Description

This document is the CAIQ v3.1, that contains an updated questionnaire since its predecessor CAIQ v3.0.1.

CAIQ provices a cloud consumer and cloud auditor with the opportunity to ascertain that their cloud service provider is compliant to the Cloud Controls Matrix (CCM). Therefore, it helps cloud customers to gauge the security posture of prospective cloud service providers and determine if their cloud services are suitably secure.

The document is structured as follows. The "CSA CAIQ v3.1" tab contains the CAIQ questionnaire, in which columns A-D contain the CCM v3.0.1 controls, column E the consensus assessment questions and W-Y the column for the answers. The "Changelog" provides the list of changes applied to the CAIQ in terms of edited/shifted/ new created questions.

The CSA and the CCM working group hope that organizations will find this document useful for their cloud security compliance programs.

The contents of this document could contain technical inaccuracies, typographical errors and out-of-date information.

If you would like to volunteer in the CCM working group, please sign up here: https://cloudsecurityalliance.org/research/join-working-group/

Acknowledgements

Contributors

Jon-Michael Brook
Kevin Bugin
Angela Dogan
Shawn Harris
Harry Lu
Kevin Pike
Michael Roza
Dinesh Udaiwal
Andrew Williams

CSA Staff

Daniele Catteddu
Victor Chin
Alain Pannetrat
Eleftherios Skoutaris

Change Log

Date	Version	Notes
30/09/2019	1	Publication of the Consensus Assessments Initiative Questionnaire (CAIQ) version 3.1.

CAIQv3.1

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?		X		
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?		X		
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	X			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (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		
Application & Interface Security *Customer Access*	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			
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	X			
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	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			
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	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?				
		AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?				
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?			X	
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?				
		AAC-02.4		Do you conduct internal audits at least annually?	X			
		AAC-02.5		Do you conduct independent audits at least annually?	X			
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?		X		
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?		X		
Audit Assurance & Compliance *Information System*	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	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			
		BCR-01.2		Do you have more than one provider for each service you depend on?			X	
		BCR-01.3		Do you provide a disaster recovery capability?			X	
		BCR-01.4		Do you monitor service continuity with upstream providers in the event of provider failure?	X			
		BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?			X	
		BCR-01.6		Do you provide a tenant-triggered failover option?			X	
		BCR-01.7		Do you share your business continuity and redundancy plans with your tenants?		X		
Business Continuity Management &	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	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?		X		
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and			X	
		BCR-03.2		Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?			X	
Business Continuity	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides,	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized	X			
Business Continuity	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as	Is physical damage anticipated and are countermeasures included in the design of physical protections?			X	
Business Continuity	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods,			X	
Business Continuity Management &	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?			X	
		BCR-07.2		Do you have an equipment and datacenter maintenance routine or plan?			X	
Business Continuity	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures,			X	
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 use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			
		BCR-09.2		Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			
Business Continuity	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	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 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				
		BCR-11.3		Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			
		BCR-11.4		If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?			X	
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?			X	
		BCR-11.6		Does your cloud solution include software/provider independent restore and recovery capabilities?			X	
		BCR-11.7		Do you test your backup or redundancy mechanisms at least annually?	X			
Change Control &	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business	Are policies and procedures established for management authorization for development or acquisition of new applications,	X			
Change Control & Configuration	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	X			
		CCC-02.2		Are policies and procedures adequately enforced to ensure external business partners comply with change management	X			
Change Control & Configuration *Management* *Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			
		CCC-03.2		Is documentation describing known issues with certain products/services available?	X			
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service			X	
		CCC-03.4		Do you have controls in place to ensure that standards of quality are being met for all software development?	X			
		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			
Change Control &	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?			X	
Change Control & Configuration Management	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual)	Do you provide tenants with documentation that describes your production change management procedures and their	X			
		CCC-05.2		Do you have policies and procedures established for managing risks with respect to change management in production	X			
		CCC-05.3		Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in	X			
Data Security & Information Lifecycle Management	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest			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	
Data Security & Information Lifecycle Management *Data Inventory /*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical	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			
Data Security & Information Lifecycle Management	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 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			
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?			X	
Data Security & Information Lifecycle Management *Handling / Labeling /*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for 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		
Data Security &	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	**X**			
Data Security &	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?		X		
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?			X	
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing			X	
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	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			
		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			X	
Datacenter Security	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates,	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication			X	
Datacenter Security *Equipment*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to	Do you have a capability to use system geographic location as an authentication factor?		X		
		DCS-03.2		Is automated equipment identification used as a method to validate connection authentication integrity based on known			X	
Datacenter Security	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?			X	
Datacenter Security	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of	Can you provide tenants with your asset management policies and procedures?			X	
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure			X	
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies,			X	
Datacenter Security	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor			X	
Datacenter Security	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises,			X	
Datacenter Security	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support	Do you restrict physical access to information assets and functions by users and support personnel?			X	
Encryption & Key	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there	Do you have key management policies binding keys to identifiable owners?		X		
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	Do you have a capability to allow creation of unique encryption keys per tenant?		X		
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?		X		
		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		
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	Do you encrypt tenant data at rest (on disk/storage) within your environment?		X		
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and		X		
		EKM-03.3		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?		X		
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question),	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?		X		
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?		X		
		EKM-04.3		Do you store encryption keys in the cloud?		X		

		EKM-04.4	but maintained by the cloud consumer or trusted key management	Do you have separate key management and key usage duties?		X		
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	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating			X	
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?			X	
Governance and Risk Management	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for	X			
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X			
Governance and Risk	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security	X			
Governance and Risk Management	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes	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			
Governance and Risk	GRM-05	GRM-05.1	Executive and line management shall take formal action to support	Do executive and line management take formal action to support information security through clearly-documented	X			
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	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized	X			
		GRM-06.2		Are information security policies authorized by the organization's business leadership (or other accountable business role or	X			
		GRM-06.3		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			
		GRM-06.4		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or	X			
		GRM-06.5		Do you disclose which controls, standards, certifications, and/or regulations you comply with?		X		
Governance and Risk Management	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			
Governance and Risk	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies,	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain	X			
Governance and Risk Management	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	Do you notify your tenants when you make material changes to your information security and/or privacy policies?		X		
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	X			
Governance and Risk Management	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals,	X			
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X			
Governance and Risk Management	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with	Do you have a documented, organization-wide program in place to manage risk?	X			
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?			X	
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	Upon termination of contract or business relationship, are employees and business partners adequately informed of their	X			
		HRS-01.2		Do you have asset return procedures outlining how assets should be returned within an established period?	X			
Human Resources	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved			X	
Human Resources *Employment*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and	X			
		HRS-03.2		Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting	X			
Human Resources *Employment*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			
Human Resources	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data	X			
Human Resources	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data	X			
Human Resources	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned	X			
		HRS-08.2		Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	X			
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues	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			
		HRS-09.4		Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to			X	
		HRS-09.5		Are personnel trained and provided with awareness programs at least once a year?	X			
		HRS-09.6		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies,	X			
		HRS-10.2		Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			
		HRS-10.3		Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			
		HRS-11.2		Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive	X			
Identity & Access Management	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	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls,	X			
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			
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	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	X			
		IAM-02.3		Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least	X			
		IAM-02.4		Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X			
		IAM-02.5		Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X			
		IAM-02.6		Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case	X			
		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		X		
Identity & Access	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			
Identity & Access Management	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	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?				
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?			X	
Identity & Access	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?			X	
Identity & Access Management	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	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is	X			
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is				
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood	Does your organization conduct third-party unauthorized access risk assessments?	X			
		IAM-07.2		Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access?	X			
Identity & Access Management *User Access*	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	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of		X		
		IAM-08.2		Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of		X		
		IAM-08.3		Do you limit identities' replication only to users explicitly defined as business necessary?	X			
Identity & Access Management	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers	X			
		IAM-09.2		Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants),		X		
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	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and	X			
		IAM-10.2		Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			
		IAM-10.3		Do you ensure that remediation actions for access violations follow user access policies?			**X**	
		IAM-10.4		Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant			**X**	
Identity & Access Management	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual)	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data	X			
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of	X			
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?		X		
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?		X		
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing		X		
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		X		
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and	X			
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user		X		
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?		X		
		IAM-12.8		Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout	X			
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?		X		
		IAM-12.10		Do you support the ability to force password changes upon first logon?	X			
		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	X			
Identity & Access	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object,	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and			X	
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	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by	X			
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X			
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has			X	
		IVS-01.4		Are audit logs centrally stored and retained?	X			
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			
Infrastructure & Virtualization Security	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?			X	
		IVS-02.2		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to			X	
		IVS-02.3		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made			X	
Infrastructure &	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			
Infrastructure & Virtualization Security *Capacity / Resource*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you			X	
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			X	
		IVS-04.3		Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems	X			
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements	X			
Infrastructure &	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization			X	
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence			X	
		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			X	
		IVS-06.4		Are all firewall access control lists documented with business justification?			X	
Infrastructure &	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using	X			
Infrastructure & Virtualization Security	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	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	
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	X			
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:	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security			X	
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and			X	
		IVS-09.3		Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure			X	
		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,	X			
		IVS-09.5		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive			X	
Infrastructure & Virtualization	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual			X	
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual			X	
Infrastructure &	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting			X	
Infrastructure & Virtualization 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:	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network			X	
		IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with			X	
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the			X	
Infrastructure & Virtualization	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance	X			
		IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and			X	
Interoperability &	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			
Interoperability &	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability,	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your	X			
		IPY-03.2		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?				
		IPY-03.3		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from	X			
Interoperability & Portability	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry	X			
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol	X			
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure			X	
		IPY-05.2		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to			X	
		IPY-05.3		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available			X	
Mobile Security	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			X	
Mobile Security	MOS-02	MOS-02.1	A documented list of approved application stores has been	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data	?			
Mobile Security	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved	?			
Mobile Security	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD			X	
Mobile Security	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted	X			
Mobile Security	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company	X			
Mobile Security	MOS-07	MOS-07.1	The company shall have a documented application validation process to	Do you have a documented application validation process for testing device, operating system, and application compatibility	X			
Mobile Security	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			X	
Mobile Security	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g.,	X			
Mobile Security	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store,	?			
Mobile Security	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive	?			
Mobile Security *Jailbreaking and*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or	?			
		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the	?			
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	
		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			
Mobile Security	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	X			
Mobile Security	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change	X			
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	X			
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?	?			
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	X			
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X	
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	?			

Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software	Do your mobile devices have the latest available security-related patches installed upon general release by the device	**X**			
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X	
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	
Security Incident	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			
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 policies and procedures.	Do you have a documented security incident response plan?	X			
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?	X			
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security		X		
		SEF-02.4		Have you tested your security incident response plans in the last year?		X		
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03	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.	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent	X			
		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			
Security Incident Management, E-Discovery, & Cloud Forensics	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes	X			
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing	X			
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			
Security Incident Management, E-	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?		X		
Supply Chain Management,	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct	X			
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based	X			
Supply Chain	STA-02	STA-02.1	The provider shall make security incident information available to all	Do you make security incident information available to all affected customers and providers periodically through electronic			X	
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?			X	
		STA-03.2		Do you provide tenants with capacity planning and use reports?	X			
Supply Chain	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting	X			
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship,	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and	X			
		STA-05.2		Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?			X	
		STA-05.3		Does legal counsel review all third-party agreements?	X			
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X			
		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			
		STA-05.6		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?			X	
		STA-05.7		Can you provide the physical location/geography of storage of a tenant’s data upon request?	X			
		STA-05.8		Can you provide the physical location/geography of storage of a tenant's data in advance?	X			
		STA-05.9		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		X		
		STA-05.10		Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their	X			
		STA-05.11		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?			X	
		STA-05.12		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		X		
Supply Chain	STA-06	STA-06.1	Providers shall review the risk management and governance processes of	Do you review the risk management and governance processes of partners to account for risks inherited from other members of			X	
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining	X			
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain	X			
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X			
		STA-07.4		Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			
		STA-07.5		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?		X		
		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?	0		X	
		STA-07.8		Do you review all service level agreements at least annually?	X			
Supply Chain Management,	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			
Supply Chain Management,	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security			X	
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and	X			
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT	X			
		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			
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?			X	
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?		X		
		TVM-02.5		Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			
		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			
Threat and Vulnerability Management	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	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized			X	
		TVM-03.2		Is all unauthorized mobile code prevented from executing?			X	

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1 Detailed Changelog			
Question ID	Consensus Assessment Questions	Type of Change	Description
AIS-01.1	Do you use industry standards (OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	Edited	Edits have been made to AIS-01.1. Included OWASP Software Assurance Maturity Model and ISO/IEC 27034 as examples.
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	No Change	No change to AIS-01.2.
AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	No Change	No change to AIS-01.3.
AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	No Change	No change to AIS-01.4.
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	No Change	No change to AIS-01.5.
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?	No Change	No change to AIS-02.1.
AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	No Change	No change to AIS- 02.2.
AIS-03.1	Do your data management policies and procedures require audits to verify data input and output integrity routines?	Shifted	HRS-11.2 has been shifted to AIS-03.1. Question has also been edited to more accurately reflect CCM control.
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?	Edited	Edits have been made to AIS-03.2. MD5 and SHA checksums have been used as the examples.
AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	No Change	No change to AIS-04.1.
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?	New Question	New question added to AAC-01.1.
AAC-0.1.2	Does your audit program take into account effectiveness of implementation of security operations?	Shifted	AAC-02.8 has been shifted to AAC-0.1.2. Also edited for clarify.

AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	No Change	No change to AAC-02.1.
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	Edited	Edits have been made to AAC-02.2. Cadence of penetration tests have been changed to align with CCM requirements.
AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	No Change	No change to AAC-02.3.
AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	No Change	No change to AAC-02.4.
AAC-02.5	Do you conduct internal audits at least annually?	Edited	Edits have been made to AAC-02.5. Cadence of audits have been changed to align with CCM requirements.
AAC-02.6	Do you conduct external audits at least annually?	Edited	Edits have been made to AAC-02.6. Cadence of audits have been changed to align with CCM requirements. Changed "external" with "independent".
AAC-02.7	Are the results of internal and external audits available to tenants at their	No Change	No change to AAC-02.7.
AAC-03.1	Do you have a program in place that includes the ability to monitor changes to	No Change	No change to AAC-03.1.
BCR-01.1	Does your organization have a plan or framework for business continuity	New Question	New question added to BCR-01.1.
BCR-01.2	Do you have more than one provider for each service you depend on?	Shifted	IAM-07.3 has been shifted to BCR-01.2.
BCR-01.3	Do you provide multi-failure disaster recovery capability?	Shifted	IAM-07.1 has been shifted to BCR-01.3.
BCR-01.4	Do you monitor service continuity with upstream providers in the event of	Shifted	IAM-07.2 has been shifted to BCR-01.4.
BCR-01.5	Do you provide access to operational redundancy report, including the	Shifted	IAM-07.4 has been shifted to BCR-01.5. Edits have also
BCR-01.6	Do you provide a tenant-triggered failover option?	Shifted	IAM-07.6 has been shifted to BCR-01.6.
BCR-01.7	Do you share your business continuity and redundancy plans with your	Shifted	IAM-07.7 has been shifted to BCR-01.7.
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon	No Change	No change to BCR-02.1.
BCR-03.1	Does your organization adhere to any international or industry standards	New Question	New question added to BCR-03.1.
BCR-03.2	Has your organization implemented environmental controls, fail-over	New Question	New question added to BCR-03.2.
BCR-04.1	Are information system documents (e.g., administrator and user guides,	No Change	No change to BCR-04.1.
BCR-05.1	Is physical damage anticipated and are countermeasures included in the	Edited	Edits have been made to BCR-05.1. The question has been
BCR-06.1	Are any of your data centers located in places that have a high	No Change	No change to BCR-06.1.
BCR-07.1	Do you have a documented policies, procedures and supporting business	New Question	New question added to BCR-07.1.
BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?	New Question	New question added to BCR-07.2.
BCR-08.1	Are security mechanisms and redundancies implemented to protect	No Change	No change to BCR-08.1.
BCR-09.1	Do you use industry standards and frameworks to determine the impact of any	New Question	New question added to BCR-09.1.

BCR-09.2	Does you organization conduct impact analysis pertaining to possible	New Question	New question added to BCR-09.2.
BCR-10.1	Are policies and procedures established and made available for all personnel	No Change	No change to BCR-10.1.
BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	Edited	Edits have been made to BCR-11.1. 'Control' has been
BCR-11.2	Do you have documented policies and procedures demonstrating adherence	New Question	New question added to BCR-11.2.
BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance	Edited	Edits have been made to BCR-11.3. Changed 'redunday
BCR-11.4	If using virtual infrastructure, does your cloud solution include independent	Shifted	BCR-07.1 has been shifted to BCR-11.4.
BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to	Edited	Changed "state in time" to "configuration"
BCR-11.6	Does your cloud solution include software/provider independent restore and	Shifted	BCR-07.5 has been shifted to BCR-11.6.
BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	No Change	No change to BCR-11.7.
CCC-01.1	Are policies and procedures established for management authorization for	No Change	No change to CCC-01.1.
CCC-02.1	Are policies and procedures for change management, release, and testing	New Question	New question added to CCC-02.1.
CCC-02.2	Are policies and procedures adequately enforced to ensure external business	New Question	New question added to CCC-02.2.
CCC-03.1	Do you have a defined quality change control and testing process in place	New Question	New question added to CCC-03.1.
CCC-03.2	Is documentation describing known issues with certain products/services	No Change	No change to CCC-03.2.
CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs	No Change	No change to CCC-03.3.
CCC-03.4	Do you have controls in place to ensure that standards of quality are being met	Shifted	CCC-02.1 has been shifted to CCC-03.4.
CCC-03.5	Do you have controls in place to detect source code security defects for any	Shifted	CCC-02.2 has been shifted to CCC-03.5.
CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements	No Change	No change to CCC-03.6.
CCC-04.1	Do you have controls in place to restrict and monitor the installation of	No Change	No change to CCC-04.1.
CCC-05.1	Do you provide tenants with documentation that describes your production	No Change	No change to CCC-05.1.
CCC-05.2	Do you have policies and procedures established for managing risks with	New Question	New question added to CCC-05.2.
CCC-05.3	Do you have technical measures in place to ensure that changes in production	New Question	New question added to CCC-05.3.
DSI-01.1	Do you provide a capability to identify data and virtual machines via policy	No Change	No change to DSI-01.1.
DSI-01.2	Do you provide a capability to identify data and hardware via policy	No Change	No change to DSI-01.2.
DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident	No Change	No change to DSI-02.1.
DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical	No Change	No change to DSI-02.2.
DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption	Edited	Edits have been made to DSI-03.1. Original example of
DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure	No Change	No change to DSI-03.2.
DSI-04.1	Are policies and procedures established for data labeling and handling in order	Edited	Edits have been made to DSI-04.1. Semantic of the
DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML	Shifted	DSI-01.6 has been shifted to DSI-04.2.
DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as	No Change	No change to DSI-04.3.
DSI-05.1	Do you have procedures in place to ensure production data shall not be	No Change	No change to DSI-05.1.
DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned,	No Change	No change to DSI-06.1.
DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of	Edited	The reference to tenant is removed as there may be cases
DSI-07.2	Can you provide a published procedure for exiting the service arrangement,	No Change	No change to DSI-07.2.
DCS-01.1	Do you classify your assets in terms of business criticality, service-level	Edited	Edits have been made to DCS-01.1. Phrasing has been

DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all	New Question	New question added to DCS-01.2.
DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates,	No Change	No change to DCS-02.1.
DCS-03.1	Do you have a capability to use system geographic location as an	Shifted	DSI-01.3 has been shifted to DCS-03.1.
DCS-03.2	Is automated equipment identification used as a method to validate	No Change	No change to DCS-03.2.
DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software,	New Question	New question added to DCS-04.1.
DCS-05.1	Can you provide tenants with your asset management policies and	Edited	Edits have been made to DCS-05.1. Language has been
DCS-06.1	Can you provide evidence that policies, standards, and procedures have been	No Change	No change to DCS-06.1.
DCS-06.2	Can you provide evidence that your personnel and involved third parties have	No Change	No change to DCS-06.2.
DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards,	New Question	New question added to DCS-07.1.
DCS-08.1	Are ingress and egress points, such as service areas and other points where	No Change	No change to DCS-08.1.
DCS-09.1	Do you restrict physical access to information assets and functions by users	No Change	No change to DCS-09.1.
EKM-01.1	Do you have key management policies binding keys to identifiable owners?	No Change	No change to EKM-01.1.
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per	No Change	No change to EKM-02.1.
EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	No Change	No change to EKM-02.2.
EKM-02.3	Do you maintain key management procedures?	No Change	No change to EKM-02.3.
EKM-02.4	Do you have documented ownership for each stage of the lifecycle of	No Change	No change to EKM-02.4.
EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage	No Change	No change to EKM-02.5.
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	No Change	No change to EKM-03.1.
EKM-03.2	Do you leverage encryption to protect data and virtual machine images during	No Change	No change to EKM-03.2.
EKM-03.3	Do you have documentation establishing and defining your encryption	No Change	No change to EKM-03.3.
EKM-04.1	Do you have platform and data appropriate encryption that uses	No Change	No change to EKM-04.1.
EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key	No Change	No change to EKM-04.2.
EKM-04.3	Do you store encryption keys in the cloud?	No Change	No change to EKM-04.3.
EKM-04.4	Do you have separate key management and key usage duties?	No Change	No change to EKM-04.4.
GRM-01.1	Do you have documented information security baselines for every component	No Change	No change to GRM-01.1.
GRM-01.2	Do you have the capability to continuously monitor and report the compliance	No Change	No change to GRM-01.2.
GRM-02.1	Does your organization's risk assessments take into account awareness of data	New Question	New question added to GRM-02.1.
GRM-02.2	Do you conduct risk assessments associated with data governance	No Change	No change to GRM-02.2.
GRM-03.1	Are your technical, business, and executive managers responsible for	No Change	No change to GRM-03.1.
GRM-04.1	Do you provide tenants with documentation describing your Information	No Change	No change to GRM-04.1.
GRM-04.2	Do you review your Information Security Management Program (ISMP) at least	No Change	No change to GRM-04.2.
GRM-05.1	Do executive and line management take formal action to support information	New Question	New question added to GRM-05.1.
GRM-06.1	Are your information security policies and procedures made available to all	New Question	New question added to GRM-06.1.
GRM-06.2	Are information security policies authorized by the organization's business	New Question	New question added to GRM-06.2.
GRM-06.3	Do you have agreements to ensure your providers adhere to your information	No Change	No change to GRM-06.3.
GRM-06.4	Can you provide evidence of due diligence mapping of your controls,	No Change	No change to GRM-06.4.

GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations	No Change	No change to GRM-06.5.
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have	No Change	No change to GRM-07.1.
GRM-07.2	Are employees made aware of what actions could be taken in the event of a	No Change	No change to GRM-07.2.
GRM-08.1	Do risk assessment results include updates to security policies, procedures,	No Change	No change to GRM-08.1.
GRM-09.1	Do you notify your tenants when you make material changes to your	No Change	No change to GRM-09.1.
GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security	No Change	No change to GRM-09.2.
GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and	No Change	No change to GRM-10.1.
GRM-10.2	Is the likelihood and impact associated with inherent and residual risk	Edited	Edits have been made to GRM-10.2. Risk category
GRM-11.1	Do you have a documented, organization-wide program in place to manage	No Change	No change to GRM-11.1.
GRM-11.2	Do you make available documentation of your organization-wide risk	No Change	No change to GRM-11.2.
HRS-01.1	Upon termination of contract or business relationship, are employees and	New Question	New question added to HRS-01.1.
HRS-01.2	Do you have asset return procedures outlining how assets should be returned	New Question	New question added to HRS-01.2.
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all	No Change	No change to HRS-02.1.
HRS-03.1	Do your employment agreements incorporate provisions and/or terms in	New Question	New question added to HRS-03.1.
HRS-03.2	Do you require that employment agreements are signed by newly hired or on-	New Question	New question added to HRS-03.2.
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern	No Change	No change to HRS-04.1.
HRS-04.2	Do the above procedures and guidelines account for timely revocation of	No Change	No change to HRS-04.2.
HRS-05.1	Are policies and procedures established and measures implemented to strictly	No Change	No change to HRS-05.1.
HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting	No Change	No change to HRS-06.1.
HRS-07.1	Do you provide tenants with a role definition document clarifying your	No Change	No change to HRS-07.1.
HRS-08.1	Do you have policies and procedures in place to define allowances and	New Question	New question added to HRS-08.1.
HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications	New Question	New question added to HRS-08.2.
HRS-09.1	Do you provide a formal, role-based, security awareness training program for	No Change	No change to HRS-09.1.
HRS-09.2	Do you specifically train your employees regarding their specific role and the	Shifted	HRS-03.1 has been shifted to HRS-09.2.
HRS-09.3	Do you document employee acknowledgment of training they have	Shifted	HRS-03.2 has been shifted to HRS-09.3
HRS-09.4	Is successful and timed completion of the training program(s) considered a	Shifted	HRS-03.4 has been shifted to HRS-09.4.
HRS-09.5	Are personnel trained and provided with awareness programs at least once a	Shifted	HRS-03.5 has been shifted to HRS-09.5.
HRS-09.6	Are administrators and data stewards properly educated on their legal	No Change	No change to HRS-09.6.
HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and	Edited	Edits have been made to HRS-10.1. Language has been
HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and	Edited	Edits have been made to HRS-10.2. Language has been
HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is	Edited	Edits have been made to HRS-10.3. Language has been
HRS-11.1	Are all computers and laptops configured such that there is lockout screen	New Question	New question added to HRS-11.1.
HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do	New Question	New question added to HRS-11.2.
IAM-01.1	Do you restrict, log, and monitor access to your information security	No Change	No change to IAM-01.1.
IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to	No Change	No change to IAM-01.2.
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that	No Change	No change to IAM-02.1.

IAM-02.2	Do you have policies, procedures and technical measures in place to ensure	New Question	New question added to IAM-02.2.
IAM-02.3	Do you have procedures and technical measures in place for user account	New Question	New question added to IAM-02.3.
IAM-02.4	Do you have procedures and technical measures in place for data access	New Question	New question added to IAM-02.4.
IAM-02.5	Do you enforce data access permissions based on the rules of Authentication,	New Question	New question added to IAM-02.5.
IAM-02.6	Do your policies and procedures incorporate security controls for establishing	New Question	New question added to IAM-02.6.
IAM-02.7	Do you provide metrics to track the speed with which you are able to remove	No Change	No change to IAM-02.7.
IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized	New Question	New question added to IAM-03.1.
IAM-04.1	Do you manage and store the identity of all personnel who have access to the	No Change	No change to IAM-04.1.
IAM-04.2	Do you manage and store the user identity of all personnel who have network	No Change	No change to IAM-04.2.
IAM-05.1	Do you provide tenants with documentation on how you maintain segregation	No Change	No change to IAM-05.1.
IAM-06.1	Are controls in place to prevent unauthorized access to your application,	No Change	No change to IAM-06.1.
IAM-06.2	Are controls in place to prevent unauthorized access to tenant application,	No Change	No change to IAM-06.2.
IAM-07.1	Does your organization conduct third-party unauthorized access risk	New Question	New question added to IAM-07.1.
IAM-07.2	Are preventive, detective corrective compensating controls in place to	New Question	New question added to IAM-07.2.
IAM-08.1	Do you document how your grant, approve and enforce access restrictions to	New Question	New question added to IAM-08.1.
IAM-08.2	Based on the rules of least privilege, do you have policies and procedures	New Question	New question added to IAM-08.2.
IAM-08.3	Do you limit identities' replication only to users explicitly defined as business	New Question	New question added to IAM-08.3.
IAM-09.1	Does your management provision the authorization and restrictions for user	No Change	No change to IAM-09.1.
IAM-09.2	Do you provide upon the request of users with legitimate interest access (e.g.,	Edited	Edits have been made to IAM-09.2. Question has been
IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually)	Edited	Edits have been made to IAM-10.1. Unclear terms (e.g.
IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-	New Question	New question added to IAM-10.2.
IAM-10.3	Do you ensure that remediation actions for access violations follow user access	Edited	Edits have been made to IAM-10.3. Edited question to
IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if	Edited	Edits have been made to IAM-10.4. Unclear terms (e.g.
IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the	No Change	No change to IAM-11.1.
IAM-11.2	Is any change in user access status intended to include termination of	No Change	No change to IAM-11.2.
IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign	No Change	No change to IAM-12.1.
IAM-12.2	Do you use open standards to delegate authentication capabilities to your	No Change	No change to IAM-12.2.
IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-	No Change	No change to IAM-12.3.
IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce	No Change	No change to IAM-12.4.
IAM-12.5	Do you have an identity management system (enabling classification of data	No Change	No change to IAM-12.5.
IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g.,	No Change	No change to IAM-12.6.
IAM-12.7	Do you allow tenants to use third-party identity assurance services?	No Change	No change to IAM-12.7.
IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and	No Change	No change to IAM-12.8.
IAM-12.9	Do you allow tenants/customers to define password and account lockout	No Change	No change to IAM-12.9.
IAM-12.10	Do you support the ability to force password changes upon first logon?	No Change	No change to IAM-12.10.
IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been	No Change	No change to IAM-12.11.

IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g.	Edited	Edits have been made to IAM-13.1. Significantly' has been
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools	No Change	No change to IVS-01.1.
IVS-01.2	Is physical and logical user access to audit logs restricted to authorized	No Change	No change to IVS-01.2.
IVS-01.3	Can you provide evidence that due diligence mapping of regulations and	No Change	No change to IVS-01.3.
IVS-01.4	Are audit logs centrally stored and retained?	No Change	No change to IVS-01.4.
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with	No Change	No change to IVS-01.5.
IVS-02.1	Do you log and alert any changes made to virtual machine images regardless	No Change	No change to IVS-02.1.
IVS-02.2	Does the virtual machine management infrastructure include a tamper audit	Shifted	HRS-11.3 has been shifted to IVS-02.2.
IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent	No Change	No change to IVS-02.3.
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all	No Change	No change to IVS-03.1.
IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network,	No Change	No change to IVS-04.1.
IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the	No Change	No change to IVS-04.2.
IVS-04.3	Do your system capacity requirements take into account current, projected,	No Change	No change to IVS-04.3.
IVS-04.4	Is system performance monitored and tuned in order to continuously meet	No Change	No change to IVS-04.4.
IVS-05.1	Do security vulnerability assessment tools or services accommodate the	No Change	No change to IVS-05.1.
IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to	No Change	No change to IVS-06.1.
IVS-06.2	Do you regularly update network architecture diagrams that include data flows	No Change	No change to IVS-06.2.
IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity	No Change	No change to IVS-06.3.
IVS-06.4	Are all firewall access control lists documented with business justification?	No Change	No change to IVS-06.4.
IVS-07.1	Are operating systems hardened to provide only the necessary ports,	No Change	No change to IVS-07.1.
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate	No Change	No change to IVS-08.1.
IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create	No Change	No change to IVS-08.2.
IVS-08.3	Do you logically and physically segregate production and non-production	No Change	No change to IVS-08.3.
IVS-09.1	Are system and network environments protected by a firewall or virtual	No Change	No change to IVS-09.1.
IVS-09.2	Are system and network environments protected by a firewall or virtual	Edited	Edits have been made to IVS-09.2. Legislative' has been
IVS-09.3	Have you implemented the necessary measures for the appropriate isolation	New Question	New question added to IVS-09.3.
IVS-09.4	Do you have the ability to logically segment or encrypt customer data such	Shifted	AAC-03.1 has been shifted to IVS-09.4.
IVS-09.5	Are system and network environments protected by a firewall or virtual	No Change	No change to IVS-09.5.
IVS-10.1	Are secured and encrypted communication channels used when migrating	No Change	No change to IVS-10.1.
IVS-10.2	Do you use a network segregated from production-level networks when	No Change	No change to IVS-10.2.
IVS-11.1	Do you restrict personnel access to all hypervisor management functions or	No Change	No change to IVS-11.1.
IVS-12.1	Are policies and procedures established and mechanisms configured and	No Change	No change to IVS-12.1.
IVS-12.2	Are policies and procedures established and mechanisms implemented to	No Change	No change to IVS-12.2.
IVS-12.3	Are policies and procedures established and mechanisms implemented to	No Change	No change to IVS-12.3.
IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments	No Change	No change to IVS-13.1.
IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques	No Change	No change to IVS-13.2.

IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are	No Change	No change to IPY-01.1.
IPY-02.1	Is unstructured customer data available on request in an industry-standard	No Change	No change to IPY-02.1.
IPY-03.1	Do you provide policies and procedures (i.e. service level agreements)	No Change	No change to IPY-03.1.
IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be	Shifted	BCR-07.3 has been shifted to IPY-03.2.
IPY-03.3	Do you provide policies and procedures (i.e. service level agreements)	No Change	No change to IPY-03.3.
IPY-04.1	Is data import, data export, and service management be conducted over	Edited	Edits have been made to IPY-04.1. Mandatory
IPY-04.2	Do you provide consumers (tenants) with documentation detailing the	No Change	No change to IPY-04.2.
IPY-05.1	Do you use an industry-recognized virtualization platform and standard	No Change	No change to IPY-05.1.
IPY-05.2	If using virtual infrastructure, are machine images made available to the	Shifted	BCR-07.4 has been shifted to IPY-05.2.
IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and	No Change	No change to IPY-05.3.
MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your	No Change	No change to MOS-01.1.
MOS-02.1	Do you document and make available lists of approved application stores for	No Change	No change to MOS-02.1.
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only	No Change	No change to MOS-03.1.
MOS-04.1	Does your BYOD policy and training clearly state which applications and	No Change	No change to MOS-04.1.
MOS-05.1	Do you have a documented mobile device policy in your employee training	No Change	No change to MOS-05.1.
MOS-06.1	Do you have a documented list of pre-approved cloud based services that are	No Change	No change to MOS-06.1.
MOS-07.1	Do you have a documented application validation process for testing device,	No Change	No change to MOS-07.1.
MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility	No Change	No change to MOS-08.1.
MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing	No Change	No change to MOS-09.1.
MOS-10.1	Do you have a centralized mobile device management solution deployed to all	No Change	No change to MOS-10.1.
MOS-11.1	Does your mobile device policy require the use of encryption for either the	No Change	No change to MOS-11.1.
MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security	No Change	No change to MOS-12.1.
MOS-12.2	Do you have detective and preventative controls on the device or via a	No Change	No change to MOS-12.2.
MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements	No Change	No change to MOS-13.1.
MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-	New Question	New question added to MOS-13.2.
MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen	No Change	No change to MOS-14.1.
MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels,	No Change	No change to MOS-15.1.
MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or	No Change	No change to MOS-16.1.
MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	No Change	No change to MOS-16.2.
MOS-16.3	Do your password policies prohibit the changing of authentication	No Change	No change to MOS-16.3.
MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified	No Change	No change to MOS-17.1.
MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of	No Change	No change to MOS-17.2.
MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software	No Change	No change to MOS-17.3.
MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-	No Change	No change to MOS-18.1.
MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-	No Change	No change to MOS-18.2.
MOS-19.1	Do your mobile devices have the latest available security-related patches	No Change	No change to MOS-19.1.

MOS-19.2	Do your mobile devices allow for remote validation to download the latest	No Change	No change to MOS-19.2.
MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or	No Change	No change to MOS-20.1.
MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a	No Change	No change to MOS-20.2.
SEF-01.1	Do you maintain liaisons and points of contact with local authorities in	No Change	No change to SEF-01.1.
SEF-02.1	Do you have a documented security incident response plan?	No Change	No change to SEF-02.1.
SEF-02.2	Do you integrate customized tenant requirements into your security incident	No Change	No change to SEF-02.2.
SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs.	No Change	No change to SEF-02.3.
SEF-02.4	Have you tested your security incident response plans in the last year?	No Change	No change to SEF-02.4.
SEF-03.1	Are workforce personnel and external business relationships adequately	New Question	New question added to SEF-03.1.
SEF-03.2	Do you have predefined communication channels for workforce personnel and	New Question	New question added to SEF-03.2.
SEF-04.1	Does your incident response plan comply with industry standards for legally	No Change	No change to SEF-04.1.
SEF-04.2	Does your incident response capability include the use of legally admissible	No Change	No change to SEF-04.2.
SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific	No Change	No change to SEF-04.3.
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in	No Change	No change to SEF-04.4.
SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all	No Change	No change to SEF-05.1.
SEF-05.2	Will you share statistical information for security incident data with your	No Change	No change to SEF-05.2.
STA-01.1	Do you inspect and account for data quality errors and associated risks, and	No Change	No change to STA-01.1.
STA-01.2	Do you design and implement controls to mitigate and contain data security	No Change	No change to STA-01.2.
STA-02.1	Do you make security incident information available to all affected customers	No Change	No change to STA-02.1.
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud	No Change	No change to STA-03.1.
STA-03.2	Do you provide tenants with capacity planning and use reports?	No Change	No change to STA-03.2.
STA-04.1	Do you perform annual internal assessments of conformance and	No Change	No change to STA-04.1.
STA-05.1	Do you select and monitor outsourced providers in compliance with laws in	No Change	No change to STA-05.1.
STA-05.2	Do you select and monitor outsourced providers to ensure that they are in	New Question	New question added to STA-05.2.
STA-05.3	Does legal counsel review all third-party agreements?	No Change	No change to STA-05.3.
STA-05.4	Do third-party agreements include provision for the security and protection of	No Change	No change to STA-05.4.
STA-05.5	Do you have the capability to recover data for a specific customer in the case	Shifted	AAC-03.2 has been shifted to STA-05.5.
STA-05.6	Do you have the capability to restrict the storage of customer data to specific	Shifted	AAC-03.3 has been shifted to STA-05.6.
STA-05.7	Can you provide the physical location/geography of storage of a tenant’s data	Shifted	DSI-01.4 has been shifted to STA-05.7.
STA-05.8	Can you provide the physical location/geography of storage of a tenant's data	Shifted	DSI-01.5 has been shifted to STA-05.8.
STA-05.9	Do you allow tenants to define acceptable geographical locations for data	Shifted	DSI-01.7 has been shifted to STA-05.9.
STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants	Shifted	HRS-01.1 has been shifted to STA-05.10.
STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via	Shifted	HRS-08.3 has been shifted to STA-05.11.
STA-05.12	Do you provide the client with a list and copies of all subprocessing	No Change	No change to STA-05.12.
STA-06.1	Do you review the risk management and governanced processes of partners to	No Change	No change to STA-06.1.
STA-07.1	Are policies and procedures established, and supporting business processes	No Change	No change to STA-07.1.

STA-07.2	Do you have the ability to measure and address non-conformance of	No Change	No change to STA-07.2.
STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from	No Change	No change to STA-07.3.
STA-07.4	Do you provide tenants with ongoing visibility and reporting of your	Shifted	BCR-09.1 has been shifted to STA-07.4.
STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.)	Shifted	BCR-09.2 has been shifted to STA-07.5.
STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA	Shifted	BCR-09.3 has been shifted to STA-07.6.
STA-07.7	Do your data management policies and procedures address tenant and service	Shifted	HRS-11.1 has been shifted to STA-07.7.
STA-07.8	Do you review all service level agreements at least annually?	New Question	New question added to STA-07.8.
STA-08.1	Do you assure reasonable information security across your information supply	No Change	No change to STA-08.1.
STA-08.2	Does your annual review include all partners/third-party providers upon which	No Change	No change to STA-08.2.
STA-09.1	Do you mandate annual information security reviews and audits of your third	New Question	New question added to STA-09.1.
STA-09.2	Do you have external third party services conduct vulnerability scans and	No Change	No change to STA-09.2.
TVM-01.1	Do you have anti-malware programs that support or connect to your cloud	No Change	No change to TVM-01.1.
TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or	No Change	No change to TVM-01.2.
TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by	No Change	No change to TVM-02.1.
TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by	No Change	No change to TVM-02.2.
TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as	No Change	No change to TVM-02.3.
TVM-02.4	Will you make the results of vulnerability scans available to tenants at their	No Change	No change to TVM-02.4.
TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your	No Change	No change to TVM-02.5.
TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified	New Question	New question added to TVM-02.6.
TVM-03.1	Is mobile code authorized before its installation and use, and the code	No Change	No change to TVM-03.1.
TVM-03.2	Is all unauthorized mobile code prevented from executing?	No Change	No change to TVM-03.2.