Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
					Yes	No	Not Applicable	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (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)?	Yes			The development team follows the OWASP secure coding guidelines.
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?		No		
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	Yes			The development team follows the OWASP secure coding guidelines.
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Yes			Opencontent CMS-based services uses the open source software EzPublish that has a structured process to manage security issues. For more info see also *http://share.ez.
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes			The development team follows the OWASP secure coding guidelines.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	Yes			Prior to granting customers access to their production instance of our Saas, a Master Services Agreement set forth the terms and conditions of Saas's delivery and customer receipt of any services. Customer data submitted to our SaaS ("Customer Data") is managed by the customer in their use of the SaaS. As such, customers retain responsibility to ensure their use of our services is in compliance with applicable laws and regulations.
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	Yes			Customers manage their organization's own access privileges within their SaaS instance. The organization administrators are appointed by the customer and are responsible for managing users, assets and permission.
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	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 corruption of data?	Yes			Data integrity controls are in place to prevent manual or systematic processing errors, corruption of data or misuse. Backups are available if and when required for restoring data in the event of data corruption.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e. g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	Yes			Our Data Security Architecture is designed to incorporate the industry best practices such as: "Amazon AWS security best practices". Our architecture is designed to balance the need for flexibility and agility with the need for robust controls ensuring the confidentiality, integrity, and availability of our customers' data.
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you 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.)?	Yes			Opencontent has established an annual calendar for Security and IT internal audit and compliance activities. Opencontent assesses itself against this CSA format.
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?		No		
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Yes			Network layer security is in charge of our IaaS provider AWS.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes			Opencontent has established an annual calendar for Security and IT internal audit and compliance activities. Opencontent assesses itself against this CSA format.
		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	Yes			Opencontent has established an annual calendar for Security and IT internal audit and compliance activities. Opencontent assesses itself against this CSA format.
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?		No		
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	Yes			
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	Yes			
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?	Yes			
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have 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?	Yes			Opencontent implements this ability using two different approaches: 1) a single-database per tenant approach, with dedicated access credentials; 2) data isolated at application layer and stored in a single shared database for all tenants.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		AAC-03.2		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Yes			
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	Yes			All Opencontent Production Data Centers are held within the European data centers of AWS.
		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?	Yes			
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval	Do you provide tenants with geographically resilient hosting options?	Yes			Our SaaS infrastructure leverages for resiliency on two availability zones within the AWS Europe (Ireland) region. AMAZON AWS Availability Zones are on several independent data centers distributed in a geographical region. We currently don't support multi-regional SaaS services, anyway we are able to rebuild our infrastructure from scratch in a new region in a short time thanks to the use of Infrastructure as Code approach (Cloudformation, Cloud-init, Ansible, Dockerized deploy, Git configuration).

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		BCR-01.2	approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Do you provide tenants with infrastructure service failover capability to other providers?			n/a	Opencontent is not a IaaS or PaaS, Opencontent service offering is a multi-tenant SaaS.
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes			
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Do you provide tenants with documentation showing the transport route of their data between your systems?	Yes			
		BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?		No		Opencontent SaaS services are located only in European data centers of AWS.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Yes			Opencontent maintains information system and configuration documentation and make it available to authorized personnel.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	Yes			Our IaaS/PaaS provider (Amazon Web Services) implements a wide variety of countermeasures and controls to mitigate these risks. More information can be found at https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		No		Our IaaS/PaaS provider (Amazon Web Services) implements a wide variety of countermeasures and controls to mitigate these risks. More information can be found at https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?			x	Not Applicable (our service is a Saas).
		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	
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?			x	
		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	
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?			x	
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Yes			Our IaaS/PaaS provider (Amazon Web Services) implements a wide variety of countermeasures and controls to mitigate these risks. More information can be found at https://d0. awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Yes			A public status page is available for SaaS services at https://status.opencontent.io The status page summarize current status of services and historical values. The page show also the Apdex (Application Performance Index), an open standard for measuring performance of software applications in computing. Its purpose is to convert measurements into insights about user satisfaction, by specifying a uniform way to analyze and report on the degree to which measured performance meets user expectations.
		BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Yes			
		BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes			
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical control capabilities to enforce tenant data	Yes			
		BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third	Yes			
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes			
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	Yes			
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Yes			The description and provisioning of all resources services and infrastructure are created & maintained thanks to AWS CloudFormation in an automated and secure manner https://aws.amazon.com/cloudformation where all changes are.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		CCC-01.2	and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Is documentation available that describes the installation, configuration, and use of products/services/features?	Yes			
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?			*	We do not outsource software development.
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?			*	
Change Control & Configuration Management *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 provide your tenants with documentation that describes your quality assurance process?		No		This is deemed Opencontent internal confidential data, and not shared with customers.
		CCC-03.2		Is documentation describing known issues with certain products/services available?	Yes			Known issues are publicly visible to customers and to non customers on github public repositories.
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	Yes			Opencontent adopted an integrated approach to debug production systems: dedicated tools are available to debug the production environment without affecting the overall service performance and without any interference with the normal use of the final users.
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes			Our SaaS Infrastructure is completely managed as code and deployed using AWS Cloudformation and is immutable once in production. All access, changes are logged and monitored continuously for unauthorized changes. Alerts are generated based on events and sent to our incident management system. We also on an ongoing basis review systems usage, resources utilization, administrator activities, suspicious events, vulnerabilities, etc.
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	Yes			Policies & Procedures are clearly defined on the contract with the customer.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
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 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)?	Yes			Opencontent approach to configuration management allows to tag every single resource provisioned for each environment. Tags are associated to resources according to service name, environment type (e.g. development, production, qa), resource role (web server, proxy, database).
		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	This is delegated to our Iaas provider (Amazon AWS, qualified Agid).
		DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?		No		
		DSI-01.4		Can you provide the physical location/geography of storage of a tenant’s data upon request?	Yes			
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?	Yes			The physical location is AWS Europe Region 1 (Ireland).

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		DSI-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Yes			We used a highly structured data system for both data and objects containing data, with a data classification policy in place. Data is classified into four general categories: Standard (Public), Restricted, Expired and Hidden data. We also use other more specific classifications based on knowledge domains. To a general overview of the approach of our CMS to data classification check also: https://doc.ez.no/eZ-Publish/Technical-manual/4.x/Concepts-and-basics/Access-control
		DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		No		
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	Yes			Internally, we tracks data flows and network connectivity among its SaaS infrastructure.
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	Yes			All customer instances of our Saas and their associated data storage are assigned to one of our production environments when provisioned based on the data location requirement. As AWS Customers we designate in which physical region their content will be located. AWS will not move our content from the selected regions without notifying us, unless required to comply with the law or

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide open encryption methodologies (3.4ES, 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)?	Yes			
		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)?	Yes			We integrate with some external services. All communication with external services happen over https. Apart from integration with third party services, all other intra service communication happens inside a dedicated VPC.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	Yes			
		DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Yes			The OpenSource CMS that Opencontent adopted to develop the OpenPA Suite of products supports this feature natively. For

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes			
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?		No		
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 secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?		No		Our IaaS provider (Amazon AWS) has a process for secure deletion and secure disposal of end of life equipment for our SaaS. AWS Security is detailed at https://aws.amazon.com/security/ But all these procedures are not determined or under control of the tenant.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		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?	Yes			When approved for deletion, the procedure outlined in DSI-07.1 is followed to delete customer data.
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	Yes			
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	Yes			
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?	Yes			Our IaaS provider (Amazon AWS) implements a wide variety physical and environmental controls. More information can be found in the "Aws security processes whitepaper" at https://aws.amazon.com/whitepapers/overview-of-security-processes

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	yes			Our IaaS provider (Amazon Web Services) manages equipment identification in alignment with ISO 27001 standard, see https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	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)?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
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 until it can be destroyed.	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	yes			Our provider, AWS, takes good care of this: in alignment with ISO 27001 standards, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. see https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	yes			Our provider, AWS, is ISO 27001 certified, and covers this issue: see https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	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)?	yes			
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	yes			
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?	Yes			No physical access is allowed from our side, our IaaS provider, AWS Amazon, is qualified Agid and cover this issue.
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	Yes			Currently, we manage all encryption for our customers. Thanks to the Key Management Service from our IaaS/PaaS provider (Amazon AWS) we are able, upon request, to offer Encryption & Key Management to tenants thanks to the Key Management Service designed by our IaaS/PaaS provider (Amazon AWS). Specific encryption of data at rest is implemented for sensible data.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per		No		
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	Yes			
		EKM-02.3		Do you maintain key management procedures?	Yes			
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	Yes			
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	Yes			
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes			
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Yes			
		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)?		No		
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	Yes			
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?		No		
		EKM-04.3		Do you store encryption keys in the cloud?	Yes			
		EKM-04.4		Do you have separate key management and key usage duties?	Yes			
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	yes			Our SaaS Infrastructure is completely managed as code and deployed using AWS Cloudformation: each server is created by CloudFormation starting from a base server that has been deeply checked.
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?		No		
		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	Not applicable (our service is a Software as a Service based on an infrastructure provided by our IaaS provider: Amazon AWS).

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	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)?		No		
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	Yes			
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	Yes			We provides periodic security awareness training for all employees.
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		No		

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		GRM-04.2	loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Do you review your Information Security Management Program (ISMP) at least once a year?		No		Thanks to the service of a specialized security we conduct vulnerability scans and penetration testing of our SaaS (applications and infrastructure); we will provide to our customer upon request an attestation of the penetration test conducted by the third party security firm. We allows penetration testing initiated by the customer at customer's expense. Customer testing may only be run against a test instance of the our SaaS that is a copy of production so that the test does not impact other customers. We must be provided advanced notice before such testing. Customers initiate this process by contacting our support.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?	Yes			Amazon AWS is the provider we have chosen, and is only provider for our Saas service: all AWS services, too, are chosen based on our needs and policy regarding privacy and security.
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	yes			
		GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Yes			Amazon AWS is the provider we have chosen, and is only provider for our Saas service: all AWS services, too, are chosen based on our needs and policy regarding privacy and security.
		GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	Yes			We can provide upon request an overview of our controls, standards, certifications and regulations we comply with.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		GRM-06.4		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	Yes			
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes			
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes			
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	Yes			
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Yes			
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Yes			We focus on qualitative methods; our goal is to face risk assessments in a way it would be easily understandable by all people involved in risk mitigation: we consider this approach a good help to lower the risk of missing the identification of a risk. With regards to risks concerning the IaaS we rely on, AWS, we know that, in alignment with ISO 27001, AWS has developed a Risk Management program to mitigate and manage risk; AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
		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)?	Yes			
Governance and Risk Management *Program*	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and	Do you have a documented, organization-wide program in place to manage risk?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Program		GRM-11.2	with reasonable resolution time frames and stakeholder approval.	Do you make available documentation of your organization-wide risk management program?	Yes			Opencontent does not make its enterprise risk management program documentation available publicly: it can be available upon request or contract obligation.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Yes			Opencontent has processes in place to ensure that all equipment is returned and accounts terminated, In addition, our DevOps and Security team have systems and processes in place to monitor for data breaches and notify tenants in the event that such a breach may have impacted their data. Our incident response plan includes specific procedures to notify affected customers of confirmed data breaches. If a privacy breach is identify in our incident management process. We will notify our customer without undue delay.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		HRS-01.2		Is your Privacy Policy aligned with industry standards?	Yes			
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?	Yes			
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	Yes			
		HRS-03.2		Do you document employee acknowledgment of training they have completed?	Yes			
		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	Yes			
		HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	Yes			
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	Yes			
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	Yes			
Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization’s facilities)?	Yes			
Human Resources *Non-Disclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	Yes			
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	Yes			
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally owned or managed user	Do you provide documentation regarding how you may access tenant data and metadata?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		HRS-08.2	of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)?	Yes			
		HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	Yes			
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	Yes			
		HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	Yes			
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		HRS-10.2	• Maintaining a safe and secure working environment	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	Yes			
		HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	Yes			
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Do your data management policies and procedures address tenant and service level conflicts of interests?	Yes			Opencontent's policies and procedures have been created in support of customer service level requirements.
		HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	Yes			Opencontent's policies include provisioning access according to least privilege and monitoring production systems access for an unauthorized access to systems and/or 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?	Yes			Opencontent resources and containers are built via version controlled software repositories and are 'read only' preventing tampering.
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	Yes			Access to logs and monitoring are restricted using AWS IAM to authorized personnel only. Access to buckets in AWS S3 containing logs are monitored by internal auditing functionalities of the service.
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	Yes			
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Yes			Opencontent HR defines internal management responsibilities to be followed for termination and role change of employees to ensure system access is removed when no longer required for business purposes.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers	Notes
		IAM-02.2	and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)	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?	No	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Yes			Management access to our SaaS infrastructure is restricted to authorised individuals and connections through the use of VPN from notebook network to our infrastructure on Amazon AWS.
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Yes			Opencontent uses AWS IAM to manage user identities and access policies for our SaaS infrastructure. Specific roles and access level is also tracked in the System Administrators document required by the EU General Data Protection Regulation (GDPR).
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	Yes			
Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Yes			Opencontent enforces segregation of duties through user defined groups and access policies to minimize the risk of unintentional or unauthorized access or change to production systems. System access is restricted based on the user's job responsibilities.
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per	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?	Yes			Access to our application, program or object source code is restricted to our technical teams. At Opencontent we use a robust peer review system to ensure changes to source code are always reviewed.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		IAM-06.2	established user access policies and procedures.	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	Not applicable, we offer a Software as a Service.
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you provide multi-failure disaster recovery capability?	Yes			
		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	Yes			We monitor our IaaS provider to ensure service continuity.
		IAM-07.3		Do you have more than one provider for each service you depend on?		No		Our critical dependency is limited to our IaaS provider (Amazon AWS). We follow AWS best practices to ensure the availability our our SaaS infrastructure. We also have the capability to recover in another AWS regions in the event of a major outage. We also assessed the Amazon AWS own resilience and fault tolerance practices to ensure they meet our overall service delivery and continuity requirements.
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	Yes			Details of our operational continuity performance is available to customer with specific SLA objectives. A general overview is available at our public status page: http://status.opencontent.io
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?		No		

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		IAM-07.6		Do you provide a tenant-triggered failover option?		No		
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?	Yes			
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?	Yes			
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	Yes			
Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	Yes			We use a "need-to- know" and "least-privilege" approach to access provisioning.
		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?	Yes			We use a "need-to- know" and "least-privilege" approach to access provisioning.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Yes			Opencontent performs periodic reviews of access permissions, the reviews include administrative accounts to development systems and tools and all our SaaS infrastructures including the production.
		IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Yes			We track the activity of inspection and remediation applied.
		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?	Yes			
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	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?	Yes			
		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?	Yes			
Identity & Access Management *User ID*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?		No		

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Credentials		IAM-12.2	accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you use open standards to delegate authentication capabilities to your tenants?	Yes			Upon request.
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?		No		
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		No		
		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?		No		
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?		No		
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?	Yes			Upon request.
		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?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	Yes			Upon request.
		IAM-12.10		Do you support the ability to force password changes upon first logon?	Yes			
		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)?	Yes			
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	Yes			
		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.)?	Yes			Our provider (Amazon AWS, certified Agid IaaS) implements controls to mitigate these risks. For more information: http://aws.amazon.com/security.
		IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	Yes			Every resource is created with AWS CloudFormation with instructions that are stored in a repository, and has a unique ID we cannot change. Our IaaS provider (Amazon AWS) log any changes in any resources. The application code, too, is stored in a dedicated repository making it easy to spot any changes.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	Yes			There is no physical access to audit logs: our IaaS provider (AWS) store audit logs: only authorized personnel can access to it, and nobody can modify its content.
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	Yes			We evaluates pertinent regulations, standards and best practices for our operations on a regular basis. Our architecture, processes and controls follow a continuous improvement model.
		IVS-01.4		Are audit logs centrally stored and retained?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Yes			Our IaaS provider AWS has a built in very fast and easy console to review logs: these logs are the first source of information when we need details on what is going on. We also take advantage of AWS GuardDuty: an automated tool by AmazonAWS that has an intelligent option for continuous threat detection: the service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats, see https://aws.amazon.com/guardduty/
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?			x	In our SaaS infrastructure, individual containers don't have an image,when the container is initiated, an image is picked from a standard repository. We maintain ongoing auditing for each of the images and provide for re-application of the images by our configuration tools when necessary. As a result,changes are not made to the virtual machine images.
		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	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?			x	Not applicable (our service is a SaaS).
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			x	Not applicable (our service is a SaaS).
		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?	Yes			We monitor our SaaS infrastructure on a non going basis and alerts are setup when metrics exceed predefined thresholds. Extra capacity can be provisioned in a matter of minutes.
		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?	Yes			
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?			x	Not applicable (our service is a SaaS). The virtualization technologies are transparent to the Vulnerability tools that we utilize.
Infrastructure & Virtualization Security *Network*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			x	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Security		IVS-06.2	supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	yes			
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	yes			
		IVS-06.4		Are all firewall access control lists documented with business justification?	yes			
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	yes			
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	yes			Typically, only the production environment is provided to our customers. However, a test environment can be made available to customers when required, and in a separate environment.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		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?	yes			
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	yes			Our SaaS infrastructure has a variety of controls to ensure the protection and isolation of the environments, servers, containers, subnets. The logical firewall, the Load Balancers, the network ACL, application routers all work together. This ensure that only authorized traffic from the internet, from our datacenter and between servers are allowed.
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, and contractual requirements?	yes			
		IVS-09.3		Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	yes			
		IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	yes			
Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?			x	Not applicable (our service is a SaaS). No physical-to-virtual migrations are undertaken.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?			x	Not applicable (our service is a SaaS). No physical-to-virtual migrations are undertaken.
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	yes			We enforce the concept of least privilege, allowing only the necessary access for authorized users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires an elevation of privileges. All accounts require two-factor authentication, management access is done over TLS or SSH and all access are logged in an audit trail.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			x	Our offices wireless network is protected by WPA, but access to this network does not gain, at all, any kind of privileges on the connection to our SaaS servers and services or to any companies server/resource, as to say: access to our wireless office network set a user in the same condition as if he was just connected to the internet from anywhere else. This is our policy.
		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	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		IVS-12.3	• The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			x	
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e. g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	Yes			
		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?	yes			Our SaaS setup are able to use firewall rules, ip whitelisting, ip geolocation, network ACLs, Web Application Firewalls, load balancers to prevent spoofed traffic and restrict incoming and outgoing traffic to our SaaS infrastructure. The SaaS network is segregated to separate customer traffic from management traffic. Additionally, we can established automated controls to monitor and detect certain types of attacks. DDoS capabilities are provided by our IaaS Provider (Amazon AWS, qualified Agid).

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Interoperability & Portability *APIs*	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Yes			
Interoperability & Portability *Data Request*	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or . pdf)?	Yes			Formats are: ODF, JSON, XML, CSV.
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Yes			Refer to the documentation of our Restful API.
		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?	Yes			Customer will be able to retrieve their data using the Restful API.
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	Yes			All communication are encrypted in transit using Transport Layer Security (TLS).

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Yes			
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, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?			x	Not applicable, our service is a Saas: the control is delegated to our Agid qualified IaaS provider Amazon AWS.
		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	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			x	This one, and all Mobile Security (MOS) Controls are not applicable: for security reasons, our policies and procedures avoid the use of mobiles for uses different then voice communications
Mobile Security *Application Stores*	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			x	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Mobile Security *Approved Applications*	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			x	
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			x	
Mobile Security *Awareness and Training*	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			x	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Mobile Security *Cloud Based Services*	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			X	
Mobile Security *Compatibility*	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			x	
Mobile Security *Device Eligibility*	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			x	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Mobile Security *Device Inventory*	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory.	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			x	
Mobile Security *Device Management*	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			x	
Mobile Security *Encryption*	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			x	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			x	
		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			x	
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			x	
		MOS-13.2		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 *Lockout Screen*	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			x	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Mobile Security *Operating Systems*	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			x	
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			x	
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?			x	
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			x	
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			x	
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			x	
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			x	
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			x	
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			x	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			x	
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			x	
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			x	
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			x	
Security Incident Management, E-Discovery, & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	Yes			We have developed a robust processes to facilitate a coordinated response to incidents if one was to occur. The process follows the following phases: *Identification of declaration of a potential incident * Assign an incident severity * Investigation and diagnosis * Containment * Eradication * Recovery * Collection of evidence (as required) Communication Lessons Learned
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?	Yes			Yes, upon request
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	Yes			
		SEF-02.4		Have you tested your security incident response plans in the last year?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	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?	Yes			
		SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	Yes			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Yes			In the event of a security incident, proper forensic procedures will be performed for collection, retention, and presentation of evidence.
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Yes			
		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?	Yes			We can provide data from a single customer from a single point in time, on request.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes			We can provide single customer data snapshot/backup to support any litigation or law enforcement requests.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	Yes			
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	Yes			
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Yes			
		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?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	Yes			
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and	Do you collect capacity and use data for all relevant components of your cloud service offering?	Yes			
		STA-03.2		Do you provide tenants with capacity planning and use reports?	Yes			
Supply Chain Management, Transparency, and Accountability *Provider*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	Yes			
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	Yes			Third party security and privacy requirements are established through vendor due-diligence reviews; our IaaS and PaaS providers are Agid qualified.
		STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		STA-05.3	and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider	Does legal counsel review all third-party agreements?	Yes			
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	Yes			
		STA-05.5		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	Yes			
Supply Chain Management, Transparency, and Accountability *Supply Chain Governance*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	Yes			
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	Yes			
		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)?	Yes			
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		STA-07.4		Do you review all agreements, policies, and processes at least annually?	Yes			
Supply Chain Management, Transparency, and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?	Yes			
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	Yes			
Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you permit tenants to perform independent vulnerability assessments?	Yes			We contract a specialized security firm to conduct vulnerability scans and penetration testing of our SaaS (applications and infrastructure); we will provide to our customer upon request an attestation of the penetration test conducted by the third party security firm. We allows penetration testing initiated by the customer at customer's expense. Customer testing may only be run against a test instance of the our SaaS that is a copy of production so that the test does not impact other customers. We must be provided advanced notice before such testing. Customers initiate this process by contacting our support.
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Yes			

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	Yes			
		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?	Yes			
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			We use a combination of automated and manual vulnerability scanning/exploitation tools in order to detect or confirm the presence of vulnerabilities in our SaaS infrastructure and application.
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes			
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	Yes			
		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	Yes			We have implemented a very fast patch process, so high-risk or critical security patches goes in production with deliberate speed. The patches or fixes are prioritised based on the

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Opencontent Answers			Notes
		TVM-02.6	(tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Will you provide your risk-based systems patching time frames to your tenants upon request?	Yes			risk associated to the respective vulnerabilities. We will provide a patching time frame to our customer as required.
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			x	Our Saas does not provide a specific app version for mobile
		TVM-03.2		Is all unauthorized mobile code prevented from executing?			x	