CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC		La Società mantiene e implementa piani di audit che vengono eseguiti annualmente per testare l'efficienza e efficacia dei controlli di sicurezza implementati.	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Audit and Assurance Policy and Procedures	Audit & Assurance
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	Shared CSP and CSC		Procedura gestione Audit (paragrafo "revisione procedura") Procedura di gestione della documentazione				
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	Shared CSP and CSC			A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	Shared CSP and CSC			A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	Shared CSP and CSC		La Società mantiene ed implementa annualmente i piani di audit eseguiti per testare l'efficienza e efficacia dei controlli di sicurezza implementati	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	Shared CSP and CSC		Procedura gestione Audit (paragrafo "modelli di audit")	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC		Procedura di valutazione del rischio (paragrafo "remediation")	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	No	CSC-owned		I report possono essere resi disponibili su richiestam come riassunto dei report generali, in quanto si tratta di report interni aziendali				
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	Shared CSP and CSC		La Società ha una politica di sicurezza di applicazioni, sistemi e servizi, che supporta lo sviluppo sicuro. Procedura di sicurezza delle applicazioni (paragrafo "standard di sviluppo")	AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	Application and Interface Security Policy and Procedures	Application & Interface Security
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC		Procedura di sicurezza delle applicazioni (paragrafo "revisione procedura")				
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	Shared CSP and CSC			AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	Shared CSP and CSC		Procedura di sicurezza delle applicazioni (paragrafo "metriche tecniche e operative")	AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSC-owned		La Società incorpora le best practice OWASP del settore Procedura di sicurezza delle applicazioni (paragrafo "Standard applicativi OWASP")	AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSC-owned		Test di sicurezza eseguiti tenendo in considerazione gli standard di settore tra cui le OWASP Test Guide Procedura di sicurezza delle applicazioni (paragrafo "Standard applicativi OWASP")	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application Security Testing	
AIS-05.2	Is testing automated when applicable and possible?	No	CSC-owned						
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSC-owned		Test OWASP sviluppo sicuro del software Procedura di sicurezza delle applicazioni (paragrafo "Standard applicativi OWASP")	AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	

ID	Question	Answer	Ownership	Documentation	Control ID	Control Description	Control Title	Domain
AIS-06.2	Is the deployment and integration of application code automated where possible?	No	CSC-owned				Application Deployment	
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	Shared CSP and CSC		AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	No	CSC-owned					
BCR-01.1	Are business continuity management and operational resiliency policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	Procedura di Business Continuity Plan (BCP)	BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and Procedures	
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	Procedura di Business Continuity Plan (paragrafo "revisione procedura")				
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	Shared CSP and CSC	Procedura di Business Continuity Plan (paragrafo "strategie di resilienza operativa") Template Business Continuity Plan (BCP)	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis	
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	Shared CSP and CSC	La piattaforma SaaS e' implementata su un'infrastruttura certificata (CSP Qualificato AgID in possesso di certificazioni ISO 27001, 27017 e 27018)	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	Shared CSP and CSC	Procedura di Business Continuity Plan (paragrafo "strategie di resilienza operativa")	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSC-owned	Procedura di Business Continuity Plan (paragrafo "strategie di resilienza operativa")	BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	Documentation	Business Continuity Management and Operational Resilience
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSC-owned	Eventualmente disponibile su richiesta, è possibile condividere un riassunto generico, in quanto il documento, per policy aziendale, non può essere condiviso all'esterno				
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	Shared CSP and CSC					
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	Shared CSP and CSC	Procedura di Business Continuity Plan (paragrafo "testing")	BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSC-owned	Procedura di Business Continuity Plan (paragrafo "stakeholders")	BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	Procedura di backup e ripristino dei dati	BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup	
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	Shared CSP and CSC	Procedura di backup e ripristino dei dati (paragrafo "riservatezza,'integrità e disponibilità delle informazioni")				
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	Shared CSP and CSC	Procedura di backup e ripristino dei dati				
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	Shared CSP and CSC	Procedura di disaster recovery	BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	Shared CSP and CSC	Procedura di disaster recovery (paragrafo "revisione procedura") Procedura di change management (paragrafo "revisione procedura")				

ID	Question	Response	Ownership	Procedura	Control ID	Control Description	Control Name	Category
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	Shared CSP and CSC	Procedura di disaster recovery (paragrafo "testing")	BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	Response Plan Exercise	
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	NA	CSC-owned					
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes	Shared CSP and CSC	Dati conservati in ambiente cloud certificato e garantito	BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy	
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	Shared CSP and CSC	Procedura di change management (paragrafo "valutazione del rischio") Template registro di change management	CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy and Procedures	Change Control and Configuration Management
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	Procedura di change management (paragrafo "revisione procedura")				
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	Shared CSP and CSC	Procedura di change management (paragrafo "testing")	CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	Shared CSP and CSC	Procedura di change management (paragrafo "valutazione del rischio")	CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	Change Management Technology	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	Shared CSP and CSC	Procedura di change management (paragrafo "Change Advisory Board")	CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection	
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Yes	Shared CSP and CSC	SLA definiti nel contratto formalizzato con il CSP qualificato AgID	CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSC-owned	Procedura di change management (paragrafo "change baselines")	CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSC-owned	Procedura di change management (paragrafo "change baselines")	CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSC-owned	Procedura change management (paragrafo "configurations")	CCC-08	'Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.'	Exception Management	
CCC-08.2	'Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	CSC-owned	Procedura change management				
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	Shared CSP and CSC	Procedura change management (paragrafo "politiche di roll back")	CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Change Restoration	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	Procedura di crittografia dei dati e della gestione delle chiavi crittografiche	CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	Encryption and Key Management Policy and Procedures	
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and CSC	Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "revisione procedura")				
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSC-owned	Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "ruoli e responsabilità")	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	

CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSC-owned		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "gestione in-transit e at-rest") Su richiesta del cliente e' possibile cifrare i dati archiviati a riposo	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	Shared CSP and CSC		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "standard algoritmi")	CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm	
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	No	Shared CSP and CSC		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "gestione delle modifiche")	CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	No	Shared CSP and CSC		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "valutazione del rischio")	CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Encryption Change Cost Benefit Analysis	
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	Shared CSP and CSC		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "valutazione del rischio")	CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Yes	Shared CSP and CSC		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (cap. "gestione delle chiavi crittografiche")	CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability	
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	No	CSC-owned		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "valutazione del rischio")	CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	Encryption and Key Management Audit	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	No	CSC-owned		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "revisione procedura")				
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	CSC-owned		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "standard algoritmi")	CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSC-owned			CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	No	CSC-owned			CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation	Cryptography, Encryption & Key Management
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	No	CSC-owned			CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation	
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	CSC-owned		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "distruzione delle chiavi")	CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction	
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSC-owned			CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation	
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "sospensione delle chiavi")	CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Key Suspension	

	Question	Answer	Ownership		Notes (IT)	Ref	Control Description	Control Title
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "disattivazione delle chiavi")	CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Key Deactivation
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "archiviazione delle chiavi")	CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Key Archival
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSC-owned			CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Key Compromise
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSC-owned			CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Key Recovery
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	Shared CSP and CSC		Procedura di crittografia dei dati e della gestione delle chiavi crittografiche (paragrafo "inventario delle chiavi")	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Key Inventory Management
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned		Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che l'infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018	DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	Off-Site Equipment Disposal Policy and Procedures
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	Shared CSP and CSC		procedura di data retention (paragrafo "cancellazione dei dati")			
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	CSP-owned		Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che l'infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018			
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	NA	Shared CSP and CSC		Viene utilizzato un CSP certificato e qualificato AgID, pertanto non è possibile trasferire hardware, dati e software ad altri CSP che non siano certificati e qualificati	DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	Off-Site Transfer Authorization Policy and Procedures
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	NA	Shared CSP and CSC		Viene utilizzato un CSP certificato e qualificato AgID, pertanto non è possibile trasferire hardware, dati e software ad altri CSP che non siano certificati e qualificati			
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	NA	Shared CSP and CSC		Viene utilizzato un CSP certificato e qualificato AgID, pertanto non è possibile trasferire hardware, dati e software ad altri CSP che non siano certificati e qualificati			
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned		Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che l'infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018	DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures

	Question		Ownership	Notes		Control Description	Control Title	Domain
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che l'infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018			Procedures	
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	CSP-owned	Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che l'infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018	DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	CSP-owned	Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che l'infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018				
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	Shared CSP and CSC	Documento di Analisi dei rischi	DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	Datacenter Security
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned	Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018	DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	CSP-owned		DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	Controlled Access Points	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned					
DCS-08.1	Is equipment identification used as a method for connection authentication?	No	CSC-owned		DCS-08	Use equipment identification as a method for connection authentication.	Equipment Identification	
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	CSP-owned		DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned					
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	CSP-owned		DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	CSP-owned		DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	CSP-owned	Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018	DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Cabling Security	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	CSP-owned	Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018	DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Environmental Systems	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	Shared CSP and CSC	Piano di Business Continuity (BCP)	DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Secure Utilities	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	CSP-owned	Viene Utilizzato un datacenter di un CSP certificato e qualificato AgID, che garantisce che l'infrastruttura e i processi siano conformi a quanto previsto dalla ISO 27001, 27017 e 27018	DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Equipment Location	
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSC-owned	Procedura per la gestione della protezione dei dati personali	DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	Security and Privacy Policy and Procedures	

ID	Question		Ownership		Reference (IT)	Control ID	Control Description	Control Name	Domain
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Procedura per la gestione della protezione dei dati personali (paragrafo "revisione procedura")			...and Procedures	
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	CSC-owned		In conformita' al GDPR si provvede comunque alla cancellazione sicura dei dati come da procedura di data retention (paragrafo "cancellazione dei dati")	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	CSC-owned		Procedura per la gestione della protezione dei dati personali (paragrafo "inventario")	DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	No	CSC-owned			DSP-04	Classify data according to its type and sensitivity level.	Data Classification	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	Shared CSP and CSC		Procedura per la gestione della protezione dei dati personali (paragrafo "data mapping")		Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.		
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	Shared CSP and CSC		Procedura per la gestione della protezione dei dati personali (paragrafo "revisione procedura")	DSP-05		Data Flow Documentation	
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	Shared CSP and CSC		Procedura per la gestione della protezione dei dati personali (paragrafo "data mapping")		Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.		
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	No	CSC-owned		Procedura per la gestione della protezione dei dati personali (paragrafo "revisione procedura")	DSP-06		Data Ownership and Stewardship	
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSC-owned		In compliance con il GDPR (art. 25)	DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSC-owned		In compliance con il GDPR (art. 25)		Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.		
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	CSC-owned		In compliance con il GDPR (art. 25)	DSP-08		Data Privacy by Design and Default	
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	Yes	CSC-owned		In compliance con il GDPR (art.35)	DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment	Data Security and Privacy Lifecycle Management
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	CSC-owned		Procedura per la gestione della protezione dei dati personali (paragrafo "gestione categorie particolari di dati personali")	DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	CSC-owned		Procedura diritti dell'interessato	DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	CSC-owned		Procedura per la gestione della protezione dei dati personali (paragrafo "misure tecniche e organizzative")	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	Shared CSP and CSC		Procedura per la gestione della protezione dei dati personali (paragrafo "gestione sub-responsabili")	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	

ID	Question	Answer	Ownership			Riferimento (IT)		Control	Control Name	Domain
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	CSC-owned			Procedura per la gestione della protezione dei dati personali (paragrafo "gestione sub-responsabili")	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes	CSC-owned			Vengono utilizzati dati fittizi come prescritto dalle apposite procedure operative aziendali	DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	CSC-owned			Procedura di data retention	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSC-owned			Procedura per la gestione della protezione dei dati personali (paragrafo "gestione categorie particolari di dati personali")	DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	NA	CSC-owned			Non applicabile perché contrattualmente non è previsto che il CSP contrattualizzato acceda ai dati personali presenti nell'applicativo.	DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	Disclosure Notification	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	NA	CSP-owned			Non applicabile perché contrattualmente non è previsto che il CSP contrattualizzato acceda ai dati personali presenti nell'applicativo.				
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	Shared CSP and CSC			procedura di backup (paragrafo "localizzazione dei backup")	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location	
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned			Procedure legate alla ISO 9001	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	Governance Program Policy and Procedures	
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSC-owned			Procedure legate alla ISO 9001				
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSC-owned			Procedura valutazione dei rischi	GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program	Governance, Risk and Compliance
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSC-owned			Procedure legate alla ISO 9001 (revisioni)	GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews	
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSC-owned			Procedura di gestione delle Non Conformità (NC) e Azioni correttive (AC) come da ISO 9001	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSC-owned			Procedura di comunicazione con gli stakeholders	GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSC-owned			Procedure legate alla ISO 9001	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSC-owned			Coma da ISO 9001 (normative di settore)	GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	

ID	Question			Reference	ID2	Description	Control Name	Category
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	No	CSC-owned		GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Special Interest Groups	
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	Procedure legate alla ISO 9001	HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	Background Screening Policy and Procedures	
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes	CSC-owned	Procedure legate alla ISO 9001				
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSC-owned	Procedure legate alla ISO 9001				
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	Regolamento Informatico	HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	Acceptable Use of Technology Policy and Procedures	
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	CSC-owned	Regolamento Informatico (capitolo "revisione regolamento")				
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	Regolamento Informatico (capitolo "clean desk policy")	HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	Clean Desk Policy and Procedures	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSC-owned	Regolamento Informatico (capitolo "revisione regolamento")				
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	Regolamento Informatico (capitolo "telelavoro")	HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	Remote and Home Working Policy and Procedures	Human Resources
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	CSC-owned	Regolamento Informatico (capitolo "revisione regolamento")				
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli assets") Procedura di valutazione dei rischi (paragrafo	HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli assets") Procedura di valutazione dei rischi (paragrafo	HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Employment Termination	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSC-owned		HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSC-owned		HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSC-owned		HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities	

ID	Question	Answer	Ownership	Notes	Ref	Control Description	Control Title
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSC-owned		HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Non-Disclosure Agreements
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSC-owned		HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSC-owned				
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSC-owned	In compliance al GDPR	HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Personal and Sensitive Data Awareness and Training
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSC-owned	Procedura per la gestione della protezione dei dati personali (paragrafo "formazione")			
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	CSC-owned	Tramite ISO 9001	HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Compliance User Responsibility
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli accessi")	IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSC-owned	Regolamento Informatico (capitolo "revisione regolamento")			
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione delle password")	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSC-owned	Regolamento Informatico (capitolo "revisione regolamento") Vengono revisionate periodicamente o in caso di particolari necessità date da cambi di			
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSC-owned	Regolamento Informatico (capitolo "Inventario di sistema") I sistemi di autorizzazione e di autenticazione	IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	CSC-owned	Procedura per la gestione della protezione dei dati personali (paragrafo "ruoli e responsabilità")	IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli accessi")	IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli accessi")	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli accessi")	IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli accessi")	IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli accessi")	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	Segregation of Privileged Access Roles

ID	Question	Response	Ownership	Notes	Control ID	Control Description	Control Title	Domain
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli accessi")	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles	Identity & Access Management
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli accessi")				
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	NA	CSC-owned	Non sono previsti ruoli con accessi privilegiati che comportano un alto livello di rischio.	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	CSCs Approval for Agreed Privileged Access Roles	
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	NA	CSC-owned		IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	NA	CSC-owned					
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSC-owned	Regolamento Informatico (capitolo "termini e definizioni") Regolamento Informatico (capitolo "gestione degli accessi")	IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	Uniquely Identifiable Users	
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	No	CSC-owned	non vengono applicate soluzioni di strong authentication	IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	No	CSC-owned	non vengono applicate soluzioni di strong authentication				
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione delle password")	IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	CSC-owned	Regolamento Informatico (capitolo "gestione degli accessi")	IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms	
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "Interoperabilità dei sistemi)	IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	Interoperability and Portability Policy and Procedures	
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "Interoperabilità dei sistemi")				
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "Standard di sviluppo")				

ID	Question		Ownership	Reference	Control ID	Control Description	Control Name	Domain
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "Standard applicativi OWASP")				Interoperability & Portability
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "revisione procedura")				
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	CSC-owned		IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "Interoperabilità dei sistemi")	IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	CSC-owned		IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Data Portability Contractual Obligations	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "Virtualizzazione dei sistemi")	IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	Infrastructure and Virtualization Security Policy and Procedures	
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "revisione procedura")				
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "gestione della scalabilità del servizio")	IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning	
IVS-03.1	Are communications between environments monitored?	Yes	Shared CSP and CSC	regolamento informatico (capitolo "standard di sicurezza dell'interoperabilità dei sistemi")		Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.		
IVS-03.2	Are communications between environments encrypted?	Yes	Shared CSP and CSC	regolamento informatico (capitolo "standard di sicurezza dell'interoperabilità dei sistemi")				
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSC-owned	regolamento informatico (capitolo "standard di sicurezza dell'interoperabilità dei sistemi")	IVS-03		Network Security	Infrastructure & Virtualization Security
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSC-owned					
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSC-owned	regolamento informatico (capitolo "standard di sicurezza dell'interoperabilità dei sistemi")				

ID	Question				ID			
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	Shared CSP and CSC	procedura di sicurezza delle applicazioni (paragrafo "Standard applicativi OWASP") Schema di rete	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "Standard di sviluppo")	IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?		CSC-owned	Applicazione multi-tenant	IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSC-owned	procedura di sicurezza delle applicazioni (paragrafo "Interoperabilità dei sistemi")	IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSC-owned	Procedura di valutazione del rischio (paragrafo "classificazione dei rischi")	IVS-08	Identify and document high-risk environments.	Network Architecture Documentation	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	CSC-owned	Procedura di incident management Procedura di valutazione del rischio (paragrafo "misure di sicurezza")	IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	Regolamento informatico (capitolo " gestione log management")	LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures	
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSC-owned	Regolamento informatico (capitolo "gestione log management")				
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSC-owned	Regolamento informatico (capitolo "gestione log management")	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSC-owned	Procedura di incident management (paragrafo "gestione degli eventi") Regolamento informatico (capitolo "gestione log management")	LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	Security Monitoring and Alerting	
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	Shared CSP and CSC	Procedura di incident management (paragrafo "gestione degli eventi") Procedura di data breach (paragrafo "gestione data breach in qualità di responsabile del trattamento")				
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSC-owned	Registro eventi sicurezza Registro violazione dei dati	LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSC-owned	Regolamento informatico (capitolo "gestione log management") Registri di log applicativi e di sistema	LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Audit Logs Monitoring and Response	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSC-owned	Procedura di incident management (paragrafo "gestione degli eventi")				
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSC-owned		LOG-06	Use a reliable time source across all relevant information processing systems.	Clock Synchronization	Logging and Monitoring
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSC-owned	Regolamento informatico (capitolo "gestione log management") Registri di log applicativi e di sistema In compliace con la normativa sulla protezione dei dati (riferimento normativo: Regolamento informatico (capitolo "gestione log management")	LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	Logging Scope	
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSC-owned					

ID	Question	Response	Ownership	Reference (IT)	Control ID	Control Description	Control Title	Domain
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSC-owned	Registri di log applicativi e di sistema	LOG-08	Generate audit records containing relevant security information.	Log Records	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSC-owned	Regolamento informatico (capitolo "gestione log management") Registri di log applicativi e di sistema	LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	No	Shared CSP and CSC		LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	No	CSC-owned		LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	NA	CSC-owned		LOG-12	Monitor and log physical access using an auditable access control system.	Access Control Logs	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSC-owned	Procedura di incident management (paragrafo "gestione degli eventi") Registri di log applicativi e di sistema	LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Failures and Anomalies Reporting	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSC-owned	Procedura di incident management (paragrafo "gestione degli eventi")				
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	Procedura di incident management (paragrafo "gestione degli eventi") Non si applica il processo di 'e-discovery' (recupero di prove digitali per finalità forensi)	SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	Security Incident Management Policy and Procedures	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSC-owned	Procedura di incident management (paragrafo "revisione procedura")				
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	Procedura di incident management	SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	Service Management Policy and Procedures	
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSC-owned	Procedura di incident management (paragrafo "revisione procedura")				
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	Procedura di incident management (paragrafo "gestione degli eventi") Procedura di disaster recovery Procedura legata alla Business Continuity + piano di Business Continuity (BCP)	SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.'	Incident Response Plans	
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSC-owned	Procedura di disaster recovery (paragrafo "testing") Registri di test disaster recovery effettuati + indicatori di efficienza Procedura legata alla Business Continuity +	SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing	
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSC-owned	Procedura di disaster recovery (paragrafo "RPO e RTO")	SEF-05	Establish and monitor information security incident metrics.	Incident Response Metrics	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSC-owned	Procedura di valutazione del rischio (paragrafo "remediation")	SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSC-owned	Procedura di data breach (paragrafo "gestione data breach in qualità di responsabile del trattamento"). Ricomprende anche la gestione delle informazioni per aiutare il titolare del trattamento a procedere alla notifiche da inviare al Garante + agli interessati (artt. 33-34 GDPR)	SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Breach Notification	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSC-owned	Procedura di data breach (paragrafo "gestione data breach in qualità di responsabile del trattamento"). Ricomprende anche la gestione delle informazioni per aiutare il titolare del trattamento a procedere alla notifiche da inviare al Garante + agli interessati (artt. 33-34 GDPR)				
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSC-owned	In caso di data breach vengono applicate le modalità previste sul sito del Garante per la protezione dei dati personali.	SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	Points of Contact Maintenance	

ID	Question	Answer	Ownership	Note	Control ID	Description	Control Name	Domain
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned	Valutazione fornitori annuale tramite ISO 9001	STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	SSRM Policy and Procedures	Supply Chain Management, Transparency, and Accountability
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSC-owned	Valutazione fornitori annuale tramite ISO 9001				
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	Shared CSP and CSC	Procedura ISO 9001	STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain	
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSC-owned	Accessibile su richiesta del cliente	STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance	
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	Shared CSP and CSC		STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSC-owned		STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSC-owned		STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSC-owned	Procedura ISO 9001	STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	E' prevista nell'analisi dei rischi	STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management	
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	CSP-owned		STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy	Primary Service and Contractual Agreement	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned	Procedura ISO 9001	STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review	
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	Shared CSP and CSC	Procedura ISO 9001	STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	Internal Compliance Testing	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	Shared CSP and CSC	CSP certificato ISO 27001	STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	Supply Chain Service Agreement Compliance	
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSC-owned	Procedura ISO 9001	STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	Supply Chain Governance Review	
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSC-owned	Procedura ISO 9001	STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment	
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	CSC-owned	Procedura di sicurezza delle applicazioni (paragrafo "remediation" + paragrafo "standard applicativi OWASP")	TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	Threat and Vulnerability Management Policy and Procedures	
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSC-owned	Procedura di sicurezza delle applicazioni (paragrafo "remediation" + paragrafo "standard applicativi OWASP")				

ID	Question				Reference	Group	Description	Control	Domain
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned		Procedura di sicurezza delle applicazioni (paragrafo "politica di gestione delle minacce e pianificazione")	TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy and Procedures	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Procedura di sicurezza delle applicazioni (paragrafo "politica di gestione delle minacce e pianificazione")				
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications(based on the identified risk)?	Yes	CSC-owned		Procedura di sicurezza delle applicazioni (paragrafo "gestione delle release" + paragrafo "standard applicativi OWASP")	TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSC-owned		Regolamento informatico (capitolo "Antivirus e sistemi di protezione") Antivirus con aggiornamento automatico	TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	Threat & Vulnerability Management
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	CSC-owned		procedura di sicurezza delle applicazioni (paragrafo "Interoperabilità dei sistemi")	TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSC-owned		procedura di sicurezza delle applicazioni (paragrafo "testing") PT effettuati almeno una volta all'anno	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Penetration Testing	
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	CSC-owned		procedura di sicurezza delle applicazioni (paragrafo "testing") VA effettuate almeno una volta all'anno	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	CSC-owned		Procedura di sicurezza delle applicazioni (paragrafo "remediation" + paragrafo "standard applicativi OWASP")	TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSC-owned		procedura di sicurezza delle applicazioni (paragrafo "testing") Su richiesta del cliente	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSC-owned		procedura di sicurezza delle applicazioni (paragrafo "testing")	TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSC-owned		Regolamento informatico (capitolo "endpoint security")	UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	Endpoint Devices Policy and Procedures	
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Regolamento informatico (capitolo "endpoint security")				
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Yes	CSC-owned		Regolamento informatico (capitolo "whitelist")	UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSC-owned		Regolamento informatico (capitolo "endpoint security")	UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSC-owned		Asset inventory	UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSC-owned		Regolamento informatico (capitolo "endpoint security")	UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSC-owned		Regolamento Informatico (capitolo "clean desk policy")	UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	Universal Endpoint Management
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSC-owned		procedura change management (paragrafo "gestione modifiche endpoint")	UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	

UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	NA	CSC-owned		Le informazioni non sono archiviate sugli endpoint	UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	No	CSC-owned			UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSC-owned		procedura di sicurezza delle applicazioni (paragrafo "endpoint")	UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Yes	CSC-owned		procedura di sicurezza delle applicazioni (paragrafo "endpoint") Regolamento informatico (capitolo "endpoint	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	NA	CSC-owned		Non viene applicata la funzionalità di geolocalizzazione remota	UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	No	CSC-owned			UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	NA	CSC-owned		Non vengono utilizzati endpoint di terze parti.	UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	Third-Party Endpoint Security Posture

End of Standard