CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1		Comuni-Chiamo srl - March 2019				
Control Domain	Question ID	Consensus Assessment Questions	Consensus Assessment Answers			Notes
			Yes	No	Not Applicable	
Application & Interface Security Application Security	AIS-01.1	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?		x		
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	x			Standard python linters like pep8, pyflakes and similar are used to detect the most common programming errors and pitfalls at all stages of development
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	x			Unit testings and integration testings are in place to detect security defects prior to production
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		x		
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	x			We do human driven code reviews during development and before pushing any changes to production
Application & Interface Security Customer Access Requirements	AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	x			All data access and security requirements are thoroughly discussed with clients and expectations are explained
	AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	x			
Application & Interface Security Data Integrity	AIS-03.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or	x			This is tested in development phase with thorough unit testing, during the production phase with internal application/database integrity checks and at support time by manual inspection.
Application & Interface Security Data Security / Integrity	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	x			There is no explicit compliance on the application side as we are using a cloud service provider for all infrastructure but there is full compliance on the Saas/PaaS/IaaS side (AWS Cloud)
Audit Assurance & Compliance Audit Planning	AAC-01.1	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?			x	The software is provided as a service and there are no resources, hosts, domains or computing resources in control of the users.
Audit Assurance & Compliance Independent Audits	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	x			Our clients and stakeholders are informed about all the IaaS/SaaS our platform uses and are redirected upon request to the relevant certification reports for any provider.
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	x			There is AWS GuardDuty (https://aws.amazon.com/es/guardduty/) automatically running in background on the main internet-exposed endpoints providing alerts that are human-actioned as soon as an issue is detected

	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	x			Once a year an externally contracted security firm performs a full application vulnerability scan on the public/exposed endpoints and services. The report from this scan is then submitted and used to create actionable items that are solved during the iteration cycle.
	AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	x			There is an internal annual security evaluation, credentials rotation and all collaborators and employees are continuosly formed and instructed on best data and security practices
	AAC-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	x			
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	x			
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	x			
	AAC-02.8	Do you have an internal audit program that allows for cross-functional audit of assessments?	x			This is already on schedule for being implemented during 2019
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	x			All customer data is segmented by tenant ID and all data operations are keyed based on this ID.
	AAC-03.2	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	x			
	AAC-03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	x			Data is stored in the North European region of the AWS service, data can be moved to a different region upon request, depending on the local availability of compliant and compatbile storage solutions in the region of destination.
	AAC-03.4	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	x			
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01.1	Do you provide tenants with geographically resilient hosting options?	x			The DBMS on Amazon AWS use Multi-AZ option that in turn is geographically resilient in their own datacenters.
	BCR-01.2	Do you provide tenants with infrastructure service failover capability to other providers?		x		All data and services are inside the AWS cloud - Refer to AWS Overview of Cloud Security whitepaper for additional details - available at http://aws.amazon.com/security.
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Meetings are scheduled every months, plus straordinary meetings (with relevant stakeholders) are organized whenever significant changes occour
Business Continuity Management & Operational	BCR-03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?			x	All systems are located in the same AWS region and there are not movements between regions

Resilience Power / Telecommunications	BCR-03.2	Can tenants define how their data is transported and through which legal jurisdictions?			x	All systems are located in the same AWS region and there are not movements between regions
Business Continuity Management & Operational Resilience Documentation	BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?			x	The tenant receives usage documentation, but no installation, configuration or operations of any systems are performed on their part. The tenants are users of the system with no control on its installation, configuration or operations.
Business Continuity Management & Operational Resilience Environmental Risks	BCR-05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	x			we use a full third party cloud solution: Amazon AWS - AWS data centers incorporate physical protection against environmental risks
Business Continuity Management & Operational Resilience	BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?			x	we use a full third party cloud solution: Amazon AWS - AWS data centers incorporate physical protection against environmental risks
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?			x	we use a full third party cloud solution: Amazon AWS
	BCR-07.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?			x	we provide a full SaaS service, so the tenants do not need Virtual Machine
	BCR-07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	x			We have been working for the last two years to a have a 100% capability to port all infrastructure, data and procedures to a different cloud provider. The process is almost completed and is expected to be completed by EOY 2019.
	BCR-07.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?			x	we provide a full SaaS service, so the tenants do not need Virtual Machine
	BCR-07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	x			All backup data storage and recovery is performed by AWS
Business Continuity Management & Operational Resilience	BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	x			we use a full third party cloud solution: Amazon AWS - AWS equipment is protected from utility service outages in alignment with ISO 27001 standard.
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	x			The status.comuni-chiamo.com status page allows clients to monitor SLA performances
	BCR-09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?		x		

	BCR-09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	x			The status.comuni-chiamo.com status page allows clients to monitor SLA performances
Business Continuity Management & Operational Resilience Policy	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	x			
Business Continuity Management & Operational Resilience Retention Policy	BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?			x	Being a SaaS all data retention policies a tenant might have are dependant on the subscription being continued. Upon subscription termination all data is dumped and provided to the tenant.
	BCR-11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	x			There is no internal documentation at time of writing to comply for a government data request, but the required procedures and methodologies are already in place and data can be presented upon request.
	BCR-11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	x			All backup data storage and recovery is performed by AWS - https://aws.amazon.com/it/security/
	BCR-11.5	Do you test your backup or redundancy mechanisms at least annually?	x			
Change Control & Configuration Management New Development / Acquisition	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?			x	At the time there is no plan on acquiring any external services or providers and this has not happened in the past.
	CCC-01.2	Is documentation available that describes the installation, configuration, and use of products/services/features?	x			The documentation provided allows the client to configure their platform, and every new relevant update is communicated to them and the relevant documentation updated
Change Control & Configuration Management Outsourced Development	CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software	x			The CIO and internal development team performs quality and security checks
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	x			The CIO and internal development team performs quality and security checks. We do not generally outsource development of software
Change Control & Configuration Management Quality Testing	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?		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 service offerings?	x			The development lifecycle incorporates industry best practices which include design reviews about secuity, threat modeling and completion of a risk assessment.

	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	x			
Change Control & Configuration Management Unauthorized Software Installations	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?			x	Users have no access to the relevant hosts, there is no internal access to the hosts themselves except via a monitored bastion host with ip and credentials login restrictions
Change Control & Configuration Management Production Changes	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	x			
Data Security & Information Lifecycle Management Classification	DSI-01.1	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?			x	There are no virtual machines that are user-accessible, all data can be accessed only by a region-locked bastion host.
	DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			x	There is no owned hardware, all systems are on the AWS cloud
	DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?	x			The software is provided as a service, so logins must be made possible from any geographical location. Strict user IP provenance is monitored and if a user logs in from an unknown of unseen IP a notification is sent to the user.
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	x			All data is stored in the Republic of Ireland. The system is GDPR compliant
	DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	x			All data is stored in the Republic of Ireland. The system is GDPR compliant
	DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		x		
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?			x	
Data Security & Information Lifecycle Management	DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	x			The system has been designed to be GDPR compliant

Data Inventory / Flows	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	x			Our application doesn't allow migration. AWS ensure that data do not migrate: https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf
Data Security & Information Lifecycle Management E-commerce Transactions	DSI-03.1	Do you provide open encryption methodologies (3.4 ES, 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			All data in transit is encrypted with TLSv1.2 from the client to the infrastructure border. The following is the border ssl termination supported list of protocols in OpenSSL format: 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK';
	DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	x			
Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	x			
	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	x			
Data Security & Information Lifecycle Management Nonproduction Data	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	x			Production and others environment are in isolated. The credential are different for each environment, so we don't need any internal procedure. Different DB Schema are present in each environment, so even if an application bug tried to propagate the data it would fail during inception due to schema incompatibilities.
Data Security & Information Lifecycle Management	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	x			We are GDPR compliant and we have privacy policy and terms of service that specify required information
Data Security & Information Lifecycle Management Secure Disposal	DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?			x	Internal AWS procedure already do this when data deletion occurs.
	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			The procedure exists internally but it's not yet documented to be publicly released. It will be by Q2 2019.
Datacenter Security Asset Management	DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?			x	We provie a Software as a service, AWS has documented practices for this.

	DCS-01.2	Do you maintain a complete inventory of all of your critical supplier relationships?			x
Datacenter Security Controlled Access Points	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?			x
Datacenter Security Equipment Identification	DCS-03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?			x
Datacenter Security Offsite Authorization	DCS-04.1	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, replication)?			x
Datacenter Security Offsite Equipment	DCS-05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?			x
Datacenter Security Policy	DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?			x
	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
Datacenter Security Secure Area Authorization	DCS-07.1	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?			x

Datacenter Security Unauthorized Persons Entry	DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?			x	
Datacenter Security User Access	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?			x	
Encryption & Key Management Entitlement	EKM-01.1	Do you have key management policies binding keys to identifiable owners?			x	
Encryption & Key Management Key Generation	EKM-02.1	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	Tenants do not have access to encryption keys and do not require it for operating the SaaS
	EKM-02.3	Do you maintain key management procedures?	x			All key management is handled by AWS IAM
	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			Internal company users and external contractors are required to use either LastPass or password-store.
Encryption & Key Management Encryption	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?			x	All tenant data is located in either AWS RDS or AWS S3
	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?			x	Virtual machine images are never transported, instance migration is internally handled by the AWS platform
	EKM-03.3	Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?			x	
	EKM-03.4	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	x			https://docs.aws.amazon.com/iam/index.html#lang/it_it
Encryption & Key Management Storage and Access	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	x			https://docs.aws.amazon.com/iam/index.html#lang/it_it
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	x			All keys are on AWS: https://docs.aws.amazon.com/iam/index.html#lang/it_it
	EKM-04.3	Do you store encryption keys in the cloud?	x			All keys are on AWS: https://docs.aws.amazon.com/iam/index.html#lang/it_it
	EKM-04.4	Do you have separate key management and key usage duties?	x			All keys are on AWS: https://docs.aws.amazon.com/iam/index.html#lang/it_it
Governance and Risk Management Baseline Requirements	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?			x	All this is delegated to AWS

	GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?			x	All this is delegated to AWS
	GRM-01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?			x	Users do not have acces, need or require virtual machines of any sort.
Governance and Risk Management Risk Assessments	GRM-02.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?			x	
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	x			
Governance and Risk Management Management Oversight	GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	x			
Governance and Risk Management Management Program	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	x			The document will be made public by EOY 2019
	GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	x			
Governance and Risk Management Management Support / Involvement	GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	x			
Governance and Risk Management Policy	GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?		x		
	GRM-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	x			
	GRM-06.3	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?		x		
	GRM-06.4	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	x			
Governance and Risk Management Policy Enforcement	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	x			
	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-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	x			
Governance and Risk Management Policy Reviews	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	x			
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	x			We are assisted by a legal team to ensure that privacy and security policies are updated
Governance and Risk Management Assessments	GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?		x		
	GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?		x		
Governance and Risk Management Program	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?		x		
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	x			The document will be made public by EOY 2019
Human Resources Asset Returns	HRS-01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	x			There is AWS GuardDuty (https://aws.amazon.com/es/guardduty/) automatically running in background on the main internet-exposed endpoints providing alerts that are human-actioned as soon as an issue is detected
	HRS-01.2	Is your Privacy Policy aligned with industry standards?	x			We are assisted by a legal team to ensure that privacy adn security policies are updated
Human Resources Background Screening	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?		x		
Human Resources Employment Agreements	HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	x			
	HRS-03.2	Do you document employee acknowledgment of training they have completed?		x		
	HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	x			

	HRS-03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?		x		
	HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	x			
Human Resources Employment Termination	HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?		x		The company is way too small for this
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	x			All passwords are expired and users deleted across all systems
Human Resources Portable / Mobile Devices	HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?			x	The access is managed via the same software as a service as above
Human Resources Non-Disclosure Agreements	HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	x			
Human Resources Roles / Responsibilities	HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	x			It is already under development, will be provided before EOY 2019
Human Resources Acceptable Use	HRS-08.1	Do you provide documentation regarding how you may access tenant data and metadata?	x			The process is the same as GDPR compliance
	HRS-08.2	Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)?	x			
	HRS-08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		x		

Human Resources Training / Awareness	HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	x			
	HRS-09.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	x			
Human Resources User Responsibility	HRS-10.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	x			All tenants receive a basic security policy briefing, a document will be published by EOY 2019.
	HRS-10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	x			All tenants receive a basic security policy briefing, a document will be published by EOY 2019.
	HRS-10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	x			All tenants receive a basic security policy briefing, a document will be published by EOY 2019.
Human Resources Workspace	HRS-11.1	Do your data management policies and procedures address tenant and service level conflicts of interests?		x		
	HRS-11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	x			There is a "changelog" of changes and operations on tenant data.
	HRS-11.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?			x	We rely on AWS for this
Identity & Access Management Audit Tools Access	IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	x			All logins are routed via a bastion host where standard logging systems are in place.
	IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	x			SSH access logs will be persisted before Q1 2019. Application logins and logouts are already logged. Database audit logging will be in place by Q1 2019.
Identity & Access Management User Access Policy	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	x			
	IAM-02.2	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		x		Working with less than 5 people there is not enough turnover for this to be a recurring issue.
Identity & Access Management Diagnostic / Configuration Ports Access	IAM-03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	x			All hosts live in a internet-unrachable AWS EC2 VPC and all connections to these hosts are made via a bastion host.

Identity & Access Management Policies and Procedures	IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	x			
	IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	x			
Identity & Access Management Segregation of Duties	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?			x	Tenants only use the webapp, there can be no missing segregation due to separate user accounts.
Identity & Access Management Source Code Access Restriction	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	x			All code repositories are internal and can only be accessed via a pre-configured SSH key from each deployiment host. All code is code reviewed before reaching the master deploy branch.
	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	Being SaaS there is no tenant code or applications
Identity & Access Management Third Party Access	IAM-07.1	Do you provide multi-failure disaster recovery capability?	x			
	IAM-07.2	Do you monitor service continuity with upstream providers in the event of provider failure?	x			AWS provides status pages that are queried when publishing the site status report
	IAM-07.3	Do you have more than one provider for each service you depend on?		x		All code and systems run on Amazon AWS
	IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	x			This will be included in the status page.
	IAM-07.5	Do you provide the tenant the ability to declare a disaster?	x			
	IAM-07.6	Do you provide a tenant-triggered failover option?			x	There is no failover option for the tenant as they only see the main web application
	IAM-07.7	Do you share your business continuity and redundancy plans with your tenants?	x			All service impacting migrations and redundancy considerations are communicated to the tenants
Identity & Access Management User Access Restriction / Authorization	IAM-08.1	Do you document how you grant and approve access to tenant data?		x		

	IAM-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?			x	
Identity & Access Management User Access Authorization	IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	x			
	IAM-09.2	Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	x			
Identity & Access Management User Access Reviews	IAM-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	x			from 2019 will do annualy
	IAM-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	x			
	IAM-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	x			
Identity & Access Management User Access Revocation	IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	x			
	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-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?		x		
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?			x	Authentication is allowre only via the webapp, all interaction happens there.
	IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?			x	
	IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?			x	

	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	
	IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?		x		Feature planned for EOY 2019
	IAM-12.7	Do you allow tenants to use third-party identity assurance services?		x		
	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			
	IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?		x		
	IAM-12.10	Do you support the ability to force password changes upon first logon?		x		Feature planned for EOY 2019
	IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	x			
Identity & Access Management Utility Programs Access	IAM-13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	x			We rely on the AWS interface for these operations.
	IAM-13.2	Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?			x	All virtualization is controlled by the cloud provider.
	IAM-13.3	Are attacks that target the virtual infrastructure prevented with technical controls?			x	All virtualization is controlled by the cloud provider.
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	x			
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	x			
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?		x		
	IVS-01.4	Are audit logs centrally stored and retained?	x			
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	x			
Infrastructure & Virtualization Security Change Detection	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?		x		All virtualization is controlled by the cloud provider.
	IVS-02.2	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?		x		

Infrastructure & Virtualization Security Clock Synchronization	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	x			
Infrastructure & Virtualization Security Capacity / Resource Planning	IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?			x	All virtualization is controlled by the cloud provider.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			x	
	IVS-04.3	Do your system capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	x			
	IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	x			
Infrastructure & Virtualization Security Management - Vulnerability Management	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	x			
Infrastructure & Virtualization Security Network Security	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			x	We do not provide an IaaS offering
	IVS-06.2	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 OS Hardening and Base Controls	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	x			
Infrastructure & Virtualization Security	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?		x		The tenant can participate in a demo of the new platform that is developed in staging before launch

Production / Non-Production Environments	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			x	We do not provide an IaaS offering
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	x			
Infrastructure & Virtualization Security Segmentation	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	x			
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, and contractual requirements?			x	There is no legislative, regulatory or contractual requirement to do so
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	x			
	IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	x			
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	x			
	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-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	x			We rely on AWS IAM for this access
Infrastructure & Virtualization Security Wireless Security	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			x	
	IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			x	
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			x	
Infrastructure & Virtualization Security	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?			x	

Network Architecture	IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?			x	Inside an AWS VPC
Interoperability & Portability APIs	IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	x			
Interoperability & Portability Data Request	IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	x			These data can be requested on the platform, and custom requests can be done to our Support team
Interoperability & Portability Policy & Legal	IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?			x	There is no third party application possible
	IPY-03.2	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?			x	
Interoperability & Portability Standardized Network Protocols	IPY-04.1	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	x			
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?		x		
Interoperability & Portability Virtualization	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?			x	
	IPY-05.2	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			x	

Mobile Security Anti-Malware	MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
Mobile Security Application Stores	MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			x	
Mobile Security Approved Applications	MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			x	
Mobile Security Approved Software for BYOD	MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			x	Personal devices are not allowed to access or store relevant company data. The company provides the devides required for the job
Mobile Security Awareness and Training	MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	x			Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
Mobile Security Cloud Based Services	MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?		x		Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform

Mobile Security Compatibility	MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?		x		
Mobile Security Device Eligibility	MOS-08.1	Do you have a BYOD policy that defines the device (s) and eligibility requirements allowed for BYOD usage?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
Mobile Security Device Inventory	MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
Mobile Security Device Management	MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
Mobile Security Encryption	MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
Mobile Security Jailbreaking and Rooting	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
	MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			x	
Mobile Security Legal	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
	MOS-13.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform

Mobile Security Lockout Screen	MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			x	
Mobile Security Operating Systems	MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			x	
Mobile Security Passwords	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	x			
	MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?			x	
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			x	
Mobile Security Policy	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
	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-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			x	
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
Mobile Security Security Patches	MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			x	
	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-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			x	Mobile devices are not allowed to access or store relevant company data. Customer are responsible to manage mobile security devices and the access to the customer's content on our platform

Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	x			Each tenant has an in-house contact point for regulation and changes
Security Incident Management, E-Discovery, & Cloud Forensics Incident Management	SEF-02.1	Do you have a documented security incident response plan?		x		
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?		x		
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		x		
	SEF-02.4	Have you tested your security incident response plans in the last year?		x		
Security Incident Management, E-Discovery, & Cloud Forensics Incident Reporting	SEF-03.1	Does your security information and event management (SIEM) system merge data sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?		x		
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?			x	
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Legal Preparation	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?		x		
	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			A snapshot of the production data can be obtained and analyzed from there without distrupting the operations of other tenants
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	x			
Security Incident Management, E-Discovery, & Cloud Forensics	SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?		x		
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?		x		
Supply Chain Management, Transparency, and Accountability Data Quality and Integrity	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	x			
	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	x			

Supply Chain Management, Transparency, and Accountability Incident Reporting	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	x			Starting Q1 2019 a newsletter to all tenants will be sent upon any security or operational incident
Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	x			
	STA-03.2	Do you provide tenants with capacity planning and use reports?			x	
Supply Chain Management, Transparency, and Accountability Provider Internal Assessments	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	x			
Supply Chain Management, Transparency, and Accountability Third Party Agreements	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?			x	AWS and related services are all GDPR and local regulations compliant.
	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?			x	AWS and related services are all GDPR and local regulations compliant.
	STA-05.3	Does legal counsel review all third-party agreements?	x			All relevant third-party agreement are reviewed by our legal team
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	x			
	STA-05.5	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		x		
Supply Chain Management, Transparency, and Accountability Supply Chain Governance Reviews	STA-06.1	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?		x		
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	x			
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?		x		

	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?			x	
	STA-07.4	Do you review all agreements, policies, and processes at least annually?	x			
Supply Chain Management, Transparency, and Accountability Third Party Assessment	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	x			
	STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	x			
Supply Chain Management, Transparency, and Accountability Third Party Audits	STA-09.1	Do you permit tenants to perform independent vulnerability assessments?			x	
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	x			
Threat and Vulnerability Management Antivirus / Malicious Software	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?		x		
	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted time frames?		x		
Threat and Vulnerability Management Vulnerability / Patch Management	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?		x		
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?		x		
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?		x		
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?		x		

	TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	x			
	TVM-02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	x			
Threat and Vulnerability Management Mobile Code	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			x	
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	x			
