine di limitare le porte, i protocolli e i servizi alle sole necessarie funzioni. Vengono continuamente effettuate delle scansioni alla rete affinche possano essere corrette quelle situazioni in cui porte, protocolli e servizi non dovessero essere più necessari. Sono installati antivirus per la prevenzione dai virus e malware.
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Gli ambienti di test sono forniti a richiesta e sono completamente segregati rispetto agli ambiti di produzione.
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			X	Zucchetti non prevede l'erogazione di servizi di questo tipo.
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	X			L'ambiente di produzione è completamente segregato rispetto ad altri ambienti di non produzione, sia a livello di erogazione del servizio che di sviluppo e produzione dei programmi oggetto del servizio SAAS.
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			Tutti gli ambienti di rete e di sistema sono protetti da firewall al fine di soddisfare i requisiti di sicurezza in conformità agli standard ISO 27001, oltre a quelli legislativi, normativi e contrattuali.

		IVS-09.2	users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			Gli stessi garantiscono la separazione degli ambienti di produzione da quelli di non produzione per garantire la protezione e l'isolamento dei dati sensibili.
		IVS-09.3		Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?			X	Non è consentito l'accesso all'infrastruttura da parte dei Clienti
		IVS-09.4		Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			I dati risiedono su db separati con sistemi di elaborazione comuni.
		IVS-09.5		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			Tutti gli ambienti di rete e di sistema sono protetti da firewall al fine di soddisfare i requisiti di sicurezza in conformità agli standard ISO 27001, oltre a quelli legislativi, normativi e contrattuali. Gli stessi garantiscono la separazione degli ambienti di produzione da quelli di non produzione per garantire la protezione e l'isolamento dei dati sensibili.
Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			Gli interventi sull'infrastruttura che eroga il servizio SAAS sono effettuati solo da personale tecnico Zucchetti autorizzato. Il cliente non è possibilitato a trasferire direttamente le immagini delle proprie macchine virtuali. Limitatamente al servizio SAAS non è possibile la copia diretta dei programmi o dei dati, le operazioni di migrazione vengono effettuate sempre con l'ausilio di tecnici Zucchetti. Tutte le operazioni di importazioni di dati e programmi sull'infrastruttura di DC Zucchetti avvengono in un'area di rete separata e segregata dagli ambienti di non produzione.
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?			X	
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			In linea con lo standard ISO 27001 e con la privacy by default BS10012, Zucchetti applica il principio del privilegio minimo, consentendo agli utenti dei sistemi che erogano il servizio SAAS soltanto l'accesso necessario per svolgere le proprie mansioni lavorative. I tecnici che dovessero avere necessità di accedere a livelli superiori rispetto a quello configurato devono ottenere l'autorizzazione adeguata dagli amministratori di sistema del DC Zucchetti. Per i servizi SAAS il cliente ha facoltà di creare gli utenti in modo autonomo per disporre dell'accesso ai soli programmi erogati e non all'infrastruttura dei server.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	X			Zucchetti ha messo in atto le necessarie misure per proteggere la propria rete da accessi non autorizzati . In merito alla rete wireless sono state implementate delle impostazioni di sicurezza con crittografia avanzata per l'autenticazione.
		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)?	X			
		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?	X			
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall 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.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	X			I diagrammi di architettura di rete del DC Zucchetti identificano chiaramente gli ambienti ad alto rischio e i flussi di dati che potrebbero avere ripercussioni sulla conformità legale. Sono state adottate procedure e processi per la verifica continua di tali ambiti al fine di poter intervenire con le dovute revisioni. I servizi prima di essere venduti sono analizzati con logiche di privacy by design in modo da applicare la sicurezza by default preventiva all'utilizzo del sistema da parte del cliente

		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?	X			Per il proprio data center, Zucchetti adotta misure tecniche difensive per il rilevamento di attacchi basati sulla rete al fine di reperire le dovute informazioni per rispondere tempestivamente agli eventi.
Interoperability & Portability *APIs*	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			Le API pubblicate sono relative agli standard erogati dai programmi del Servizio SAAS, sono intese come funzionalità dei programmi in uso.
Interoperability & Portability *Data Request*	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			I dati non strutturati dei clienti contenuti nell'ambiente del Servizio SAAS sono disponibili nei seguenti formati: .csv, .pdf, .xls, .doc. L'estrazione può essere configurata in base alle esigenze dei clienti.
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	X			A livello contrattuale vengono rilasciate le policy e le procedure che disciplinano l'utilizzo del Servizio SAAS, unitamente ai programmi in uso oltre al livello di servizio garantito (SLA). Per la migrazione dei dati viene fatto un Privacy level agreement dal quale sono definiti i tempi e modi dell'attività di conversione.
		IPY-03.2		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		X		Tutte le funzionalità legate all'infrastruttura che ospita il servizio SAAS possono essere gestite dal solo personale tecnico Zucchetti.
		IPY-03.3		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X			A livello contrattuale vengono rilasciate le policy e le procedure che disciplinano l'utilizzo del Servizio SAAS, unitamente ai programmi in uso oltre al livello di servizio garantito (SLA). Per la migrazione dei dati viene fatto un Privacy level agreement dal quale sono definiti i tempi e modi dell'attività di conversione.
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			I programmi Zucchetti in uso nel servizio SAAS permettono le funzioni di import ed export di dati mediante servizi standardizzati sicuri. E' il cliente che determina come gestire i file estratti e come comunicarli.
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			Vengono rilasciate le informazioni riguardanti l'interoperabilità attraverso le comunicazioni pubbliche in Internet e per le conversioni attraverso la redazione e condisione del PLA (Privacy Level Agreement)
	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?			X	Le tecnologie utilizzate e le modalità di configurazione dell'infrastruttura restano riservate alla struttura tecnica Zucchetti.
		IPY-05.2		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?			X	
		IPY-05.3		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			X	
Mobile Security *Anti-Malware*	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	X			La formazione e la sensibilizzazione alla sicurezza delle informazioni al personale tecnico che gestisce l'infrastruttura di erogazione è improntata alla conoscenza delle problematiche relative alle diverse piattaforme di erogazione e fruizione.
Mobile Security *Application Stores*	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	X			Non è possibile utilizzare altri store per l'accesso ai dati se non quelli autorizzati da Zucchetti. Nei processi operativi interni Zucchetti ogni app deve essere autorizzata ed inserita in una white list di app utilizzabili.
Mobile Security *Approved Applications*	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	X			Tutti i dipendenti sono formati in merito a tale argomento e sono tenuti a rispettare tali indicazioni. Gli applicativi non hanno policy perché gestiscono un ambito in cui ci sono app specifiche previamente autorizzate. Le app sono sviluppate come accessorio del prodotto e si basano sullo stesso db dell'applicazione. Per questo c'è la lista delle app autorizzate che il cliente conosce perchè facenti parte dell'offerta di servizio.
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	
Mobile Security *Awareness and Training*	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	X			
Mobile Security *Cloud Based Services*	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	X			

Mobile Security *Compatibility*	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?	X			Zucchetti ha adottato logiche di test delle APP in riferimento ai diversi dispositivi e S.O. per l'ottenimento della compatibilità e certificazione all'uso. Le attività sono svolte da addetti al controllo qualità del software che eseguono tutte le verifiche prima del rilascio in produzione.
Mobile Security *Device Eligibility*	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			X	Tutti i dipendenti sono formati in merito a tale argomento e sono tenuti a rispettare tali indicazioni. Ogni prodotto viene testato e verificato e sulla comunicazione di rilascio sono indicate anche le caratteristiche di compatibilità che deve avere l'infrastruttura per supportare il servizio, come ad esempio i browser, sistemi operativi, app di terze parti , etc.
Mobile Security *Device Inventory*	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory.	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	X			
Mobile Security *Device Management*	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	X			
Mobile Security *Encryption*	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			X	
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	X			Non è possibile bypassare tramite le app i controlli di sicurezza . Gli users devono appartenere alla medesima URL di configurazione e allo stesso ambiente ed i profili vengono presi dal sistema e sono immodificabili nell'app. Nel caso uno di questi due parametri venga modificato, la base dati locale viene automaticamente distrutta e ricreata, richiedendo il download completo di tutta la configurazione server-side. L'autenticazione supportata è quella disponibile dalla piattaforma Zucchetti (Applicativa, da LDAP e tramite Single Sign-on). Nel caso di SSO l'App autentica l'utente sulla base di un certificato rilasciato con apposita procedura dal server. Se così configurata l'App non supporta più il local multi-user, ed un device ammette UN SOLO USER. Viene inoltre disabilitata la funzionalità di cambio password dall'App
		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?	X			
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	
		MOS-13.2		Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?			X	Non è consentito l'utilizzo di apparati BYOD
Mobile Security *Lockout Screen*	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	Le versioni dei sistemi utilizzati dalle app sono testati e verificati dagli addetti al controllo qualità. Le caratteristiche tecniche di compatibilità sono presenti sulla comunicazione di rilascio. Il processo è quello descritto al punto precedente.
Mobile Security *Operating Systems*	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?		X		
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	X			
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?	X			
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	X			
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	Non è consentito l'utilizzo di apparati BYOD
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X	
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			X	
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?		X		Ci sono procedure operative interne che permettono di verificare la necessità di installare patch di prodotto e sistema e di vericare il corretto funzionamento delle stesse. Se le patch superano il controllo di conformità allora saranno installate sugli strumenti a cui si riferiscono. Questo riferito agli strumenti utilizzati da Zucchetti per l'erogazione del servizio.
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?		X		
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	

Security Incident Management, E-Discovery, & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			Zucchetti mantiene contatti con organizzazioni e organismi del settore che operano nell'ambito del rischio e della conformità, enti locali e organismi di regolamentazione.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	X			Zucchetti ha sviluppato piani, procedure e programmi di risposta agli incidenti secondo gli standard ISO 27001 e BS10012. Vengono forniti dettagli sulle attività di controllo, sulle responsabilità della Zucchetti e del cliente in caso di incidente di sicurezza. I piani di sicurezza vengono sottoposti annualmente a test di verifica.
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?		X		
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X			
		SEF-02.4		Have you tested your security incident response plans in the last year?	X			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	x			Ogni evento di sicurezza delle informazioni che possa comportare un presento data breach deve seguire la procedura prevista nelle relative linee guida formalizzate per la BS10012
		SEF-03.2		Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			Tali comunicazioni avvengo tramite lo strumento di Ticket utilizzato per le attività di post vendita e c'è un ufficio preposto che prende in carico le segnalazioni
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			I piani di risposta rispettano gli standard ISO 27001. Non sono aderenti alle norme per le indagini legali. Zucchetti si rende disponibile a fornire la massima collaborazione a fronte di eventuali richieste delle forze dell'ordine e a definire con i clienti a livello progettuale dei sistemi di data collector che garantiscano i livelli di sicurezza richiesti dalle analisi forensi.
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?		X		
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			I parametri di sicurezza Zucchetti sono monitorati e analizzati quotidianamente dal gruppo sicurezza IT. I dati non sono forniti ai clienti se non a seguito di specifica richiesta e dopo la sottoscrizione di un NDA
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?		X		
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	X			Zucchetti ha messo in atto politiche, procedure e meccanismi per correggere errori di qualità dei dati e rischi associati per i servizi in SaaS. Zucchetti fa accedere ai sistemi dei clienti i propri addetti solo previa richiesta del cliente e col profilo dallo stesso attribuito. Tutte le attività sono registrate in uno strumento di ticketing che può essere interrogato e letto insieme ai log di accesso in caso di incidente
		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?	X			
Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			Zucchetti ha sviluppato piani, procedure e il programma di risposta agli incidenti in conformità allo standard ISO 27001 e BS10012. Zucchetti fornisce i dettagli sulle attività di controllo in specifici rapporti in seguito a richiesta formale dei clienti.
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			Zucchetti gestisce le capacità e i dati di utilizzo in linea con i principi definiti dagli standard ISO 27001 per il servizio SaaS.
		STA-03.2		Do you provide tenants with capacity planning and use reports?			X	
Supply Chain Management, Transparency, and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			Le valutazioni interne annuali di conformità ed efficacia delle politiche, delle procedure, delle misure di supporto e delle metriche di supporto sono realizzate in linea con quanto previsto dagli standard ISO 27001, BS10012.

Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			Eventuali accordi con terze parti sono esaminate dall'Ufficio legale e privacy Zucchetti e dall'Ufficio Gestione Fornitori Zucchetti. Esiste un iter di qualifica che fa riferimento anche alle misure di sicurezza messe in atto dai sub fornitori per la tutela dei dati. Ogni sub fornitore deve dichiarare dove tratterà i dati dei clienti. I clienti sono informati qualora i dati siano trattati fuori dal territorio dell'Unione Europea
		STA-05.2	• Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			
		STA-05.3		Does legal counsel review all third-party agreements?	X			
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X			Il sistema di sicurezza delle informazioni Zucchetti è stato progettato e implementato per soddisfare le best practice di settore in materia di sicurezza in linea con gli standard ISO 27001 e BS10012. Verso i fornitori sono messi in atto audit e questionari indirizzati a verificare la loro maturità rispetto alle problematiche di sicurezza.
		STA-05.5		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			E' sempre possibile ripristinare i dati del cliente dai salvataggi in regime di backup.
		STA-05.6		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			Zucchetti eroga servizi in logica SaaS esclusivamente da Datecenter dislocati sul teritorio italiano e nella comunità europea
		STA-05.7		Can you provide the physical location/geography of storage of a tenant's data upon request?		X		Tutti i dati sono contenuti nei datacenter gestiti da Zucchetti dislocati in Europa. L'ubicazione dei dati è consociuta in anticipo da parte del cliente e non vengono spostati se non a seguito di preventiva comunicazione
		STA-05.8		Can you provide the physical location/geography of storage of a tenant's data in advance?		X		
		STA-05.9		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		X		Zucchetti non consente la definizione di specifiche dislocazioni dei dati in differenti posizioni geografiche.
		STA-05.10		Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X			In caso di Data Breach, Zucchetti include nel processo di gestione dell'incident di sicurezza il coinvolgimento del "Team Pivacy". La notifica al cliente viene effettuata a fronte dell'impatto dell'incidente sulla tipologia dei dati. La procedura in caso di violazione di dati personali è quello definito dalla procedura per la comunicazione dei Data breach definita in conformità allo standard BS10012 . La procedura può essere consegnata ai clienti su richiesta.
		STA-05.11		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?			X	Zucchetti non effettua questa tipologia di trattamento dei dati in quanto non previsto dagli accordi contrattuali.
		STA-05.12		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		X		Ai clienti viene fornita la lista dei fornitori a richiesta. Nel registro del trattamento sono specificati i trattamenti affidati all'esterno e se i trattamenti comportano trasferimento dei dati fuori dall'italia.
Supply Chain Management, Transparency, and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	X			I fornitori devono rispettare determinati requisiti contrattuali in modo da essere in linea alle politiche di gestione della Zucchetti. Dove necessario, vengono espletati verso ogni fornitore una serie di controlli addizionali per verificarne la conformità. Nei confronti dei propri fornitori, Zucchetti mette in atto procedure e controlli per la verifica annuale delle disposizioni contrattuali e per adempiere agli eventuali interventi correttivi. Ci sono in essere processi di qualifica dei fornitori secondo le procedure Iso 27001 e BS10012. Ogni fornitore in sede di qualifica deve dichiarare le misure di sicurezza sia tecniche che organizzative implementate a tutela dei dati
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	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)?	X			
		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)?	X			

		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X			
		STA-07.4		Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?		X		Gli SLA (Service Level Agreement) del servizio SAAS sono documentati e forniti ai clienti su richiesta. Qualora il cliente voglia uno sla dedicato deve essere acquistato dal cliente
		STA-07.5		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X			Zucchetti rende disponibili le metriche standard adottate nel documento di SLA
		STA-07.6		Do you provide customers with ongoing visibility and reporting of your SLA performance?		X		Gli SLA (Service Level Agreement) del servizio sono documentati e forniti ai clienti su richiesta e solo qualora sia attivo il contratto di sla di servizio. Per il saas sono attivi tre livelli di servizio: SLA00: Questo servizio consiste nella messa a disposizione al Cliente dell'accessibilità a tutti gli strumenti di richiesta assistenza disponibili alla data di effettuazione della richiesta, secondo le specifiche di cui –SERVIZI HELPDESK PRO, . Il Fornitore si impegna a fornire una risposta alla richiesta di assistenza del Cliente formulata ai sensi del servizio di cui alla presente sezione nel minor tempo possibile, considerata la disponibilità del Fornitore e fatta salva, in ogni caso la precedenza di eventuali richieste in gestione da parte del Fornitore pervenute da clienti ai sensi del servizio Helpdesk Pro Premium SLA99; SLA01: Questo servizio consiste nella messa a disposizione al Cliente dell'accessibilità esclusivamente a tutti gli strumenti di richiesta assistenza di tipo WEB disponibili alla data di effettuazione della richiesta, restando espressamente esclusi strumenti di assistenza diversi (a titolo esemplificativo: assistenza telefonica ecc.), secondo le specifiche di cui all'allegato ai SERVIZI HELPDESK PRO. Il Fornitore si impegna a fornire una risposta alla richiesta di assistenza del Cliente formulata ai sensi del servizio di cui alla presente sezione nel minor tempo possibile, considerata la disponibilità del Fornitore e fatta salva, in ogni caso la precedenza di eventuali richieste in gestione da parte del Fornitore pervenute da clienti ai sensi del servizio Helpdesk Pro Premium SLA99. SLA99: Questo servizio consiste nella messa a disposizione al Cliente dell'accessibilità a tutti gli strumenti di richiesta assistenza disponibili alla data di effettuazione della richiesta. Il cliente che acquista questo servizio viene collocato in un percorso di risoluzione problematiche dedicato, secondo il dettaglio di cui ai SERVIZI HELPDESK PRO.
		STA-07.7		Do your data management policies and procedures address tenant and service level conflicts of interests?	x			I ruoli sono definiti contrattualmente e nei confronti dei clienti non possono mai esserci cnflitti di interesse
		STA-07.8		Do you review all service level agreements at least annually?	X			Tutti gli SLA vengono rivisti almeno una volta all'anno
Supply Chain Management, Transparency, and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			I fornitori devono rispettare determinati requisiti contrattuali in modo da essere in linea alle politiche di gestione della Zucchetti. Dove necessario, vengono espletati verso ogni fornitore una serie di controlli addizionali per verificarne la conformità. Nei confronti dei propri fornitori, Zucchetti mette in atto procedure e controlli per la verifica annuale delle disposizioni contrattuali e per adempiere agli eventuali interventi correttivi. Ci sono in essere processi di qualifica dei fornitori secondo le procedure Iso 27001 e BS10012. Ogni fornitore in sede di qualifica deve dichiarare le misure di sicurezza sia tecniche che organizzative implementate a tutela dei dati
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			
Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?			X	Non sono interessati fornitori di terze parti per l'erogazione del servizio SaaS
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			Zucchetti si avvale periodicamente di imprese che operano nel settore della cybersecurity per eseguire valutazioni di vulnerabilità sulle minacce esterne. A richiesta, i risultati di tali valutazioni possono essere forniti ai clienti previa sottoscrizione di un NDA
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	X			Zucchetti ha adottato processi e procedure per la gestione di software antivirus/antimalware e procedure per il loro aggiornamento che avviene in modo costante nel corso della giornata.
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X			
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			Zucchetti esegue scansioni periodiche a tutte le componenti del Servizio SaaS (network, S.O., programmi, ecc.) utilizzando tool proprietari e tool presenti in commercio.
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			

		TVM-02.3	testing, to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	X			Zucchetti fornisce i risultati delle scansioni di sicurezza per i servizi in SaaS dietro accettazione di un accordo di non divulgazione (NDA).
		TVM-02.5		Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			Zucchetti prevede la gestione della risoluzione delle vulnerabilità nei processi di change. Le tempistiche sono quelle standard definite dagli sla per i servizi saas
		TVM-02.6		Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?		X		Zucchetti ha in atto politiche di controllo e monitoraggio al fine di risolvere tutte le debolezze infrastrutturali presenti
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	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?			X	Zucchetti non permette ai clienti la gestione di applicazioni client in base alle proprie esigenze.
		TVM-03.2		Is all unauthorized mobile code prevented from executing?			X	