CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

Q. ID	Consensus Assessment Questions	Consensus Assessment Answers			Notes
		Yes	No	N/A	
AIS-01.1	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?		x		-
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	x			Use of SonarQube to find security defacts
AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	x			-
AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		x		-
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	x			OWASP directives are followed and bugs are reported internally on Vigilium Trac system
AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	x			See EULA on creating new account
AIS-02.2	Are all requirements and trust levels for customers' access defined and documented?	x			See EULA on creating new account
AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?		x		-
AIS-03.2	Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?		x		-
AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?		x		-

AAC-01.1	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?		x		-
AAC-01.2	Does your audit program take into account effectiveness of implementation of security operations?		x		-
AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	x			See AWS CSA CAIQ
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	x			See AWS CSA CAIQ
AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	x			Yearly planned vulnerability scan and penetration test
AAC-02.4	Do you conduct internal audits at least annually?	x			See AWS CSA CAIQ
AAC-02.5	Do you conduct independent audits at least annually?	x			See AWS CSA CAIQ
AAC-02.6	Are the results of the penetration tests available to tenants at their request?		x		See AWS CSA CAIQ
AAC-02.7	Are the results of internal and external audits available to tenants at their request?	x			See AWS CSA CAIQ
AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	x			See AWS CSA CAIQ
BCR-01.1	Does your organization have a plan or framework for business continuity management or disaster recovery management?	x			See AWS CSA CAIQ
BCR-01.2	Do you have more than one provider for each service you depend on?	x			See AWS CSA CAIQ
BCR-01.3	Do you provide a disaster recovery capability?	x			Disaster recovery procedure enabled (database backup on another region)
BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?	x			See AWS CSA CAIQ
BCR-01.5	Do you provide access to operational redundancy reports, including the services you rely on?		x		See AWS CSA CAIQ
BCR-01.6	Do you provide a tenant-triggered failover option?		x		Vigilium works in multi-tenant configuration
BCR-01.7	Do you share your business continuity and redundancy plans with your tenants?		x		See AWS CSA CAIQ
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	x			See AWS CSA CAIQ

BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	x			See AWS CSA CAIQ
BCR-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	x			See AWS CSA CAIQ
BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	x			See AWS CSA CAIQ
BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?	x			See AWS CSA CAIQ
BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		x		See AWS CSA CAIQ
BCR-07.1	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	x			See AWS CSA CAIQ
BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?	x			See AWS CSA CAIQ
BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	x			See AWS CSA CAIQ
BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	x			See AWS CSA CAIQ
BCR-09.2	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	x			See AWS CSA CAIQ
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	x			See AWS CSA CAIQ
BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	x			-
BCR-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	x			See INT_RicezioneArchivi procedure
BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	x			We backup data daily, weekly and monthy using dedicated AWS services
BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	x			We use a monitoring system to restart not working services

BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	x			Both software and infrastructure are coded and versionate
BCR-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?	x			AMIs can be exported and used on premise or at another provider
BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?		x		-
CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	x			See MRQ-07_01_MansionarioAziendale procedures
CCC-02.1	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	x			No external business partners
CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	x			No external business partners
CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	x			See PQ-8.3_SviluppoSoftware procedures
CCC-03.2	Is documentation describing known issues with certain products/services available?	x			See PQ-8.3_SviluppoSoftware procedures
CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	x			See PQ-8.3_SviluppoSoftware procedures
CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?		x		We use internal defined procedures for software development that are inspired to quality standards
CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?		x		-
CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	x			See PQ-8.3_SviluppoSoftware procedures
CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	x			See AWS CSA CAIQ
CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		x		We do not provide this level of granularity to customers
CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?	x			See AWS CSA CAIQ and CI/CD configuration on AWS
CCC-05.3	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	x			See AWS CSA CAIQ

DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	x			-
DSI-01.2	Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?		x		-
DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?		x		-
DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	x			See AWS CSA CAIQ
DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	x			See AWS CSA CAIQ
DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	x			Every public comunication from and to AWS applications make use of HTTPS and TSL
DSI-04.1	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?		x		-
DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		x		-
DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?		x		-
DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	x			See AWS CSA CAIQ
DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?		x		-
DSI-07.1	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	x			See AWS CSA CAIQ
DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	x			See AWS CSA CAIQ / appointment by GDPR
DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	x			See AWS CSA CAIQ
DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	x			See AWS CSA CAIQ

DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	x			See AWS CSA CAIQ
DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?	x			See AWS CSA CAIQ
DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	x			See AWS CSA CAIQ
DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	x			See AWS CSA CAIQ
DCS-05.1	Can you provide tenants with your asset management policies and procedures?	x			See AWS CSA CAIQ
DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	x			See AWS CSA CAIQ
DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	x			See AWS CSA CAIQ
DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	x			See AWS CSA CAIQ
DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	x			See AWS CSA CAIQ
DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	x			See AWS CSA CAIQ
EKM-01.1	Do you have key management policies binding keys to identifiable owners?		x		-
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?		x		Vigilium works in multi-tenant configuration
EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?		x		-
EKM-02.3	Do you maintain key management procedures?		x		-
EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?		x		-
EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?		x		-
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	x			We encrypt tenant data where necessary (IP address, email, device)

EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	x			Data on AWS are crypted; no uncrypted data exchange takes place between application network and public network; internal communication between services are not crypted
EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?		x		-
EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	x			We use Java Cryptographic Extension AES as encryption algorithm
EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?		x		We store encryption keys on configuration files in the cloud environment
EKM-04.3	Do you store encryption keys in the cloud?	x			We store encryption keys on configuration files in the cloud environment
EKM-04.4	Do you have separate key management and key usage duties?		x		-
GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	x			See AWS CSA CAIQ
GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	x			See AWS CSA CAIQ
GRM-02.1	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	x			See INT_PrivacyByDesign procedure
GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	x			As from GDPR, we conduct an annual review of risk assessment (DPIA)
GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	x			Appointment by GDPR
GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		x		-

GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?		x		-
GRM-05.1	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	x			Appointment by GDPR
GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	x			Appointment by GDPR
GRM-06.2	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?		x		-
GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	x			Appointment by GDPR
GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	x			-
GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?	x			GDPR compliance
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?		x		No sanction policies on procedure violation
GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?		x		See GRM-07.1
GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	x			As from GDPR, we conduct an annual review of risk assessment (DPIA)
GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?		x		Material changes to your information security and/or privacy policies are sent to persons involved but not notified to tenants
GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	x			Annual revision
GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	x			As from GDPR, we conduct an annual review of risk assessment (DPIA)

GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	x			As from GDPR, we conduct an annual review of risk assessment (DPIA)
GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	x			See risk assessment (DPIA) as from GDPR
GRM-11.2	Do you make available documentation of your organization-wide risk management program?		x		See risk assessment (DPIA) as from GDPR
HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	x			See INT_RestituzioneBeniInDotazione procedure
HRS-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?	x			See INT_RestituzioneBeniInDotazione procedure
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?		x		-
HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	x			Appointment by GDPR
HRS-03.2	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	x			Appointment by GDPR
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	x			See INT_InterruzioneRapportoDiLavoro procedure
HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	x			See INT_InterruzioneRapportoDiLavoro procedure
HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	x			Appointment by GDPR
HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	x			Annual revision of GDPR procedures
HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?		x		-

HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	x			Appointment by GDPR
HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	x			Appointment by GDPR
HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	x			-
HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	x			-
HRS-09.3	Do you document employee acknowledgment of training they have completed?	x			See INT_PianoFormazione procedure
HRS-09.4	Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	x			See INT_PianoFormazione procedure
HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	x			See INT_PianoFormazione procedure
HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	x			Appointment by GDPR
HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	x			Appointment by GDPR
HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	x			Appointment by GDPR
HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	x			Appointment by GDPR
HRS-11.1	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	x			Appointment by GDPR
HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	x			Appointment by GDPR
IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	x			-
IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	x			-

IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?		x		-
IAM-02.2	Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	x			Appointment by GDPR
IAM-02.3	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?		x		-
IAM-02.4	Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	x			Filters applied on database make data separation available
IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	x			Vigilium access is allowed only ti authorized users with user ID and password; new user accounts are created to have minimal access and access privileges are restricted based on business need and job responsibilities
IAM-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?		x		Multifactor authentication not required for Vigilium security needs
IAM-02.7	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		x		-
IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	x			-
IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	x			See INT_AccessoInfrastruttura procedure
IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	x			See INT_AccessoInfrastruttura procedure
IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?		x		-
IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	x			See AWS CSA CAIQ
IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	x			See AWS CSA CAIQ
IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?			x	See AWS CSA CAIQ

IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?			x	See AWS CSA CAIQ
IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?		x		We apply customer's grants on the basis of tenants' requests
IAM-08.2	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?			x	We do not allow tenants or customer to access users' identities
IAM-08.3	Do you limit identities' replication only to users explicitly defined as business necessary?			x	No identities' replication
IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	x			We apply customer's grants on the basis of tenants' requests
IAM-09.2	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	x			We apply customer's grants on the basis of tenants' requests
IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	x			We provide customers with users' list in order to check their privilege and customers have to notify users grants de-/provisioning
IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?			x	See IAM-10.1
IAM-10.3	Do you ensure that remediation actions for access violations follow user access policies?	x			See AGID-Vigilium-Saas_proc_gestione-segnalazioni and AGID-Vigilium-Saas_qualita-servizio-slo
IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?			x	-
IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	x			-
IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	x			-

IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?		x		Feature not available
IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?		x		Feature not available
IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?		x		Feature not available
IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		x		Not required for Vigilium security needs
IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?		x		Feature not available
IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?		x		Multifactor authentication not required for Vigilium security needs
IAM-12.7	Do you allow tenants to use third-party identity assurance services?		x		Feature not available
IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	x			Password minimum length and complexity and account lockout in case of repeated login failure are supported
IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?		x		Not required for Vigilium security needs
IAM-12.10	Do you support the ability to force password changes upon first logon?		x		Not required for Vigilium security needs
IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	x			A reset password procedure (sending an email continaing token) is available
IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	x			See AWS CSA CAIQ
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?			x	-
IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	x			See AWS CSA CAIQ
IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	x			See AWS CSA CAIQ
IVS-01.4	Are audit logs centrally stored and retained?	x			See AWS CSA CAIQ
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	x			See AWS CSA CAIQ

IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?			x	The infrastructure does not contain VW to be maintained; Docker images are automatically built and recorded starting from versioned source code
IVS-02.2	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	x			AWS cloudtrail monitors every API request intercating with AWS infrastructre
IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	x			We use predefined VM images managed by AWS; application images are automatically built and recorded
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	x			See AWS CSA CAIQ
IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	x			See AWS CSA CAIQ
IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	x			See AWS CSA CAIQ
IVS-04.3	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	x			See AWS CSA CAIQ
IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	x			See AWS CSA CAIQ
IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	x			See AWS CSA CAIQ
IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	x			See AWS CSA CAIQ
IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	x			-
IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	x			-
IVS-06.4	Are all firewall access control lists documented with business justification?	x			We use the least priviliges to make application works

IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	x			See AWS CSA CAIQ
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	x			-
IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	x			No Iaas offering
IVS-08.3	Do you logically and physically segregate production and non-production environments?	x			See AWS CSA CAIQ
IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	x			See AWS CSA CAIQ
IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	x			See AWS CSA CAIQ
IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	x			See AWS CSA CAIQ
IVS-09.4	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	x			All endpoints are accessed using a token related to a single tenant code that automatically filters records when querying database tables
IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	x			We use virtual firewall as Security Group to limit access to infrastructure
IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	x			We use DMS for migration, which operations are crypted using KMS
IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	x			Production data are isolated from non-production environments
IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	x			See AWS CSA CAIQ

IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			x	See AWS CSA CAIQ
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	See AWS CSA CAIQ
IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			x	See AWS CSA CAIQ
IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?		x		-
IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	x			See AWS CSA CAIQ
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	x			All APIs are customized for the purposes of the service and detailed in a PDF document
IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	x			AWS environments can be exported in any industry supported format
IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?		x		Service-to-service application (API) and/or interoperability not provided as service to customers
IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	x			AMIs can be exported and used on premise or at another provider
IPY-03.3	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?		x		-
IPY-04.1	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?			x	No import/export data flows outside AWS infrastructure (except for system initialization)

IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	x			See AWS CSA CAIQ
IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	x			See AWS CSA CAIQ
IPY-05.2	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			AMIs can be exported and used on premise or at another provider
IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?		x		See AWS CSA CAIQ
MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			x	See AWS CSA CAIQ
MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			x	See AWS CSA CAIQ
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			x	See AWS CSA CAIQ
MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			x	See AWS CSA CAIQ
MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			x	See AWS CSA CAIQ
MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			x	See AWS CSA CAIQ
MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			x	See AWS CSA CAIQ
MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			x	See AWS CSA CAIQ
MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			x	See AWS CSA CAIQ
MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			x	See AWS CSA CAIQ
MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			x	See AWS CSA CAIQ

MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			x	See AWS CSA CAIQ
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	See AWS CSA CAIQ
MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			x	See AWS CSA CAIQ
MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?			x	See AWS CSA CAIQ
MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			x	See AWS CSA CAIQ
MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			x	See AWS CSA CAIQ
MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			x	See AWS CSA CAIQ
MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?			x	See AWS CSA CAIQ
MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			x	See AWS CSA CAIQ
MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			x	See AWS CSA CAIQ
MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			x	See AWS CSA CAIQ
MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			x	See AWS CSA CAIQ
MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			x	See AWS CSA CAIQ
MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			x	See AWS CSA CAIQ
MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			x	See AWS CSA CAIQ
MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			x	See AWS CSA CAIQ
MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			x	See AWS CSA CAIQ
MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			x	See AWS CSA CAIQ

SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	x			See AWS CSA CAIQ
SEF-02.1	Do you have a documented security incident response plan?	x			See AWS CSA CAIQ
SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?		x		-
SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	x			See AWS CSA CAIQ
SEF-02.4	Have you tested your security incident response plans in the last year?	x			See AWS CSA CAIQ
SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	x			See AWS CSA CAIQ
SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	x			See AWS CSA CAIQ
SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	x			See AWS CSA CAIQ
SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	x			See AWS CSA CAIQ
SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	x			Backing-up databases, disabling users, …
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	x			Filters applied on database make data separation available
SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	x			See AWS CSA CAIQ
SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?		x		See AWS CSA CAIQ
STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?		x		-
STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	x			See AWS CSA CAIQ
STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	x			See AWS CSA CAIQ
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	x			See AWS CSA CAIQ

STA-03.2	Do you provide tenants with capacity planning and use reports?		x		We dot not provide such features to customer
STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	x			Annual revision of GDPR procedures
STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?			x	No outspurced providers beside AWS
STA-05.2	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?			x	No outspurced providers beside AWS
STA-05.3	Does legal counsel review all third-party agreements?	x			No third-party agreements beside AWS' ones; see AWS CSA CAIQ
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	x			No third-party agreements beside AWS' ones; see AWS CSA CAIQ
STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	x			By using periodic backups lost customer data can be retrieved
STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	x			All data are stored on infrastructure based in Milano, Italy
STA-05.7	Can you provide the physical location/geography of storage of a tenant's data upon request?	x			All data are stored on infrastructure based in Milano, Italy
STA-05.8	Can you provide the physical location/geography of storage of a tenant's data in advance?	x			All data are stored on infrastructure based in Milano, Italy
STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		x		Not required
STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?		x		No intrusion monitoring automatic systems available
STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		x		See AWS CSA CAIQ
STA-05.12	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		x		See AWS CSA CAIQ
STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?			x	No partner's supply chain beside AWS

STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	x			See AWS CSA CAIQ
STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?			x	See AWS CSA CAIQ
STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?			x	See AWS CSA CAIQ
STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	x			See AWS CSA CAIQ for CSP and AGID-Vigilium-Saas_performance-sla for SaaS
STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	x			AWS CloudWatch provides monitoring for Vigilum applications
STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?		x		-
STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?		x		-
STA-07.8	Do you review all service level agreements at least annually?	x			-
STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?			x	See AWS CSA CAIQ
STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?			x	See AWS CSA CAIQ
STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	x			See AWS CSA CAIQ
STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	x			Yearly planned vulnerability scan and penetration test
TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	x			See AWS CSA CAIQ
TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	x			See AWS CSA CAIQ
TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	x			See AWS CSA CAIQ

TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	x			Yearly planned vulnerability scan and penetration test
TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	x			Yearly planned vulnerability scan and penetration test
TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	x			-
TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	x			Both software and infrastructure are coded, enabling quick patches propagation on applications and infrastructure
TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?			x	Customer data are not part of the service
TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	x			All mobile code within Vigilium is compliant with design and implementation documentation
TVM-03.2	Is all unauthorized mobile code prevented from executing?			x	-