Section Heading	Control Heading	Original ID
Application & Interface Security	**Application Security**	AIS-01.1
		AIS-01.2
		AIS-01.3
		AIS-01.4
		AIS-01.5
	Customer Access Requirements	AIS-02.1
		AIS- 02.2
	Data Integrity	AIS-03.1
		AIS-03.2
	Data Security / Integrity	AIS-04.1
Audit Assurance & Compliance	**Audit Planning**	AAC-01.1
		AAC-01.2
	Independent Audits	AAC-02.1
		AAC-02.2
		AAC-02.3
		AAC-02.4

		AAC-02.5
		AAC-02.6
		AAC-02.7
	Information System Regulatory Mapping	AAC-03.1
Business Continuity Management & Operational Resilience	**Business Continuity Planning**	BCR-01.1
		BCR-01.2
		BCR-01.3
		BCR-01.4
		BCR-01.5
		BCR-01.6
		BCR-01.7
	Business Continuity Testing	BCR-02.1
	Power / Telecommunications	BCR-03.1
		BCR-03.2
	Documentation	BCR-04.1
	Environmental Risks	BCR-05.1
	Equipment Location	BCR-06.1
	Equipment Maintenance	BCR-07.1
		BCR-07.2

	Equipment Power Failures	BCR-08.1
	Impact Analysis	BCR-09.1
		BCR-09.2
	Policy	BCR-10.1
	Retention Policy	BCR-11.1
		BCR-11.2
		BCR-11.3
		BCR-11.4
		BCR-11.5
		BCR-11.6
		BCR-11.7
Change Control & Configuration Management	**New Development / Acquisition**	CCC-01.1
	Outsourced Development	CCC-02.1
		CCC-02.2
	Quality Testing	CCC-03.1
		CCC-03.2
		CCC-03.3

		CCC-03.4
		CCC-03.5
		CCC-03.6
	Unauthorized Software Installations	CCC-04.1
	Production Changes	CCC-05.1
		CCC-05.2
		CCC-0.5.3
Data Security & Information Lifecycle Management	**Classification**	DSI-01.1
		DSI-01.2
	Data Inventory / Flows	DSI-02.1
		DSI-02.2
	E-commerce Transactions	DSI-03.1
		DSI-03.2
	Handling / Labeling / Security Policy	DSI-04.1
		DSI-04.2
		DSI-04.3

	Nonproduction Data	DSI-05.1
	Ownership / Stewardship	DSI-06.1
	Secure Disposal	DSI-07.1
		DSI-07.2
Datacenter Security	**Asset Management**	DCS-01.1
		DCS-01.2
	Controlled Access Points	DCS-02.1
	Equipment Identification	DCS-03.1
		DCS-03.2
	Offsite Authorization	DCS-04.1
	Offsite Equipment	DCS-05.1
	Policy	DCS-06.1
		DCS-06.2
	Secure Area Authorization	DCS-07.1
	Unauthorized Persons Entry	DCS-08.1
	User Access	DCS-09.1

Encryption & Key Management	**Entitlement**	EKM-01.1
	Key Generation	EKM-02.1
		EKM-02.2
		EKM-02.3
		EKM-02.4
		EKM-02.5
	Encryption	EKM-03.1
		EKM-03.2
		EKM-03.3
	Storage and Access	EKM-04.1
		EKM-04.2
		EKM-04.3
		EKM-04.4
Governance and Risk Management	**Baseline Requirements**	GRM-01.1
		GRM-01.2
	Risk Assessments	GRM-02.1
		GRM-02.2
	Management Oversight	GRM-03.1
	Management Program	GRM-04.1

	GRM-04.2
Management Support / Involvement	GRM-05.1
Policy	GRM-06.1
	GRM-06.2
	GRM-06.3
	GRM-06.4
	GRM-06.5
Policy Enforcement	GRM-07.1
	GRM-07.2
Business / Policy Change Impacts	GRM-08.1
Policy Reviews	GRM-09.1
	GRM-09.2
Assessments	GRM-10.1
	GRM-10.2
Program	GRM-11.1

		GRM-11.2
Human Resources	**Asset Returns**	HRS-01.1
		HRS-01.2
	Background Screening	HRS-02.1
	Employment Agreements	HRS-03.1
		HRS-03.2
	Employment Termination	HRS-04.1
		HRS-04.2
	Portable / Mobile Devices	HRS-05.1
	Non-Disclosure Agreements	HRS-06.1
	Roles / Responsibilities	HRS-07.1
	Acceptable Use	HRS-08.1
		HRS-08.2

	Training / Awareness	HRS-09.1
		HRS-09.2
		HRS-09.3
		HRS-09.4
		HRS-09.5
		HRS-09.6
	User Responsibility	HRS-10.1
		HRS-10.2
		HRS-10.3
	Workspace	HRS-11.1
		HRS-11.2
Identity & Access Management	**Audit Tools Access**	IAM-01.1
		IAM-01.2
	User Access Policy	IAM-02.1
		IAM-02.2
		IAM-02.3

	IAM-02.4
	IAM-02.5
	IAM-02.6
	IAM-02.7
Diagnostic / Configuration Ports Access	IAM-03.1
Policies and Procedures	IAM-04.1
	IAM-04.2
Segregation of Duties	IAM-05.1
Source Code Access Restriction	IAM-06.1
	IAM-06.2
Third Party Access	IAM-07.1
	IAM-07.2
User Access Restriction / Authorization	IAM-08.1
	IAM-08.2
	IAM-08.3
User Access Authorization	IAM-09.1

	IAM-09.2
User Access Reviews	IAM-10.1
	IAM-10.2
	IAM-10.3
	IAM-10.4
User Access Revocation	IAM-11.1
	IAM-11.2
User ID Credentials	IAM-12.1
	IAM-12.2
	IAM-12.3
	IAM-12.4
	IAM-12.5
	IAM-12.6
	IAM-12.7
	IAM-12.8
	IAM-12.9

		IAM-12.10
		IAM-12.11
	Utility Programs Access	IAM-13.1
Infrastructure & Virtualization Security	**Audit Logging / Intrusion Detection**	IVS-01.1
		IVS-01.2
		IVS-01.3
		IVS-01.4
		IVS-01.5
	Change Detection	IVS-02.1
		IVS-02.2
		IVS-02.3
	Clock Synchronization	IVS-03.1
	Capacity / Resource Planning	IVS-04.1
		IVS-04.2
		IVS-04.3
		IVS-04.4
	Management - Vulnerability Management	IVS-05.1

Network Security	IVS-06.1
	IVS-06.2
	IVS-06.3
	IVS-06.4
OS Hardening and Base Controls	IVS-07.1
Production / Non-Production Environments	IVS-08.1
	IVS-08.2
	IVS-08.3
Segmentation	IVS-09.1
	IVS-09.2
	IVS-09.3
	IVS-09.4
	IVS-09.5
VM Security - Data Protection	IVS-10.1
	IVS-10.2

	VMM Security - Hypervisor Hardening	IVS-11.1
	Wireless Security	IVS-12.1
		IVS-12.2
		IVS-12.3
	Network Architecture	IVS-13.1
		IVS-13.2
Interoperability & Portability	**APIs**	IPY-01.1
	Data Request	IPY-02.1
	Policy & Legal	IPY-03.1
		IPY-03.2
		IPY-03.3
	Standardized Network Protocols	IPY-04.1

	Virtualization	IPY-04.2
		IPY-05.1
		IPY-05.2
		IPY-05.3
Mobile Security	**Anti-Malware**	MOS-01.1
	Application Stores	MOS-02.1
	Approved Applications	MOS-03.1
	Approved Software for BYOD	MOS-04.1
	Awareness and Training	MOS-05.1
	Cloud Based Services	MOS-06.1
	Compatibility	MOS-07.1
	Device Eligibility	MOS-08.1
	Device Inventory	MOS-09.1
	Device Management	MOS-10.1
	Encryption	MOS-11.1

Jailbreaking and Rooting	MOS-12.1
	MOS-12.2
Legal	MOS-13.1
	MOS-13.2
Lockout Screen	MOS-14.1
Operating Systems	MOS-15.1
Passwords	MOS-16.1
	MOS-16.2
	MOS-16.3
Policy	MOS-17.1
	MOS-17.2
	MOS-17.3
Remote Wipe	MOS-18.1
	MOS-18.2
Security Patches	MOS-19.1
	MOS-19.2
Users	MOS-20.1

		MOS-20.2
Security Incident Management, E-Discovery, & Cloud Forensics	**Contact / Authority Maintenance**	SEF-01.1
	Incident Management	SEF-02.1
		SEF-02.2
		SEF-02.3
		SEF-02.4
	Incident Reporting	SEF-03.1
		SEF-03.2
	Incident Response Legal Preparation	SEF-04.1
		SEF-04.2
		SEF-04.3
		SEF-04.4
	Incident Response Metrics	SEF-05.1
		SEF-05.2
Supply Chain Management, Transparency, and Accountability	**Data Quality and Integrity**	STA-01.1
		STA-01.2

Incident Reporting	STA-02.1
Network / Infrastructure Services	STA-03.1
	STA-03.2
Provider Internal Assessments	STA-04.1
Third Party Agreements	STA-05.1
	STA-05.2
	STA-05.3
	STA-05.4
	STA-05.5
	STA-05.6
	STA-05.7
	STA-05.8
	STA-05.9
	STA-05.10
	STA-05.11
	STA-05.12
Supply Chain Governance Reviews	STA-06.1
Supply Chain Metrics	STA-07.1

		STA-07.2
		STA-07.3
		STA-07.4
		STA-07.5
		STA-07.6
		STA-07.7
		STA-07.8
	Third Party Assessment	STA-08.1
		STA-08.2
	Third Party Audits	STA-09.1
		STA-09.2
Threat and Vulnerability Management	**Antivirus / Malicious Software**	TVM-01.1
		TVM-01.2
	Vulnerability / Patch Management	TVM-02.1
		TVM-02.2
		TVM-02.3
		TVM-02.4
		TVM-02.5

		TVM-02.6
	Mobile Code	TVM-03.1
		TVM-03.2

Question Text	Answer
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)?	Yes
Do you use an automated source code analysis tool to detect security defects in code prior to production?	Yes
Do you use manual source-code analysis to detect security defects in code prior to production?	Yes
Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	No
(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes
Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	Yes
Are all requirements and trust levels for customers' access defined and documented?	Yes
Does your data management policies and procedures require audits to verify data input and output integrity routines?	Yes
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?	Yes
Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	No
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?	Yes
Does your audit program take into account effectiveness of implementation of security operations?	Yes
Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Yes
Do you conduct network penetration tests of your cloud service infrastructure at least annually?	Yes
Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes
Do you conduct internal audits at least annually?	Yes

Do you conduct independent audits at least annually?	Yes
Are the results of the penetration tests available to tenants at their request?	Yes
Are the results of internal and external audits available to tenants at their request?	Yes
Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes
Does your organization have a plan or framework for business continuity management or disaster recovery management?	Yes
Do you have more than one provider for each service you depend on?	No
Do you provide a disaster recovery capability?	Yes
Do you monitor service continuity with upstream providers in the event of provider failure?	Yes
Do you provide access to operational redundancy reports, including the services you rely on?	No
Do you provide a tenant-triggered failover option?	No
Do you share your business continuity and redundancy plans with your tenants?	Yes
Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes
Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	Not Applicable
Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	Not Applicable
Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Yes
Is physical damage anticipated and are countermeasures included in the design of physical protections?	Yes
Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	No
Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	Not Applicable
Do you have an equipment and datacenter maintenance routine or plan?	Not Applicable

Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Yes
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) ?	No
Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	Yes
Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes
Do you have technical capabilities to enforce tenant data retention policies?	Yes
Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	Yes
Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes
If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	Yes
If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	No
Does your cloud solution include software/provider independent restore and recovery capabilities?	Yes
Do you test your backup or redundancy mechanisms at least annually?	Yes
Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Yes
Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	Yes
Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	Yes
Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	Yes
Is documentation describing known issues with certain products/services available?	No
Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Yes

Do you have controls in place to ensure that standards of quality are being met for all software development?	Yes
Do you have controls in place to detect source code security defects for any outsourced software development activities?	Not Applicable
Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	Yes
Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes
Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	Yes
Do you have policies and procedures established for managing risks with respect to change management in production environments?	Yes
Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	Yes
Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	No
Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	Yes
Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	Yes
Can you ensure that data does not migrate beyond a defined geographical residency?	Yes
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)?	Yes
Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Yes
Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	Yes
Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	No
Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Yes

Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes
Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	Yes
Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	Yes
Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Yes
Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	Yes
Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	Yes
Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	Yes
Do you have a capability to use system geographic location as an authentication factor?	Yes
Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	Yes
Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	Yes
Can you provide tenants with your asset management policies and procedures?	No
Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	Yes
Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	Yes
Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	Yes
Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Yes
Do you restrict physical access to information assets and functions by users and support personnel?	Yes

Do you have key management policies binding keys to identifiable owners?	Yes
Do you have a capability to allow creation of unique encryption keys per tenant?	Not Applicable
Do you have a capability to manage encryption keys on behalf of tenants?	Not Applicable
Do you maintain key management procedures?	Yes
Do you have documented ownership for each stage of the lifecycle of encryption keys?	Not Applicable
Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	Yes
Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes
Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Yes
Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	Yes
Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	Yes
Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	Yes
Do you store encryption keys in the cloud?	Yes
Do you have separate key management and key usage duties?	Yes
Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Yes
Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Yes
Does your organization's risk assessments take into account awareness of data residency, lega and statutory requirements for retention periods and data protection and classification?	Yes
Do you conduct risk assessments associated with data governance requirements at least once a year?	Yes
Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	Yes
Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	Yes

Do you review your Information Security Management Program (ISMP) at least once a year?	Yes
Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	Yes
Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	Yes
Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	Yes
Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Yes
Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	Yes
Do you disclose which controls, standards, certifications, and/or regulations you comply with?	Yes
Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes
Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes
Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	Yes
Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Yes
Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes
Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Yes
Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	Yes
Do you have a documented, organization-wide program in place to manage risk?	Yes

Do you make available documentation of your organization-wide risk management program?	Yes
Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	Yes
Do you have asset return procedures outlining how assets should be returned within an established period?	Yes
Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	Yes
Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	Yes
Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	Yes
Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	Yes
Do the above procedures and guidelines account for timely revocation of access and return of assets?	Yes
Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization’s facilities)?	No
Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	Yes
Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	No
Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	Yes
Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	Yes

Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	Yes
Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	Yes
Do you document employee acknowledgment of training they have completed?	Yes
Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	Yes
Are personnel trained and provided with awareness programs at least once a year?	Yes
Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	Yes
Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	Yes
Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	Yes
Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	Yes
Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	Yes
Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	Yes
Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	Yes
Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	Yes
Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Yes
Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	Yes
Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	Yes

Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	Yes
Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	Yes
Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	Yes
Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	No
Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	Yes
Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Yes
Do you manage and store the user identity of all personnel who have network access, including their level of access?	Yes
Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Yes
Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	Yes
Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	Yes
Does your organization conduct third-party unauthorized access risk assessments?	Yes
Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access?	Yes
Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	Yes
Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	Yes
Do you limit identities' replication only to users explicitly defined as business necessary?	Yes
Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	Yes

Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Yes
Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	Yes
Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	Yes
Do you ensure that remediation actions for access violations follow user access policies?	Yes
Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	Yes
Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	Yes
Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes
Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Yes
Do you use open standards to delegate authentication capabilities to your tenants?	Yes
Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	Yes
Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	No
Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	Yes
Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	Yes
Do you allow tenants to use third-party identity assurance services?	Yes
Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	Yes
Do you allow tenants/customers to define password and account lockout policies for their accounts?	Yes

Do you support the ability to force password changes upon first logon?	Yes
Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	Yes
Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	Yes
Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	Yes
Is physical and logical user access to audit logs restricted to authorized personnel?	Yes
Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	Yes
Are audit logs centrally stored and retained?	Yes
Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Yes
Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	Yes
Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	Yes
Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	Not Applicable
Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Yes
Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Yes
Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	Yes
Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	Yes
Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	Yes
Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	Yes

For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	Not Applicable
Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Yes
Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	Yes
Are all firewall access control lists documented with business justification?	Yes
Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	Yes
For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Yes
For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	Not Applicable
Do you logically and physically segregate production and non-production environments?	Yes
Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	Yes
Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	Yes
Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	Yes
Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Yes
Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	Yes
Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	Yes
Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	Yes

Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Yes
Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Yes
Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	Yes
Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Yes
Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	No
Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	Yes
Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Not Applicable
Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	Yes
Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Not Applicable
If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	No
Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Yes
Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	Yes

Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	Yes
Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	Yes
If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	No
Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	Yes
Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	Yes
Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	No
Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	No
Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	No
Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	Yes
Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	Yes
Do you have a documented application validation process for testing device, operating system, and application compatibility issues?	Yes
Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	Yes
Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	No
Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	No
Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	Yes

Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	Yes
Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	Yes
Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	No
Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?	Not Applicable
Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	No
Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	No
Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	Yes
Are your password policies enforced through technical controls (i.e. MDM)?	Yes
Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	No
Do you have a policy that requires BYOD users to perform backups of specified corporate data?	Yes
Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	No
Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	Yes
Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	No
Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	Yes
Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	Yes
Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	Yes
Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	No

Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	No
Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Yes
Do you have a documented security incident response plan?	Yes
Do you integrate customized tenant requirements into your security incident response plans?	No
Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	No
Have you tested your security incident response plans in the last year?	Yes
Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	Yes
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?	Yes
Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Yes
Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Yes
Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	Yes
Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes
Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	Yes
Will you share statistical information for security incident data with your tenants upon request?	No
Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	No
Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	No

Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	Yes
Do you collect capacity and use data for all relevant components of your cloud service offering?	Yes
Do you provide tenants with capacity planning and use reports?	No
Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	Yes
Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	Yes
Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	Yes
Does legal counsel review all third-party agreements?	Yes
Do third-party agreements include provision for the security and protection of information and assets?	Yes
Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Yes
Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	Yes
Can you provide the physical location/geography of storage of a tenant’s data upon request?	Yes
Can you provide the physical location/geography of storage of a tenant's data in advance?	Yes
Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	No
Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Yes
Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	No
Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	Yes
Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	Yes
Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	Yes

Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	No
Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Yes
Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Yes
Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	No
Do you provide customers with ongoing visibility and reporting of your SLA performance?	Yes
Do your data management policies and procedures address tenant and service level conflicts of interests?	Yes
Do you review all service level agreements at least annually?	Yes
Do you assure reasonable information security across your information supply chain by performing an annual review?	Yes
Does your annual review include all partners/third-party providers upon which your information supply chain depends?	Yes
Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	Yes
Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Yes
Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	Yes
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?	Yes
Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes
Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes
Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes
Will you make the results of vulnerability scans available to tenants at their request?	Yes
Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	Yes

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?	Yes
Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	Yes
Is all unauthorized mobile code prevented from executing?	Yes

Notes/Comment

UserTesting does not maintain its own datacenter; UserTesting relies on AWS for its datacenter.

UserTesting does not maintain its own datacenter; UserTesting relies on AWS for its datacenter.

UserTesting does not maintain its own datacenter; UserTesting relies on AWS for its datacenter.
UserTesting does not maintain its own datacenter; UserTesting relies on AWS for its datacenter.

Given the nature of UserTesting's services, we have chosen 24 hours as the company's RPO and RTO.

UserTesting does not outsource its software development activities.

UserTesting does not provide a cloud hosting service and does not have tenants.
UserTesting does not provide a cloud hosting service and does not have tenants.

UserTesting does not use encryption keys that have multi-stage lifecycles.

UserTesting does not send virtual images or machines to customers. We deploy them in our central hosting platform.

UserTesting does not provide IaaS.

UserTesting does not provide IaaS.

UserTesting does not provide customer-facing APIs.

UserTesting does not provide APIs.

UserTesting does not wipe BYO devices.