

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
Application & Interface Security <i>Application Security</i>	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			As a general, the software applications developed implement security concepts, based on OWASP recommendations and ISO Standard
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?		X		There are multiple kinds of application security tests that could be potentially integrated into development and deployment of applications: Code review, Unit testing, Regression Testing and functional testing, Static Application Security Testing and DAST
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	X			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			Does not rely on software suppliers, tests are carried out in a similar way to the internally developed code
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Multiple scanning techniques be used before the promotion of code into production.
Application & Interface Security <i>Customer Access Requirements</i>	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security,	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			In accordance with the GDPR and privacy by design principles
		AIS-02.2		Are all requirements and trust levels for customers' access defined and documented?	X			Requirements and trust levels for client access are established contractually
Application & Interface Security <i>Data Integrity</i>	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			Typically, there is no gaps in either protection of, or accountability for personal data. Are performed Data Integrity controls, and Clients are ultimately responsible for the data integrity of their workload
		AIS-03.2		Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			
Application & Interface Security <i>Data Security / Integrity</i>	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration or	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			Data Security Architecture are designed in line with CSA. As a general principle the continuous protection of personal data across the entire domain, whether the personal data is at rest, in motion or in use from initial collection through to destruction Data is encrypted in transit.

Audit Assurance & Compliance <i>Audit Planning</i>	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions.	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	X		Periodically are performed internal and external audits
		AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?	X		In accordance with our security incident management process
Audit Assurance & Compliance <i>Independent Audits</i>	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X		on customer request
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X		In accordance with the company security baselines and the ISO / IEC 27001 standard recommendations. Currently carried out internally
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X		In accordance with the company security baselines and the ISO / IEC 27001 standard recommendations. Currently carried out internally
		AAC-02.4		Do you conduct internal audits at least annually?	X		
		AAC-02.5		Do you conduct independent audits at least annually?	X		Periodically or on customer request
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	X		Executive Summary is available upon request and NDA subscription
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	X		upon customer request and NDA subscription
Audit Assurance & Compliance <i>Information System Regulatory Mapping</i>	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X		Meeting and Workshop are organized to evaluate treats, vulnerabilities, the policies and regulatory requirements governing privacy conformanceand takes decisions.
Business Continuity Management & Operational Resilience <i>Business Continuity Planning</i>	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X		
		BCR-01.2		Do you have more than one provider for each service you depend on?		X	
		BCR-01.3		Do you provide a disaster recovery capability?	X		
		BCR-01.4		Do you monitor service continuity with upstream providers in the event of provider failure?	X		
		BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?	X		On customer request
		BCR-01.6		Do you provide a tenant-triggered failover option?		X	Failover isn't automatic

		BCR-01.7	addressing priorities for testing, maintenance, and information	Do you share your business continuity and redundancy plans with your tenants?	X			On customer request
Business Continuity Management & Operational Resilience <i>Business Continuity Testing</i>	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Business continuity plans are regularly tested at least on an annual basis
Business Continuity Management & Operational Resilience <i>Power / Telecommunications</i>	BCR-03	BCR-03.1	Data center utilities services and	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?			X	As SaaS provider, we rely on qualified Infrastructure provider
		BCR-03.2	environmental conditions (e.g., water, power, temperature and humidity controls, telecommunicatio	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?			X	
Business Continuity Management & Operational Resilience <i>Documentation</i>	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: <ul style="list-style-type: none"> • Configuring, installing, and operating the information system • Effectively using the customer's 	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			technical documentation is provided authorized technical staff

<p>Business Continuity Management & Operational Resilience <i>Environmental Risks</i></p>	<p>BCR-05</p>	<p>BCR-05.1</p>	<p>Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated</p>	<p>Is physical damage anticipated and are countermeasures included in the design of physical protections?</p>			<p>X</p>	<p>As SaaS provider, we rely on qualified Infrastructure provider</p>
<p>Business Continuity Management & Operational Resilience <i>Equipment Location</i></p>	<p>BCR-06</p>	<p>BCR-06.1</p>	<p>To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable</p>	<p>Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?</p>			<p>X</p>	<p>As SaaS provider, we rely on qualified Infrastructure provider. It guarantees the data centers located</p>
<p>Business Continuity Management & Operational Resilience <i>Equipment Maintenance</i></p>	<p>BCR-07</p>	<p>BCR-07.1</p>	<p>Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and</p>	<p>Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?</p>			<p>X</p>	<p>As SaaS provider, we rely on qualified Infrastructure provider. It guarantees that all procedures are in lines with international sector standards</p>
<p>BCR-07.2</p>		<p>Do you have an equipment and datacenter maintenance routine or plan?</p>			<p>X</p>			

Business Continuity Management & Operational Resilience <i>Equipment Power Failures</i>	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?			X	As SaaS provider, we rely on qualified Infrastructure provider. It guarantees that sector's best practices were redundant.
Business Continuity Management & Operational Resilience <i>Impact Analysis</i>	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: 1. Identify critical	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			In accordance with ISO Standards
		BCR-09.2		Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			In accordance with ISO Standards
Business Continuity Management & Operational Resilience <i>Policy</i>	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			In accordance with ISO Standards
Business Continuity Management & Operational Resilience <i>Retention Policy</i>	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and	Do you have technical capabilities to enforce tenant data retention policies?	X			Retention policy is managed
		BCR-11.2		Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	X			In line with GDPR and contractual agreements
		BCR-11.3		Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			
		BCR-11.4		If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			As SaaS provider, we rely on qualified Infrastructure provider. It guarantees that guarantee the replacement of the assigned hardware
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?			X	We do not allow to Clients to admin the VMs
		BCR-11.6		Does your cloud solution include software/provider independent restore and recovery capabilities?	X			
		BCR-11.7		Do you test your backup or redundancy mechanisms at least annually?	X			

Change Control & Configuration Management <i>New Development / Acquisition</i>	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X		In accordance with quality procedures
Change Control & Configuration Management	CCC-02	CCC-02.1	External business partners shall adhere to the	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	X		In accordance with quality procedures
		CCC-02.2		Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	X		In accordance with quality procedures
Change Control & Configuration Management <i>Quality Testing</i>	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X		In accordance with quality procedures
		CCC-03.2		Is documentation describing known issues with certain products/services available?	X		Is implemented a problem Management that controls the registration, processing and documentation of fault messages (incidents), problems, known errors, workarounds. The release process oversees all the stages involved in a software release from development and testing to deployment
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X		
		CCC-03.4		Do you have controls in place to ensure that standards of quality are being met for all software development?	X		
		CCC-03.5		Do you have controls in place to detect source code security defects for any outsourced software development activities?	X		
		CCC-03.6		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X		

Change Control & Configuration Management <i>Unauthorized Software Installations</i>	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X		
Change Control & Configuration Management <i>Production Changes</i>	CCC-05	CCC-05.1	Policies and procedures shall be established for	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	X		On customer request
		CCC-05.2	managing the risks associated with	Do you have policies and procedures established for managing risks with respect to change management in production environments?	X		
		CCC-05.3	production changes	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	X		Is Maintained an continuous deployment process
Data Security & Information Lifecycle Management <i>Data Security & Information Lifecycle Management</i>	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	X		Are maintains cloud asset inventory
		DSI-01.2	classification by	Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	X		As SaaS provider, we rely on qualified Infrastructure provider that manage and maintain hardware
Data Security & Information Lifecycle Management <i>Data Inventory / Flows</i>	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	X		In line with GDPR and data processor accordance
		DSI-02.2	measures implemented, to	Can you ensure that data does not migrate beyond a defined geographical residency?	X		In line with GDPR and data processor accordance
Data Security & Information Lifecycle Management	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?		X	Typically, data are encrypted in transit using TLS 1.2. communications between infrastructure components over Internet are encrypted
		DSI-03.2	commerce (e-commerce) that	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?		X	
Data Security & Information Lifecycle Management <i>Handling / Labeling /</i>	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	X		Standard within GDPR compliant and ISO standard recommendations
		DSI-04.2	labeling, handling, and the security of	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		X	
		DSI-04.3	and the security of	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?		X	

Data Security & Information Lifecycle Management <i>Nonproduction Data</i>	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			recommendations of the ISO standard and GDPR
Data Security & Information Lifecycle Management <i>Ownership / Stewardship</i>	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			As agreed in th term of service, privacy policy and related documents
Data Security & Information Lifecycle Management <i>Secure Disposal</i>	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			Wipe mechanism is performed
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			As documented in the Privacy policy and term of service
Datacenter Security <i>Asset Management</i>	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			Part of Asset management processes accoding to ISO Standard
		DCS-01.2		Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X			
Datacenter Security <i>Controlled Access Points</i>	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?			X	physical security measures are adopts by the infrastructure provider
Datacenter Security <i>Equipment Identification</i>	DCS-03	DCS-03.1	Automated equipment identification shall be used as a	Do you have a capability to use system geographic location as an authentication factor?			X	

		DCS-03.2	method of connection authentication. Location-aware	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?			X	As SaaS provider, we rely on qualified Infrastructure provider that including equipment identification
Datacenter Security Offsite Authorization	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			Customer authorization is requested
Datacenter Security Offsite Equipment	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored	Can you provide tenants with your asset management policies and procedures?			X	Service is implemented on DataCenter of the qualified Infrastructure provider
Datacenter Security Policy	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			Service is implemented on DataCenter of the qualified provider infrastructure that ensures compliance with regulations
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			Session training are performed
Datacenter Security Secure Area Authorization	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	X			Service is implemented on DataCenter of the qualified provider infrastructure that ensures compliance with regulations

Datacenter Security Unauthorized Persons Entry	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise and	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X		Service is implemented on DataCenter of the qualified provider infrastructure that ensures compliance with regulations
Datacenter Security User Access	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X		Service is implemented on DataCenter of the qualified provider infrastructure that ensures guarantees the support of technical team
Encryption & Key Management Entitlement	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management	Do you have key management policies binding keys to identifiable owners?		X	All the network traffic is using the latest encryption standards
Encryption & Key Management Key Generation	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic	Do you have a capability to allow creation of unique encryption keys per tenant?		X	
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?		X	
		EKM-02.3		Do you maintain key management procedures?		X	
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?		X	
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?		X	
Encryption & Key Management Encryption	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures	Do you encrypt tenant data at rest (on disk/storage) within your environment?		X	
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X		In the event of travel, virtual machines are encrypted during transport
		EKM-03.3		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?		X	
Encryption & Key Management Storage and Access	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?		X	
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?		X	
		EKM-04.3		Do you store encryption keys in the cloud?		X	
		EKM-04.4		Do you have separate key management and key usage duties?		X	
Governance and Risk Management Baseline Requirements	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired,	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X		
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X		ISO 27001 and ISO 9001, both externally audited on an annual basis
Governance and Risk Management Risk Assessments	GRM-02	GRM-02.1	Risk assessments associated with data governance	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X		Standard within GDPR
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X		

Governance and Risk Management Oversight	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X		In accordance with ISO Standards, security policy are implemented and monitored in considering the characteristics of the business, location, asset and technology, legal and regulatory environment and stakeholders needs
Governance and Risk Management	GRM-04	GRM-04.1	An Information Security Management	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		X	On customer request
Governance and Risk Management		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?		X	In accordance with the company security baselines and Solari has planned the standard certification to ISO 27001
Governance and Risk Management Support / Involvement	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X		Is Established executive leadership and commitment to operationalizing
Governance and Risk Management Policy	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X		In accordance with ISO Standards
		GRM-06.2		Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	X		
		GRM-06.3		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X		
		GRM-06.4		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X		On customer request
		GRM-06.5		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X		Certificates are available if required
Governance and Risk Management Policy Enforcement	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X		Based on ISO Standards and part of standard employment terms
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X		
Governance and Risk Management Business / Policy Change Impacts	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X		Review adequacy of existing security policies, standards, guidelines and procedures in accordance with ISO standard and recommendations
Governance and Risk Management Policy Reviews	GRM-09	GRM-09.1	The organization's business leadership for	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X		Clients are informed through the institutional website, mail in relation to changes privacy policies
Governance and Risk Management Assessments	GRM-10	GRM-09.2	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least	Do you perform, at minimum, annual reviews to your privacy and security policies?	X		Regular risk assessments are conducted according to ISO standards
		GRM-10.1		Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X		
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X		Impact and likelihood of risks shall be determined using statistical method
Governance and Risk Management Program	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level.	Do you have a documented, organization-wide program in place to manage risk?	X		Covered as part of ISO 9001

		GRM-11.2	Acceptance levels based on risk criteria shall be established and	Do you make available documentation of your organization-wide risk management program?	X			On customer request
Human Resources Asset Returns	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			in consideration of the quality system procedures and contractual terms of the employees
		HRS-01.2	external business relationships, all organizationally-	Do you have asset return procedures outlining how assets should be returned within an established period?	X			
Human Resources Background Screening	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			
Human Resources Employment Agreements	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			
		HRS-03.2	terms for adherence to established	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	X			
Human Resources Employment Termination	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			Employee management procedures are maintained, including changes in employment and resolution
		HRS-04.2	change in employment procedures shall	Do the above procedures and guidelines account for timely revocation of access and return of assets?+E130:E131	X			

Human Resources <i>Portable / Mobile Devices</i>	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			No mobile device can be interfaced with the data of the system host client. There are established instructions
Human Resources <i>Non-Disclosure Agreements</i>	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			The requirements for confidentiality agreements relating to data protection are established
Human Resources <i>Roles / Responsibilities</i>	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			Roles and responsibilities are documented when using the SaaS solution
Human Resources <i>Acceptable Use</i>	HRS-08	HRS-08.1	Policies and procedures shall be established,	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			

		HRS-08.2	and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?		X		The use of company devices is governed by specific instructions, provided and initiated by all employees. The use of the personal device is not allowed unless strictly authorized
Human Resources Training / Awareness	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?		X		All employees complete annual Information Security Awareness training based to a specific role and responsibilities, in accordance with ISO standards, GDPR
		HRS-09.2		Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			
		HRS-09.3		Do you document employee acknowledgment of training they have completed?	X			
		HRS-09.4		Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?		X		
		HRS-09.5		Are personnel trained and provided with awareness programs at least once a year?	X			
		HRS-09.6		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			
Human Resources User Responsibility	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			Based on ISO standard, processes and standard employment terms
		HRS-10.2		Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			
		HRS-10.3		Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			
Human Resources Workspace	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			Internal rules and recommendations and good practices
		HRS-11.2		Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X			
Identity & Access Management Audit Tools Access	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			Segregation of access control roles (e.g. access request, access authorization, access administration) should be clearly defined and documented.
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			

Identity & Access Management <i>User Access Policy</i>	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			De-provisioning process is in place
		IAM-02.2		Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	X			Access to assets is regulated on ISO Standard
		IAM-02.3		Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	X			Refer on Access control policy on ISO standard
		IAM-02.4		Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X			
		IAM-02.5		Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X			An access control policy should be detailed and documented. Solari SpA should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data
		IAM-02.6		Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?		X		Multifactor authentication is not available
		IAM-02.7		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	X			Systems access is removed within 2 business days as when change in the user's role takes place
Identity & Access Management <i>Diagnostic / Configuration Ports Access</i>	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			configuration ports is reserved only for system administrators
Identity & Access Management <i>Policies and Procedures</i>	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			Identity management is in place. Refer on Access Control procedures
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			
Identity & Access Management <i>Segregation of Duties</i>	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			They are defined contractually. There are technical documents that inform the customer about the basic security measures
Identity & Access Management <i>Source Code Access Restriction</i>	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Refer on Information security roles and responsibilities
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			
Identity & Access Management <i>Third Party Access</i>	IAM-07	IAM-07.1	The identification, assessment, and prioritization of	Does your organization conduct third-party unauthorized access risk assessments?	X			Risks related to third party and access controls is performed as part of risk management program; are performed negotiation tactics

		IAM-07.2	risks posed by business processes	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	X			of risk management program, are performed penetration testing and policy password
Identity & Access Management User Access Restriction / Authorization	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	X			Client must approve the access to their data in case of support. SOLARI staff is not allowed to access client data unless emergency situation.
		IAM-08.2		Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	X			Clients are responsible for controls related to their usage of the SaaS platform
		IAM-08.3		Do you limit identities' replication only to users explicitly defined as business necessary?	X			Excessive access rights should be clearly defined and assigned to limited specific members. Access is monitored and audit log collected
Identity & Access Management User Access Authorization	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers)	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			There is a process of releasing credentials
		IAM-09.2	and/or supplier	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?		X		Is allow only access to published SaaS platform
Identity & Access Management User Access Reviews	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			Periodic access checks are performed to validate appropriate access provisioning. Access is revoked if the members is terminated
		IAM-10.2		Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			In line with ISO standard and GDPR regulation, they are periodically audited on authorizations granted to AdS
		IAM-10.3		Do you ensure that remediation actions for access violations follow user access policies?	X			
		IAM-10.4		Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	X			
Identity & Access Management User Access Revocation	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			SOLARI for its employees and partners has put in place procedures and processes in order to vary and revoke access to users. The control of the users of the SAAS service is requested directly from the Client
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			
Identity & Access Management User ID Credentials	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			On Client request, is possible to integrates with existing customers SSO solutions and uses industry standards SAML
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	X			
		IAM-12.3	credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X			
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		X		
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?		X		Only role based
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?		X		Default authentication provider doesn't support multifactor authentication
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?		X		SaaS platform supports third party identity assurance services
		IAM-12.8		Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X			A specific password policy should be defined and documented
		IAM-12.9	• Identity trust	Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			

		IAM-12.10 IAM-12.11	verification and service-to-service application (API)	Do you support the ability to force password changes upon first logon?	X			A specific password policy should be defined and documented
				Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			
Identity & Access Management Utility Programs Access	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			Systems component are monitoring in line with ISO standard
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			WAF in place. We rely on the cloud provider infrastructure
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X			Logging and monitoring procedure
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	X			Incident response procedure
		IVS-01.4		Are audit logs centrally stored and retained?	X			Audit logs are stored in secure storage
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			Alerts are configured for key security events
Infrastructure & Virtualization Security Change Detection	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			Servers image are monitored and protected
		IVS-02.2		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X			Production systems are monitored and audit log is collected in safety. Mechanisms are in place for identifying changes to the virtual machine configuration
		IVS-02.3		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?			X	Client do not interact with the hypervisor, physical infrastructure, image asset management
Infrastructure & Virtualization Security Clock Synchronization	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			Is used the NTP (Network Time Protocol)
Infrastructure & Virtualization Security Capacity / Resource Planning	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared and	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	X			
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			X	

		IVS-04.3	prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			There are monitoring systems in order to optimize the system performance to meet requirements on an ongoing basis regulations and contracts for all systems that provide the service
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			
Infrastructure & Virtualization Security <i>Management - Vulnerability Management</i>	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization)	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			Recommendations of the technologies used are considered
Infrastructure & Virtualization Security <i>Network Security</i>	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			X	Periodically reviews and updates network architecture diagrams and each changes are documented
		IVS-06.2	These configurations shall be reviewed at least annually, and supported by	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X			
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X			
		IVS-06.4		Are all firewall access control lists documented with business justification?	X			
Infrastructure & Virtualization Security <i>OS Hardening and Base Controls</i>	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			hardening best practices are for all hosts within the infrastructure
Infrastructure & Virtualization Security <i>Production / Non-Production Environments</i>	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Are maintained environments separate from production for testing. These environments are not accessible to Clients
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			X	
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	X			Network segmentation is aligned. The production environment is completely segregated
Infrastructure & Virtualization Security <i>Segmentation</i>	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			All network and system environments are protected by firewalls in accordance with requirements ISO standards. legislative.

		IVS-09.2	and virtual applications, and infrastructure system and network components, shall be designed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			in adherence with requirements for statutory, regulatory, regulatory and contractual
		IVS-09.3		Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?			X	Access to the infrastructure by Clients is not allowed
		IVS-09.4		Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			Data reside on separate database with common processing systems.
		IVS-09.5		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			All network and system environments are protected by firewalls in order to meet security requirements in accordance with ISOstandard standards, in addition to legislative, regulatory and contractual requirements
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			Secured and encrypted communication channels are used. Work on the infrastructure that provides the SaaS service is carried out only by authorized technical personnel. Typically, migration operations are always carried out with the help of technical staff.
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?			X	
Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			SOLARI applies the principle of least privilege, allowing your users of the systems that provide the SaaS platform only the access necessary for carry out their work duties.
Infrastructure & Virtualization Security Wireless Security	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	X			the SaaS platform back-end system environment is not directly accessible via a wireless network. Are in place the necessary measures to protect its network from unauthorized access

		IVS-12.2	measures implemented, to protect wireless network	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	X			measures to protect the network from unauthorized access
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	X			
Infrastructure & Virtualization Security Network Architecture	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	X			Network architecture diagram exists. SaaS platform infrastructure utilizes a multi-tier design that segregates the database tier from web and application tiers using firewalls and network ACL
		IVS-13.2	high-risk environments and data flows that may have legal compliance	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	X			As SaaS we rely on the qualified CSP that include these standards
Interoperability & Portability APIs	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			APIs by the SaaS platform are available and published
Interoperability & Portability Data Request	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			Data is exported in open standard formats
Interoperability & Portability Policy & Legal	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	X			The policies and procedures are released regulate the use of the SaaS platform Service and technical documentation for interoperability
		IPY-03.2	requirements for service-to-service application (API) and information processing interoperability	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		X		All the functions relating to the infrastructure hosting the SaaS platform can be managed only by technical staff.
		IPY-03.3	interoperability	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X			At the contractual level, the policies and procedures are released regulate the use of the SaaS platform and with the support of the technical staff
Interoperability & Portability Standardized Network Protocols	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			Interactions with the application (e.g., API calls, login, etc.) are encrypted in transit.
		IPY-04.2	standardized network protocols	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			On request
Interoperability & Portability Virtualization	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			
		IPY-05.2	recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	X			On request
		IPY-05.3	platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	X			Client do not interact

Mobile Security <i>Anti-Malware</i>	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?		X		Refer on Information security awareness, education and training policy. Mobile device security is part of the annual security awareness training
Mobile Security <i>Application Stores</i>	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?		X		It is recommended to loaded applications only from approved application stores
Mobile Security <i>Approved Applications</i>	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?		X		It is recommended to loaded applications only from approved application stores
Mobile Security <i>Approved Software for BYOD</i>	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	The use of BYOD devices is not allowed

Mobile Security <i>Awareness and Training</i>	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?		X	
Mobile Security <i>Cloud Based Services</i>	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?		X	It is recommended a list of approved cloud services that can be used for certain business uses.
Mobile Security <i>Compatibility</i>	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?		X	
Mobile Security <i>Device Eligibility</i>	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?		X	Not allowed

Mobile Security <i>Device Inventory</i>	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	X			Is limited to business devices
Mobile Security <i>Device Management</i>	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?		X		
Mobile Security <i>Encryption</i>	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	X			Is limited to laptop
Mobile Security <i>Jailbreaking and Rooting</i>	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	X			
		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?		X		
Mobile Security <i>Legal</i>	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	The use of BYOD devices is not allowed
		MOS-13.2		Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?			X	
Mobile Security <i>Lockout Screen</i>	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	

Mobile Security Operating Systems	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?		X			
Mobile Security Passwords	MOS-16	MOS-16.1	Password policies, applicable to mobile devices.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?		X			
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?		X			
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X	All mobile devices and BYOD have required passwords	
Mobile Security Policy	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	The use of BYOD devices is not allowed	
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X		
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X		
Mobile Security Remote Wipe	MOS-18	MOS-18.1	All mobile devices permitted for use	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	The use of BYOD devices is not allowed	
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			X		
Mobile Security Security Patches	MOS-19	MOS-19.1	Mobile devices connecting to corporate	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?		X		It is recommended	
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X		
Mobile Security Users	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	The use of BYOD devices is not allowed	
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?					X
Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			In close collaboration with experts from national Authorities.	
Security Incident Management, E-Discovery, & Cloud Forensics Incident Management	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical	Do you have a documented security incident response plan?	X			Are developed plans, procedures and response programs to incident in according to ISO standard and GDPR regulation. Security issues are communicated in accordance with appropriate confidentiality methods. The security plans are subjected to annual verification tests. Refer on Incidents handling / Personal data breaches procedures	
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?			X		
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		X			

		SEF-02.4		Have you tested your security incident response plans in the last year?	X			
Security Incident Management, E-Discovery, & Cloud Forensics <i>Incident Reporting</i>	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	X			
		SEF-03.2		Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			Communications with all parties take place through ordinary email service, system ticketing
Security Incident Management, E-Discovery, & Cloud Forensics <i>Incident Response Legal Preparation</i>	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification,	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			The response plans comply with ISO standards. SOLARI is available to collaborate with the law
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?		X		
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			using Snapshot
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			Separation of tenant data is applied
Security Incident Management, E-Discovery, & Cloud Forensics <i>Incident Response Metrics</i>	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			Security incidents that include quantifying and monitoring types of incidents, volumes of activity are documented
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?		X		Upon request and non-disclosure agreements
Supply Chain Management, Transparency, and Accountability <i>Data Quality and Integrity</i>	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	X			Refer on Supplier relationships procedure. Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) are defined, documented and agreed
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X			
Supply Chain Management, Transparency, and Accountability <i>Incident Reporting</i>	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			Security incident information is communicated using confidentially agreed methods
Supply Chain Management, Transparency, and Accountability <i>Network / Infrastructure Services</i>	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			Monitors system capacity
		STA-03.2		Do you provide tenants with capacity planning and use reports?		X		

Supply Chain Management, Transparency, and Accountability <i>Provider Internal Assessments</i>	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			Based on ISO standards annually
Supply Chain Management, Transparency, and Accountability <i>Third Party Agreements</i>	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			Any agreements with third parties are examined by the Legal and privacy office. Each supplier must declare where it will process customer data. Clients are informed if the data are processed outside the territory of the European Union
		STA-05.2		Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			
		STA-05.3		Does legal counsel review all third-party agreements?	X			
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X			Security system was designed and implemented to meet industry best practices on security in line with ISO standard. Audits and questionnaires are implemented towards suppliers aimed at verifying their maturity with respect to security issues
		STA-05.5		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			Backup and data restore procedures are defined, documented and clearly linked to roles and responsibilities
		STA-05.6		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			Datacenter located on the Italian territory and in the European regions
		STA-05.7		Can you provide the physical location/geography of storage of a tenant's data upon request?	X			The location of the data is communicated in advance by the client and they are not moved except after prior communication
		STA-05.8		Can you provide the physical location/geography of storage of a tenant's data in advance?	X			
		STA-05.9		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		X		
		STA-05.10		Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X			Incidents and personal data breaches are recorded along with details regarding the event and subsequent mitigation actions performed
		STA-05.11		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		X		
		STA-05.12		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	X			Customers can request copies of the agreements between parties / people involved
Supply Chain Management, Transparency, and Accountability <i>Supply Chain Governance Reviews</i>	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	X			Are maintained agreements with key third party suppliers

Supply Chain Management, Transparency, and Accountability <i>Supply Chain Metrics</i>	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X		Processes/Procedures related to the processing of personal data are documented. Periodically Service agreement are reviewed
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	X		The supply chain is regulated by contractual requirements. The security policy can perform on-site audit, if necessary
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X		Periodically reviews service level agreements
		STA-07.4		Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X		Upon request
		STA-07.5		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X		Upon request
		STA-07.6		Do you provide customers with ongoing visibility and reporting of your SLA performance?	X		Upon request
		STA-07.7		Do your data management policies and procedures address tenant and service level conflicts of interests?	X		The roles are defined contractually
		STA-07.8		Do you review all service level agreements at least annually?	X		
Supply Chain Management, Transparency, and Accountability <i>Third Party Assessment</i>	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review	Do you assure reasonable information security across your information supply chain by performing an annual review?	X		Key suppliers are validated annually in accordance con ISO Standard recommendations
		STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			
Supply Chain Management, Transparency, and Accountability <i>Third Party Audits</i>	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions,	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	X		Upon request
		STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X		An external auditor performs an audit, in accordance with specific laws e internal regulation	
Threat and Vulnerability Management <i>Antivirus / Malicious Software</i>	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented to	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	X		Anti-malware are installed on virtual machines
		TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X		Server based anti-malware systems are automatically updated	
Threat and Vulnerability Management <i>Vulnerability / Patch Management</i>	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X		Network-layer vulnerability scanning is done regularly by third-party providers
		TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X		Application-layer vulnerability scans are conducted at least annually by third-party	
		TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X		Operating system-layer vulnerability scans are conducted at least annually by third-party	

		TVM-02.4	implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g.,	Will you make the results of vulnerability scans available to tenants at their request?	X			On request, under NDA
		TVM-02.5		Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			Software patches should be tested and evaluated before they are installed in an operational environment
		TVM-02.6		Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	X			Summary report on Client request
Threat and Vulnerability Management <i>Mobile Code</i>	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	SOLARI does not allow Clients to manage client applications
		TVM-03.2		Is all unauthorized mobile code prevented from executing?			X	

© Copyright 2014-2019 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire CAIQ Version 3.0.1" at <http://www.cloudsecurityalliance.org> subject to the following: (a) the Consensus Assessments Initiative Questionnaire v3.0.1 may be used solely for your personal, informational, non-commercial use; (b) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be modified or altered in any way; (c) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Consensus Assessments Initiative Questionnaire v3.0.1 as permitted by the Fair Use provisions of the United