Section Heading	Control Heading	Original ID
Application & Interface Security	**Application Security**	AIS-01.2
		AIS-01.5
	Customer Access Requirements	AIS-02.1
	Data Integrity	AIS-03.1
Audit Assurance & Compliance	**Independent Audits**	AAC-02.1
		AAC-02.2
		AAC-02.3
	Information System Regulatory Mapping	AAC-03.1
Business Continuity Management & Operational Resilience	**Business Continuity Testing**	BCR-02.1
	Policy	BCR-10.1
	Retention Policy	BCR-11.1 BCR-11.3
		BCR-11.7
Change Control & Configuration Management	**Unauthorized Software Installations**	CCC-04.1
Data Security & Information Lifecycle Management	**E-commerce Transactions**	DSI-03.1
		DSI-03.2
	Nonproduction Data	DSI-05.1
	Secure Disposal	DSI-07.1
		DSI-07.2

Datacenter Security	**Asset Management**	DCS-01.2
	Controlled Access Points	DCS-02.1
	User Access	DCS-09.1
Encryption & Key Management	**Key Generation**	EKM-02.1
	Encryption	EKM-03.1
Governance and Risk Management	**Baseline Requirements**	GRM-01.1
	Policy	GRM-06.1
	Policy Enforcement	GRM-07.1
	Policy Reviews	GRM-09.1
		GRM-09.2
Human Resources	**Asset Returns**	HRS-01.1
	Background Screening	HRS-02.1
	Employment Agreements	HRS-03.1
	Employment Termination	HRS-04.1
	Training / Awareness	HRS-09.5
Identity & Access Management	**Audit Tools Access**	IAM-01.1
		IAM-01.2
	User Access Policy	IAM-02.1
	Policies and Procedures	IAM-04.1
	Source Code Access Restriction	IAM-06.1

		IAM-06.2
	User Access Restriction / Authorization	IAM-08.1
	User Access Reviews	IAM-10.1
	User Access Revocation	IAM-11.1
Infrastructure & Virtualization Security	**Audit Logging / Intrusion Detection**	IVS-01.1
		IVS-01.2
		IVS-01.5
	Clock Synchronization	IVS-03.1
	OS Hardening and Base Controls	IVS-07.1
	Production / Non-Production Environments	IVS-08.1
		IVS-08.3
	Segmentation	IVS-09.1
	VMM Security - Hypervisor Hardening	IVS-11.1
	Wireless Security	IVS-12.1
		IVS-12.2
		IVS-12.3

Interoperability & Portability	**APIs**	IPY-01.1
Mobile Security	**Approved Applications**	MOS-03.1
Security Incident Management, E-Discovery, & Cloud Forensics	**Incident Management**	SEF-02.1 SEF-02.4
	Incident Reporting	SEF-03.1 SEF-03.2
	Incident Response Legal Preparation	SEF-04.4
Supply Chain Management, Transparency, and Accountability	**Incident Reporting**	STA-02.1
	Network / Infrastructure Services	STA-03.1
	Third Party Agreements	STA-05.4 STA-05.5
	Supply Chain Metrics	STA-07.4
	Third Party Audits	STA-09.1
Threat and Vulnerability Management	**Antivirus / Malicious Software**	TVM-01.1
	Vulnerability / Patch Management	TVM-02.5
	Mobile Code	TVM-03.1

Question Text

Do you use an automated source code analysis tool to detect security defects in code prior to production?

(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?

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?

Does your data management policies and procedures require audits to verify data input and output integrity routines?

Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?

Do you conduct network penetration tests of your cloud service infrastructure at least annually?

Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?

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?

Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?

Are policies and procedures established and made available for all personnel to adequately support services operations' roles?

Do you have technical capabilities to enforce tenant data retention policies?

Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?

Do you test your backup or redundancy mechanisms at least annually?

Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?

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)?

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)?

Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?

Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?

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?

Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?
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?

Do you restrict physical access to information assets and functions by users and support personnel?

Do you have a capability to allow creation of unique encryption keys per tenant?
Do you encrypt tenant data at rest (on disk/storage) within your environment?

Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?

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)?
Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?
Do you notify your tenants when you make material changes to your information security and/or privacy policies?
Do you perform, at minimum, annual reviews to your privacy and security policies?

Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?
Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?
Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?
Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?
Are personnel trained and provided with awareness programs at least once a year?

Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?
Do you monitor and log privileged access (e.g., administrator level) to information security management systems?
Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?
Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?
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?

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?

Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?
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?
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?

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?
Is physical and logical user access to audit logs restricted to authorized personnel?
Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?
Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?
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?

For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?
Do you logically and physically segregate production and non-production environments?
Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?
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)?
Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?
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)?
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?

Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?

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?

Do you have a documented security incident response plan?

Have you tested your security incident response plans in the last year?

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?

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?

Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?

Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?

Do you collect capacity and use data for all relevant components of your cloud service offering?

Do third-party agreements include provision for the security and protection of information and assets?

Do you have the capability to recover data for a specific customer in the case of a failure or data loss?

Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?

Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?

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?

Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?

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?

Answer	Notes/Comment