Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?		X		
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?		X		
		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		X		
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information		X		The SaaS service offered consists in storing AES-256 encrypted documents and then making them available to owners
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?		X		
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic	Does your data management policies and procedures require audits to verify data input and output integrity routines?		X		
		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	X			Data will be checked the integrity for input and output using GUMP PHP library and other check libraries…

Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure,	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?		X		
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of	X			
		AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?	X			
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?		X		We conduct vulnerability assessment tests.
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices		X		We conduct vulnerability assessment tests with automatic tools
		AAC-02.4		Do you conduct internal audits at least annually?	X			
		AAC-02.5		Do you conduct independent audits at least annually?		X		
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?		X		We conduct vulnerability assessment tests with automated tools and the
		AAC-02.7		Are the results of internal and external audits available to tenants at their	X			

Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually	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			
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them	Does your organization have a plan or framework for business continuity management or disaster recovery	X			The entire infrastructure is subject to the businness continuity tools offered by the IaaS and PaaS ARUBA.
		BCR-01.2		Do you have more than one provider for each service you depend on?		X		The only services used by our solution are the PaaS and IaaS
		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			The only services used by our solution are the PaaS and IaaS services offered by ARUBA.
		BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?		X		
		BCR-01.6		Do you provide a tenant-triggered failover option?		X		
		BCR-01.7		Do you share your business continuity and redundancy plans with your tenants?		X		

Business Continuity Management & Operational Resilience *Business Continuity*	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	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			The entire infrastructure is subject to the businness continuity tools offered by the IaaS and PaaS ARUBA.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter			X	We rely on ARUBA's DataCenter, a certified provider of PaaS and IaaS services.
		BCR-03.2		Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?			X	We rely on ARUBA's DataCenter, a certified provider of PaaS and IaaS services.
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:	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			

Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear	Is physical damage anticipated and are countermeasures included in the design of physical protections?	X			We rely on ARUBA's DataCenter, a certified provider of PaaS and IaaS services. Physical protection against damage (e.g. natural causes, natural disasters, intentional attacks) is provided and designed by IaaS and PaaS Aruba which has the necessary certifications to provide the service.
Business Continuity Management & Operational Resilience	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		X		We host our service in Aruba's Datacenter. This's located near the city of Arezzo. The city of Arezzo is valued at “medium” risk of earthquake (2nd level) according to italian civil protection
Business Continuity Management & Operational Resilience	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?		X		We rely on ARUBA's DataCenter, a certified provider of PaaS and IaaS services.
		BCR-07.2		Do you have an equipment and datacenter maintenance routine or plan?		X		We rely on ARUBA's DataCenter, a certified provider of PaaS and IaaS services.
Business Continuity Management & Operational Resilience	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?		X		We rely on ARUBA's DataCenter, a certified provider of PaaS and IaaS services.

Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and	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		
		BCR-09.2		Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?		X		
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?		X		
Business Continuity Management & Operational Resilience	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of	Do you have technical capabilities to enforce tenant data retention policies?	X			
		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			

Resilience *Retention Policy*		BCR-11.3	to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			Our service is a SaaS the backUp and Restore features are provided by our IaaS / PaaS Aruba. We use Aruba Cloud Backup System (https://www.cloud.it/cloud-
		BCR-11.4		If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			Our service is a SaaS the backUp and Restore features are provided by our IaaS / PaaS Aruba. We use Aruba Cloud Backup System
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?			X	The service offered consists of archiving customer records in the cloud and returning them on request. The archived documents are encrypted in AES-256 format by customers and the infrastructure
		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 *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			
Change Control & Configurati	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?			X	

on Management		CCC-02.2	change management, release, and testing as internal developers within	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?			X	
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and	X			
		CCC-03.2		Is documentation describing known issues with certain products/services available?			X	
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and	X			
		CCC-03.4		Do you have controls in place to ensure that standards of quality are being met		X		
		CCC-03.5		Do you have controls in place to detect source code security defects for any			X	
		CCC-03.6		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software	X			
Change Control & Configuration Management *Unauthorized*	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	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			

Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	X			
		CCC-05.2		Do you have policies and procedures established for managing risks with respect to change management in		X		
		CCC-05.3		Do you have technical measures in place to ensure that changes in production environments are registered, authorized		X		
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?		X		
		DSI-01.2		Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g.,		X		

Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and	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			
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical		X		
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent	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	The service offered consists of archiving customer records in the cloud and returning them on request. The archived documents are encrypted in AES-256 format by customers and the infrastructure
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication	X			
Data Security & Information Lifecycle Management *Handling / Labeling / Security*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?			X	The service offered consists of archiving customer records in the cloud and returning them on request. The archived documents are encrypted in AES-256 format by customers and the infrastructure
		DSI-04.2		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type			X	

Security Policy		DSI-04.3	that act as aggregate containers for data.	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?			X	The service offered consists of archiving customer records in the cloud and returning them on request. The archived documents are encrypted in AES-256 format by customers and the infrastructure does not have the keys.
Data Security & Information Lifecycle Management *Ownership*	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			
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?		X		Management of physical assets is performed by IaaS and PaaS provider Aruba ISO27001 certified. We cannot perform secure deletion (e.g., cryptographic demagnetization/jamming) of stored data because we do not have access
		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	X			The archived documents are encrypted in AES-256 format by customers and the infrastructure does not have the keys.
Datacenter Security *Asset*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity		X		

Management		DCS-01.2	expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?		X		
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception	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 perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) is provided and designed by IaaS and PaaS Aruba which has the necessary
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate	Do you have a capability to use system geographic location as an authentication factor?			X	archiving encrypted documents that will eventually be downloaded by our clients' customers. We have no
		DCS-03.2		Is automated equipment identification used as a method to validate connection authentication integrity based on known		X		
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	PaaS/IaaS services of ARUBA ISO27001 certified provider. The systems are located in Europe and subject to European regulations. We don't use other systems than the
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	Can you provide tenants with your asset management policies and procedures?		X		