CAIQ Lite Kayako

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE - LITE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers				Notes
					Yes	No	Not Applicable	State	
Application & Interface Security *Application Security*	AIS-01	AIS-01.2	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 an automated source code analysis tool to detect security defects in code prior to production?	X			Generic	
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Generic	
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?	X			AWS Specific	Our company has implemented an extensive information security program designed to protect information subject to privacy laws, to ensure data security and confidentiality, protect against anticipated threats or hazards or unauthorized access. AWS's security is best-in-class and its customers benefit from limitless scalability, improved monitoring and notification, and a series of industry recognized security certifications including ISO 27018 compliance for PII, HIPAA, SOC, and PCI. Copies of the AWS compliance certifications can be obtained directly from AWS at https://aws.amazon.com/artifact/ by creating a free AWS account or using an existing account. In addition to the data security benefits we receive from AWS."
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?	X			Generic	
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			Specific	AWS maintains a series of industry recognized security certifications including SSAE16 and, more recently SSAE18. Copies of the AWS compliance certifications can be obtained directly from AWS here (https://aws.amazon.com/artifact/) by creating a free AWS account or using an existing account.
	CO-02	AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	X			Specific	Quarterly vulnerability scans are carried out.
	CO-02	AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Specific	Quarterly vulnerability scans are carried out.
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?	X			Generic	
	CO-05	AAC-03.2		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?		X		Specific	
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?	X			Generic	

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE - LITE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers				Notes
					Yes	No	Not Applicable	State	
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?	x			Specific	https://status.kayako.com/
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?	x			Generic	Operational workflows are based on JIRA/Confluence and operationalized runbooks for all processes.
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 retention policies?	x			Specific	Specific retention policies can be set, as per customers' requirements.
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	x			AWS Specific	AWS Backups
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	x			Generic	
Change Control & Configuration Management *Unauthorized Software Installations*		CCC-01.2	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	Is documentation available that describes the installation, configuration, and use of products/services/features?	x			Generic	Operational workflows are based on JIRA/Confluence and operationalized runbooks for all processes.
	CCC-04	CCC-04.1		Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	x			Generic	
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)?	x			Generic	All web interactions use TLS
	IS-28	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			Specific	
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?	x			Generic	
Data Security & Information Lifecycle Management	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	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	x			Generic	

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers				Notes
					Yes	No	Not Applicable	State	
Secure Disposal	DG-05	DSI-07.2	media, ensuring data is not recoverable by any computer forensic means.	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			Generic	We have policies and procedures in place for the removal of data from all repositories, once the customer has exited the enviroment following a termination of contract. We do not publish externally specific copies of policies or procedures.
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?	X			Generic	
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?	X			AWS Specific	We are utilizing Amazon Web Services ("AWS") for hosting. Besides the best-in-class security, AWS's customers benefit from limitless scalability, improved monitoring and notification, and a series of industry recognized security certifications including ISO 27018 compliance for PII, HIPAA, SOC, and PCI. For more information, go to https://aws.amazon.com/compliance/ Copies of the AWS compliance certifications can be obtained directly from AWS at https://aws.amazon.com/artifact/ by creating a free AWS account or using your existing account. In addition to the data security benefits we receive from AWS, several of our products undergo independent audits (SOC 1 and 2, PCI, ISO, etc) to ensure that our corporate policies, procedures and practices are aligned with the highest levels of data security.
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X			AWS Specific	AWS compliance with ISO 27001 / SSAE16 SOC1 / SOC2 cover this requirement.
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 tenant?		X		Specific	
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?	X			Specific	Databases in the EU are encrypted and for non-EU hosting, we are currently formulating a schedule for having this environment also protected with the same encryption approaches. On-premise customers are responsible for the security of their data center.

CAIQv3.0.1

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE - LITE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers				Notes
					Yes	No	Not Applicable	State	
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.)?	x			Generic	Guideline for securing all components have been provided to the SaaSOps teams by the Security team and are laid out in the organisational Information Security and Compliance Program attached.
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.)?	x			Generic	
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?	x			Generic	
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	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	x			Generic	As specified in the contractual agreement or required by applicable laws.
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	x			Generic	
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?	x			Generic	
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	x			Generic	
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?	x			Generic	All staff are required to undertake complany-wide Security Awareness training as well as role specific training related.
		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	x			Generic	
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	x			Generic	
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?	x			Generic	
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.)?	x			Generic	
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	x			Generic	

CAIQ v3.0.1

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE - LITE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers				Notes
					Yes	No	Not Applicable	State	
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 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) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	x			Generic	
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?	x			Generic	
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 established user access policies and procedures.	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			Generic	
	IS-33	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			Generic	
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?	x			Generic	

CAIQ v3.0.1

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE - LITE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers				Notes
					Yes	No	Not Applicable	State	
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)?	X			Generic	
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?	X			Generic	Company staff access is required to be fully deprovisioned within 48 hours of notice by manager. Based on risk, that may be expedited.
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?	X			Specific	AWS provides certain baseline alerting of suspicious traffic.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X			Generic	
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e. g., with automated tools)?	X			Generic	
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?	X			Generic	
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?	X			Generic	
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?	X			Generic	Test environments are separated from Production environments. Customers are provided with environments as described in the contractual agreement.
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	X			Generic	Test environments are separated from Production environments
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?	X			Generic	

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE - LITE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers				Notes
					Yes	No	Not Applicable	State	
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)?	X			Generic	
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 unauthorized (rogue) wireless network devices for a timely disconnect from the	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	X			Generic	Production networks do not use wireless technologies. All access to corporate networks requires VPN.
	SA-10	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			Generic	Production networks do not use wireless technologies. All access to corporate networks requires VPN.
	SA-10	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	Generic	Wireless networks are not available within the data centre. All devices connercting to the corporate network use VPN connection.
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?	X			Generic	
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	Specific	
Security Incident Management, E-Discovery, & Cloud Forensics	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	Do you have a documented security incident response plan?	X			Generic	See IT Security & Compliance Program attached.
		SEF-02.4		Have you tested your security incident response plans in the last year?	X			Generic	
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?			X	Generic	
	IS-23	SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	X			Generic	
	IS-24	SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			Generic	
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)?	X			Generic	As contractually agreed and legally required.
Supply Chain Management, Transparency, and Accountability	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	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			Generic	
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X			Generic	
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?		X		Generic	We are performing periodic internal vulnerability scans and can provide summary reports, if contractually agreed.
Threat and Vulnerability Management *Antivirus / Malicious*	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,	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	X			Generic	
	IS-20	TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	X			Generic	

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE - LITE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers				Notes
					Yes	No	Not Applicable	State	
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			Specific	
© Copyright 2014 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire CAIQ Version 3.0.1" at http://www.cloudsecurityalliance.org subject to the following: (a) the Consensus Assessments Initiative Questionnaire v3.0.1 may be used solely for your personal, informational, non-commercial use; (b) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be modified or altered in any way; (c) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Consensus Assessments Initiative Questionnaire v3.0.1 as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 (2014). If you are interested in obtaining a license to this material for other usages not addresses in the copyright notice, please contact info@cloudsecurityalliance.org.									