

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Conse	nsus Asses	sment Answers	Notes
Application &	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be	Do you use industry standards (i.e. OWASP Software	Yes	No	Not Applicable	
Interface Security Application Security			designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web	Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?				
		AIS-01.2	applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use an automated source code analysis tool to	х			code quality tool su apposito docker
		AIS-01.3	regulatory compliance obligations.	detect security defects in code prior to production? Do you use manual source-code analysis to detect security	x			Merge request su GitLab
		AIS-01.4		defects in code prior to production? Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development	x			menge request so onco
		AIS-01.5		Lifecycle (SDLC) security? (SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment	х			
Application &	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and	to production? Are all identified security, contractual, and regulatory	х			
Interface Security Customer Access Requirements		AIS- 02.2	information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems? Are all requirements and trust levels for customers' access	x			
Application &	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation	defined and documented? Does your data management policies and procedures	x			
Interface Security Data Integrity		AIS-03.2	and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	require audits to verify data input and output integrity. Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing		x		
Application &	AIS-04	AIS-04.1	Policies and procedures shall be established and	errors or corruption of data?	x			
Interface Security Data Security / Integrity			maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to country improper disclosure, alteraction, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?				
Audit Assurance & Compliance	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on	Do you develop and maintain an agreed upon audit plan (e.g.,		х		
Audit Planning		AAC-01.2	reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	х			
				Does your audit program take into account effectiveness of implementation of security operations?				
Audit Assurance & Compliance Independent Audits	AAC-02	AAC-02.1 AAC-02.2	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards,	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	x			VA/PT 2019 - Revalidation
		AAC-02.3	procedures, and compliance obligations.	service infrastructure at least annually? Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best	х			VA/PT 2019 - Revalidation 2020
		AAC-02.4		practices and guidance? Do you conduct internal audits at least annually?	x			pianificazione controlli
		AAC-02.5 AAC-02.6	-	Do you conduct independent audits at least annually? Are the results of the penetration tests available to tenants	X	x		pianificazione controlli documentazione tecnica
Audit Assurance &	440.03	AAC-02.7	O	मां है trie results जे internal and external addits available to bo you have a program in place triat includes the ability to	v	х		documentazione tecnica
Business Continuity	AAC-03 BCR-01	AAC-03.1 BCR-01.1	Organizations shall create and maintain a control A consistent unified framework for business continuity	Does your organization have a plan or framework for business	x			Service Provider
Management & Operational		BCR-01.2	planning and plan development shall be established, documented, and adopted to ensure all business continuity	continuity management or disaster recovery management? Do you have more than one provider for each service you depend on?		х		
Resilience Business Continuity		BCR-01.3	plans are consistent in addressing priorities for testing, maintenance, and information security requirements.	Do you provide a disaster recovery capability?	x			
Planning		BCR-01.4	Requirements for business continuity plans include the following:	Do you monitor service continuity with upstream providers in the event of provider failure?	х			
		BCR-01.5	Defined purpose and scope, aligned with relevant dependencies	Do you provide access to operational redundancy reports, including the services you rely on?	x			
		BCR-01.6	Accessible to and understood by those who will use	Do you provide a tenant-triggered failover option?	x			
		BCR-01.7	them Owned by a named person(s) who is responsible for their review, update, and approval Defined lines of communication, roles, and responsibilities	Do you share your business continuity and redundancy plans with your tenants?		x		documentazione tecnica interna
Business Continuity	BCR-02	BCR-02.1	Business continuity and security incident response plans	Are pusiness continuity pians subject to testing at pianned boes your organization acmere to any international or industry	х			
Business Continuity Management &	BCR-03	BCR-03.1 BCR-03.2	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls,		x			Service Provider
Operational Resilience Power / Telecommunications			telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for contuinal effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed	Has your organization implemented environmental controls, fail- over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?				
Business Continuity	BCR-04	BCR-04.1	with automated fail-over or other redundancies in the Information system documentation (e.g., administrator	Are information system documents (e.g., administrator and	x			solo a persone qualificate,
Business Continuity Business Continuity	BCR-05 BCR-06	BCR-05.1 BCR-06.1	Physical protection against damage from natural causes To reduce the risks from environmental threats, hazards,	Are any or your data centers located in places that have a		x	х	IAAS
Business Continuity	BCR-07	BCR-07.1	Policies and procedures shall be established, and	bio'you nave an equipment and catacenter mantenance			х	IAAS
Management & Business Continuity	BCR-08	BCR-07.2 BCR-08.1	supporting business processes and technical measures Protection measures shall be put into place to react to	Are security mechanisms and redundancies implemented to			x	IAAS IAAS
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: i Identify critical products and services I Identify all dependencies, including processes, applications, business partners, and third party service	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	providers Understand threats to critical products and services Understand threats resulting from planned or unplanned disruptions and how these vary over time Establish the maximum tollerable period for disruption Establish provides for recovery Establish recovery time abject these for segmenting of	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?		х		
Business Continuity Business Continuity	BCR-10 BCR-11	BCR-10.1 BCR-11.1	Policies and procedures shall be established, and Policies and procedures shall be established, and	Are policies and procedures established and made available by you have technical capabilities to emorce tenant data	X			
Management &		BCR-11.2	supporting business processes and technical measures	trò yoù nave documented poucies and procedures have your timpier themeoutack up or trectover y in the mains in the		х		
Operational Resilience		BCR-11.3 BCR-11.4	implemented, for defining and adhering to the retention period of any critical asset as per established policies and	ir using virtual init ascructure, does your cloud solution ir using virtual init ascructure, or you provibe renams with a	X			
Retention Policy		BCR-11.5 BCR-11.6	procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery	provider solution in the class solution in t	X			
Change Control &	CCC-01	BCR-11.7 CCC-01.1	measures shall be incorporated as part of business Policies and procedures shall be established, and	Are policies and procedures established for management	x x			Pianificazione dei controlli - Processo di progettazione
Change Control & Configuration	CCC-02	CCC-02.1 CCC-02.2	External business partners shall adhere to the same policies and procedures for change management, release,	Are policies and procedures for change management, release, Are policies and procedures adequately enforced to ensure	х	x		
Change Control &	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control	ud you have a derined quality change cohror and resting	х			Non esiste attualmente
Configuration Management		CCC-03.2 CCC-03.3	and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which	Are there'poncies and 'procedures in place to triage and	x	X		Ticketing, Gitlab issue
Quality Testing		CCC-03.4	focus on system availability, confidentiality, and integrity	อง you nave controis in place to ensure that Standards or อง you have controis in place to detect source code	X			Merge request, Hash della
		CCC-03.5 CCC-03.6	of systems and services.	Are niecriafusius in piace to ensure cuat an debugging and	X			Merge request
Change Control &	CCC-04 CCC-05	CCC-04.1 CCC-05.1	Policies and procedures shall be established, and Policies and procedures shall be established for managing	bo you have controls in place to restrict and monitor the boyour provide tenants with adcumentation mat describes by you have poincies and procedures escapished to:	X	х		Hash della release e relativo
Configuration Management		CCC-05.2 CCC-05.3	the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting	po you nave tecrificar measures in piace to ensure triat	X			Risk assessment 27001
Data Security & Information	DSI-01	DSI-01.1 DSI-01.2	Data and objects containing data shall be assigned a classification by the data owner based on data type, value,	po ybia province il capatility to ibentity uata ana naruwarė*	Х		x	
Data Security & Information	DSI-02	DSI-02.1 DSI-02.2	Policies and procedures shall be established, and supporting business processes and technical measures	co you inventory, actoment, and manuain data now to care you ensure that data does not migrate beyond a	x			

Data Security &	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that	DO YOU Provide standardized (e.g. 130/15C/11011-proprietary	lv	1		protocollo https
Information	D3F03	DSI-03.1 DSI-03.2	traverses public networks shall be appropriately classified	po you'uunze open endîyîtîon fileutoùòrogies any'ume'	x			VPN, HTTPS, autenticazione
Data Security & Information	DSI-04	DSI-04.1 DSI-04.2	Policies and procedures shall be established for labeling, handling, and the security of data and objects which	por your direction as structured data-labeling standard (e.g., iso	x	x		ISO 27001
Lifecycle		DSI-04.2 DSI-04.3	contain data. Mechanisms for label inheritance shall be	Ale medianisms for laber mineritance implemented for		X		
Data Security &	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-	do you flave procedures in piace to ensure production data. Are the tesponsionities regarding data stewardship defined,	x			ambienti separati previsti
Data Security & Data Security &	DSI-06 DSI-07	DSI-06.1 DSI-07.1	All data shall be designated with stewardship, with Policies and procedures shall be established with	Do you support the secure deletion (e.g.,	x			ISO 27001
Information			supporting business processes and technical measures	degaussing/cryptographic wiping) of archived and backed-				
Lifecycle Management			implemented for the secure disposal and complete removal of data from all storage media, ensuring data is	up data?				
Datacenter Security	DCS-01	DSI-07.2 DCS-01.1	Assets must be classified in terms of business criticality,	Do you classify your assets th terms or pusifiess criticantly,	X		Y	ISO 27001 IAAS
Asset Management		DCS-01.2	service-level expectations, and operational continuity	peryon framham a comprese inventory or all on your chical are physical security perimeters (e.g., refices; wans, dainers,			X	IAAS
Datacenter Security Datacenter Security	DCS-02 DCS-03	DCS-02.1 DCS-03.1	Physical security perimeters (e.g., fences, walls, barriers, Automated equipment identification shall be used as a	Do you nave a capability to use system geographic location			X	IAAS IAAS
Equipment	DC5-03	DCS-03.1 DCS-03.2	method of connection authentication. Location-aware	rs automfaced equipment roemunication used as a metriou to			X	IAAS
Datacenter Security	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or	is admonzation obtained prior to relocation or transfer or cardyou profluertenants who ryoth its er management			X	IAAS
Datacenter Security Datacenter Security	DCS-05 DCS-06	DCS-05.1 DCS-06.1	Policies and procedures shall be established for the secure Policies and procedures shall be established, and	call you provide edigence that policies, standards, and			X	IAAS IAAS
Policy		DCS-06.2	supporting business processes implemented, for	Carr you provide évidence triat your personner and involved Are physical access control mechanisms (e.g. CC) v			х	IAAS
Datacenter Security Datacenter Security	DCS-07 DCS-08	DCS-07.1 DCS-08.1	Ingress and egress to secure areas shall be constrained and Ingress and egress points such as service areas and other	Are ingresS and egress planics; such as service areas and			X x	IAAS IAAS
Datacenter Security	DCS-09	DCS-09.1	Physical access to information assets and functions by	bo you restrict physical access to information assets and bo you have key management policies billiong keys to			X	IAAS
Encryption & Key Encryption & Key	EKM-01 EKM-02	EKM-01.1 EKM-02.1	Keys must have identifiable owners (binding keys to Policies and procedures shall be established for the	Do you have a capability to allow creation or unique		x		
Management		EKM-02.2	management of cryptographic keys in the service's	DO YOU HAVE a CAPADINITY TO THAT THE PROPERTY OF THE PROPERTY		X		
Key Generation		EKM-02.3	cryptosystem (e.g., lifecycle management from key	Do you maintain key management procedures?		X		
		EKM-02.4 EKM-02.5	generation to revocation and replacement, public key infrastructure, cryptographic protocol design and	ΰο γοά αιίπze any tim ά party/open source/proprietary		x		
Encryption & Key	EKM-03	EKM-03.1	Policies and procedures shall be established, and	ठिठ you encrypt tenant data at rest (on diskystorage) within एक you leverage स्त्रीटा yption to protect data and virtual		х		
Management Encryption		EKM-03.2 EKM-03.3	supporting business processes and technical measures implemented, for the use of encryption protocols for	or you nave outdimentation establishing and wellining your		X		
Encryption & Key	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256)	po you have platform and data appropriate encryption mat	х			
Management Storage and Assess		EKM-04.2	in open/validated formats and standard algorithms shall be	Are your eficiýption keys mannalneo by trie Ciodó	v	Х		
Storage and Access		EKM-04.3	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud	Do you store encryption keys in the cloud?	<u></u>	х		
Governance and	GRM-01	GRM-01.1	Baseline security requirements shall be established for	bo you have documented information security baselines for	x			
Risk Management Baseline		GRM-01.2	developed or acquired, organizationally-owned or managed, physical or virtual, applications and	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your				
Requirements			infrastructure system, and network components that	information security baselines?		х		
Governance and Risk Management	GRM-02	GRM-02.1 GRM-02.2	Risk assessments associated with data governance requirements shall be conducted at planned intervals and	Does your organization's risk assessments take into account Do you conduct his assessments associated with data	×	Х		
Governance and	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of,	Are your tecrinical, ousniess, and executive managers	x			
Governance and	GRM-04	GRM-04.1	An Information Security Management Program (ISMP)	po you provide teriants with accumentation bescribing po you review your mid mation security wanage inent?	V	х		ISO 0001 E 27004
Risk Management Governance and	GRM-05	GRM-04.2 GRM-05.1	shall be developed, documented, approved, and Executive and line management shall take formal action to	Do execütive and intermanagement take romanaction	X			ISO 9001 E 27001
Governance and	GRM-06	GRM-06.1	Information security policies and procedures shall be	An e your inhorination is security polities and procedures made An e inhorination security polities authorized by the	х			ISO 27001
Risk Management Policy		GRM-06.2 GRM-06.3	established and made readily available for review by all impacted personnel and external business relationships.	vo you nave agreements to ensuré your providers autière	X			
		GRM-06.4	Information security policies must be authorized by the	carryou provide evidence to que anigence rilapping or your	^	х		
	CD14.07	GRM-06.5	organization's business leadership (or other accountable	is a formal disciplinary or sanction policy established for		X		Information a sealer of deal
Governance and Risk Management	GRM-07	GRM-07.1 GRM-07.2	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and	Are employees made aware or what actions could be taken	x	Х		Informativa e gestione degli Informativa e gestione degli
Governance and	GRM-08	GRM-08.1	Risk assessment results shall include updates to security	Do'nsk assessment resurts include applates to security	Х			
Governance and Risk Management	GRM-09	GRM-09.1 GRM-09.2	The organization's business leadership (or other accountable business role or function) shall review the	oo you periorin, at minimitum, annitar reviews to your	x			
Governance and	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk	Are tormar risk assessments aligned with the enterprise- is the intermood and impact associated with innerent and	x			
Risk Management	CD14.44	GRM-10.2	assessments shall be performed at least annually or at	transistant nasteria transistant in sealor at a commistrativa de la commistrativa de la commissión de la com	x			
Governance and Risk Management	GRM-11	GRM-11.1 GRM-11.2	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and	Do you make available documentation or your organization	^	x		
Human Resources	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or	တုပ်က termination or contract or business relationship, are ၁၀ you nave assecretum procedures outlining now assets	х			
Asset Returns Human Resources	HRS-02	HRS-01.2 HRS-02.1	expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual	Pursualne to tocarraws; regulations, etines, and contractual	x			
Human Resources	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions	Do your employment agreements incorporate provisions and/or Do your edure that employments directed a resigned by	x			
Employment Human Resources	HRS-04	HRS-03.2	and/or terms for adherence to established information Roles and responsibilities for performing employment	Are tobiamented policies, procedures, and guidelines in	X			
Employment		HRS-04.1	termination or change in employment procedures shall be	olo triè acove pi oceocrés arrogoroennes account roi tritiery	X			
Human Resources	HRS-05	HRS-05.1	Policies and procedures shall be established, and	Are policies and procedures established and measures Are requirements for holi-disclosure or confidentially	X			
Human Resources Human Resources	HRS-06 HRS-07	HRS-06.1 HRS-07.1	Requirements for non-disclosure or confidentiality Roles and responsibilities of contractors, employees, and	po you provide tetiants with a role tienimon luccuntem.	x			
Human Resources	HRS-08	HRS-08.1	Policies and procedures shall be established, and	υο γού nave ponicies and procedures in practice to dentile υο γου denne anowance and conditions for επου devices		х		
Acceptable Use Human Resources	HRS-09	HRS-08.2 HRS-09.1	supporting business processes and technical measures A security awareness training program shall be established	po'yòu provide a totmar, role-based, secunty awareness	x	X		FORMAZIONE
Training / Awareness		HRS-09.2	for all contractors, third-party users, and employees of the	ာပ you specificatify train your employees regarding their ာပ you uocument employee acknowledgment of training	x			
		HRS-09.3	organization and mandated when appropriate. All individuals with access to organizational data shall receive	1s successful and timed completion of the training	X			
		HRS-09.5	appropriate awareness training and regular updates in	Are personner d'aineu anu provided with awareness	^	x		
		HRS-09.6	organizational procedures, processes, and policies relating	Are administrators and data stewards properly educated on Are bersonner mornifed or their resubhsionities for	х			
Human Resources User Responsibility		HRS-10.1 HRS-10.2	All personnel shall be made aware of their roles and responsibilities for:	Are personner imormed or their responsibilities to:	x			
		HRS-10.3	Maintaining awareness and compliance with established	Are personner informed or their responsibilities for ensuring Are air computers and raptops configured such that there is	х			
Human Resources Workspace		HRS-11.1 HRS-11.2	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on	And order exponents and procedures or ensure triac - ?	X			
Identity & Access	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the	po you restrict, log, and thomtol access to you'linormation po you monitor and log privileged access (e.g.,	х			
Management	IAM-02	IAM-01.2 IAM-02.1	organization's information systems shall be appropriately	bo you monitor and log privileged access (e.g.,	X			
Identity & Access Management	IAWI-UZ	IAM-02.2	User access policies and procedures shall be established, and supporting business processes and technical measures	Do'you nave policies, proteutres and technicar measures in		х		
User Access Policy		IAM-02.3 IAM-02.4	implemented, for ensuring appropriate identity, entitlement, and access management for all internal	Do you nave procedures and technical measures in piace Do you nave procedures and technical theasures in piace	X			COMPETENZE
		IAM-02.4 IAM-02.5	corporate and customer (tenant) users with access to data	Do yoù emorce data access permissions pased on the rules	x			
		IAM-02.6	and organizationally-owned or managed (physical and	po you provide highics to track the speed with which you	х	L.		
Identity & Access	IAM-03	IAM-02.7 IAM-03.1	virtual) application interfaces and infrastructure network User access to diagnostic and configuration ports shall be	is user access to diagnostic and configuration ports restricted	x	^		
Identity & Access	IAM-04	IAM-04.1	Policies and procedures shall be established to store and	bo you manage and store the identity of an personner who bo you manage and store the user identity of air personner	x			COMPETENZE
Management Identity & Access	IAM-05	IAM-04.2 IAM-05.1	manage identity information about every person who User access policies and procedures shall be established,	và yàu provide tenants with documentation on how you	, x	x		COMPETENZE
Identity & Access	IAM-06	IAM-06.1	Access to the organization's own developed applications,	Are controls in piace to prevent unaturorized access to Are controls in piace to prevent unaturorized access to	х			
Management Identity & Access	IAM-07	IAM-06.2 IAM-07.1	program, or object source code, or any other form of	Does your organization conduct third-party unauthorized	X			
Management	AIVI-07	IAM-07.1 IAM-07.2	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to	Are preventive, detective corrective compensating controls in				
Third Party Access			the organization's information systems and data shall be	place to mitigate impacts of unauthorized or inappropraite access?	L			
Identity & Access	IAM-08	IAM-08.1	followed by coordinated application of resources to Policies and procedures are established for permissible	DO YOU document now you grant, approve and enforce	x			
Management		IAM-08.2	storage and access of identities used for authentication to	Based on thie tidies of feast privilege, do you have porities -	x			
User Access Identity & Access	IAM-09	IAM-08.3 IAM-09.1	ensure identities are only accessible based on rules of least	does you management provision the authorization and	x			
Management	AIVI-09	IAM-09.1 IAM-09.2	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier	po you provide upon the request or users with regithmate	x			
Identity & Access	IAM-10	IAM-10.1	User access shall be authorized and revalidated for	bo you require a perioricar autriorization and validation bo you'conect evidence to demonstrate rifat tile policy (see	X			gostiana is -1-1
Management		IAM-10.2 IAM-10.3	entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable	follow user access policies?	x			gestione incidenti di
User Access Reviews		IAM-10.4	business role or function supported by evidence to	will you share user enutrement and remediation reports with is unitery depitons orming, revocation, or modification or de-	х			COMUNICAZIONE AL
	IAM-11	IAM-11.1 IAM-11.2	Timely de-provisioning (revocation or modification) of user	rs any challge in user access status intefraeo to include	x			
Identity & Access		IAWI-11.Z	access to data and organizationally-owned or managed Internal corporate or customer (tenant) user account	bo you support use or, or integration with, existing	X			
	IAM-12	IAM-12.1		vo you use open stantuarus to délegate adtinentication	х			WS SOAP e REST
Identity & Access Management Identity & Access Management		IAM-12.2	credentials shall be restricted as per the following, ensuring	DO YOU SUPPORT IDEALITY TEDERATION STANDARDS (E.g., SAIVIL,				
Identity & Access Management Identity & Access			credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and	DO you have a roncy entorcement ront capability (e.g.,	X	x		SPID, LDAP Aziendale
Identity & Access Management Identity & Access Management		IAM-12.2 IAM-12.3 IAM-12.4 IAM-12.5	appropriate identity, entitlement, and access management and in accordance with established policies and procedures:	DO You Have a ronicy enforcement ronnt capability (e.g., DO You'riave amuentity mahagement system tenability	Х	x x		SPID, LDAP Aziendale
Identity & Access Management Identity & Access Management		IAM-12.2 IAM-12.3 IAM-12.4 IAM-12.5 IAM-12.6	appropriate identity, entitlement, and access management and in accordance with established policies and procedures: - Identity trust verification and service-to-service	DO you have a roncy entorcement ront capability (e.g.,	X X X	x x		SPID, LDAP Aziendale TOKEN OTP
Identity & Access Management Identity & Access Management		IAM-12.2 IAM-12.3 IAM-12.4 IAM-12.5 IAM-12.6 IAM-12.7 IAM-12.8	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)	DO you histe a runky emortement runk Capatomy (e.g., 100 you history make an overruty mail ageiment system renauling to you priorited defaults with strong mail to not you provided the control of the co	X X X	X X		SPID, LDAP Aziendale
Identity & Access Management Identity & Access Management		IAM-12.2 IAM-12.3 IAM-12.4 IAM-12.5 IAM-12.6 IAM-12.7	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 lett and allow the understand the contractions.	DO you'llave a' ronky cintorkennent ronk Capabinky (e.g., DO you'lave a'n bennuty mainagement system renabining bo you'ly broad ethanfas wan's strolly influentation?	X X X X	x x		SPID, LDAP Aziendale TOKEN OTP

The content of the	Identity & Access	IAM-13	IAM-13.1	Litility programs canable of notantially oversiding system	Are access to utility programs used to manage virtualized	V			
				Utility programs capable of potentially overriding system, Higher levels of assurance are required for protection,		^	х		
The content of the				retention, and lifecycle management of audit logs,		х			
					the transfer of the transfer o	x	X		
1995 1996							х		
The content of the									
March 1995					Aré changes maue co virtuar înacmiles, or îmbving or an				
1985 1985				A reliable and mutually agreed upon external time source		х			
Service Company of the Company of th								X x	
March Marc	Security					х		^	
March 1995	Capacity / Resource	IV.C OF	IVS-04.4			х		v	SAR SUI SERVIZI (VM) E
Company Comp	Infrastructure &	IVS-06	IVS-06.1					x	
Company			IVS-06.2					х	
Marchael	Security Network Security		IVS-06.3		Are an firewar access confror is its adouthenced with			X x	
The company of the	Infrastructure &	IVS-07	IVS-07.1			х			
The company of the	Infrastructure &		IVS-08.1			х	v		
Angeles of the control of the contro			113 00.2			x	^		
The company of the		IVS-09	113 03.2			Х			
The company					Pravid your imprelhenced the necessary metasures for the	x			
interpretation 10-10				deployed, and configured such that provider and customer	Do you have trie ability to logically segment or encrypt	X			
March Marc	Infractsustura 9	IVC 10				X			
The company of the						X			
Company Comp				Access to all hypervisor management functions or	grandomes stefn reticenomes by statetentin son makes forces				
Secretary 1997 1997					are figured-and/mintoennies deconstant this injectionisms				
Management Man					Are policies ariu procedures established and inechanishis				
Second Column	Infrastructure &	IVS-13		Network architecture diagrams shall clearly identify high-					
March Marc		IPV-01	IVS-13.2		ου γου puonisma niscon ain Arns avaniable in the sérvice and	x	X		
March 1972	Interoperability &	IPY-02	IPY-02.1			х			PDF, XLS, CSV
The companies	Interoperability &	IPY-03	IPY-03.1			X			
March Marc					bo you provide policies and procedures (i.e. service lever	x			
Transport of the control of the cont	Interoperability &	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and		х			
Processing Process P		IDV-OF				X			
March Month Mont	Interoperability & Portability	121-05			nrusing virtuár intrastruccuré, are mácnine liffáges inlaue	^	x		
Model Mode	Virtualization		IPY-05.3	help ensure interoperability, and shall have documented		х			
Proceedings 1905	Mobile Security Mobile Security								
Model Mode	Mobile Security								
Modes Security 905-86 (1997) (Mobile Security			The BYOD policy and supporting awareness training clearly					
The content of the					po ybu nave à doctimenteu lisc of pre-appli ovelu ciouur - 1		**		
Market Searchy (1951) (1952) (Mobile Security								
And Security 90-10 1 200-11 20 1 201-11 201-	Mobile Security								
MAGES Searchy MOD-12 MOD-12 The model above party and region that search profession of the model and the m					Do you nave a centralized mobile dévice management				
Security Models Security Models (1997) 1 Model				The mobile device policy shall require the use of		х			CRITTOGRAFATO
Models Security MOSE 31 MOSE 32 MOSE 33 MOSE 34 MOSE 34 MOSE 33 MOSE 34 MOSE 3	Mobile Security	MOS-12							
Models Security MOS-12		MOS-13			ουσές your ότου poncy cléahy denne της expectation or				
Miller Security Mod-19. Mod-1							х		
Models Security Models (Models) Models) Models (Models) Models (Models) Models) Models						X			
Models Security Models Securit	Mobile Security					^	x		
Models Security Models (Models and procedure) Models (Models and p	Passwords			documented and enforced through technical controls on	Are your password policies enforced through technical		x		
models Security MOS-18 MOS-18 MOS-18 MOS-18 MOS-19					The bright (faces \$400.00) and the common control of the control of				
Model Security Models Security	Mobile Security	MOS-17	MOS-16.3	all company devices or devices approved for BYOD usage,	.,,		х		
Models Security Purises Models Security Purises Models Security Models (Models Security Market) Models Security Models (Models Security Market) Models Security Models (Models Security Models (Models Security Models) Models Models (Models) Models (MOS-17	MOS-16.3 MOS-17.1	all company devices or devices approved for BYOD usage, The mobile device policy shall require the BYOD user to	Do'you'nave a poncy macrequires BYOD users to promote bo'you nave a promote		x x		
Models decided with models of the communication of	Policy		MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3	all company devices or devices approved for BYOD usage, 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-	Do'you'riave a poncy mat requires ธาบบ บรัตร ใช้ๆerhorin bu'you nave a poncy mat requires ธาบบ บระเร เบ promoic บับ you nave a poncy mat requires ธาบบ บระเร เบ บระ ann		X X X		
Security incident Security inc	Policy Mobile Security		MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1	all company devices or devices approved for BYOD usage, 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-	Do'you'riavie'a poncy triart requires arou uséis's to'perhòmic bus qua nakera poncy triart requires abour users to promunc do you nave a poncy triart requires arour users to use anti- uotes yout i'f provide tentore wipe til corporate usata wipe bues'your n' provide tentore wipe to'corporate usata wipe		x x x x		
Security Incident Security Inc	Policy Mobile Security	MOS-18	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1	all company devices or devices approved for BYOD usage, 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-	od you'navie a poncy mat requires a roor defers' to perfloring bu you nafee a pilitely man requires brior users ou promon they you nafee a poncy man't requires broor users to use anno- uoles you'n rife provide reintour wipe or propriate wat awaye bous' yourn'n provide reintour wipe or conjourate wat wipe for yourn mount cuerices riary of the intests a dynamous sections?	X	X X X X X		
Security Incident SEP 01 SEP 02 SEP 03 SEP	Mobile Security Remote Wipe Mobile Security Security Patches	MOS-18	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for	Do'you'riave' a poncy tract requires a root ose'n's to' perhonit bo you rake a poncy mat requires not osens to promot to you rake' a poncy mat requires not osens to use anno todes your in' provide hemote wipe to' Corporate oata wipe boe's your in' provide hemote wipe to' Corporate oata wipe tode's your in provide hemote wipe to' Corporate oata wipe tode your in roome oevices have time have a wanaoue seconny- oo'you'n moome oevices have time haves a wanaoue seconny- oo'you'n moome oevices have time haves a wanaoue seconny-	х	x x x x x x x x x x x x x x x x x x x		
Management, C. \$56,023 supporting biorises processes and technical measures of the control	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security	MOS-18	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.1	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers	od you'navie a poncy mar requires a roo oséin's to perhomit bo you navie a pilocky mar requires show users ou promon to you navie a poncy mar requires root users no use a min- uoles you'n rip rovide reinnow wiget of comporate or an wipe to use'you'n rip rovide reinnow wiget of comporate or an wipe to you'n moune cevices navie of the inters a variance seconny- oby out motione cevices navie of the inters a variance seconny- oby out motione cevices navie or reinfore variation no obces you'n strong pointsy calmy the systems a morse refers obces you'n strong pointsy user's pilotis more strain as refers obces you'n strong pointsy user's pilotis more strain as refers	X	X X X X X X		
Security Incident Amagement, E Security Incident Amagement Amagement Security Incident Amagement Security Incident Amagement Security Incident Amagement Security Incident Amagement A	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident	MOS-18 MOS-19 MOS-20 SEF-01	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.1 MOS-20.1 SEF-01.1	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities,	od you'navie a poncy triat requires a root odéin's to perhimit but you navie a pilote, trian requires a root odéin's to perhimit but you navie a poncy trian requires a root ous as it ou sea anno odes your in province reinfolk white of colipionate oara wipe those's your in province reinfolk white of colipionate oara wipe too your income oevices have the raises a almaine as county od your income oevices have the raises a almaine as economy object income oevices have the raises a single as our object you'n briton pointsy cashing the systems and service object your aroot pointsy specify officials in order of object your amount was placed in the source of object you manual massive and points or confact with no cash	х	X X X X X X		
SEPONS SE	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident Security Incident	MOS-18 MOS-19 MOS-20 SEF-01	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.1 MOS-19.2 MOS-20.1 MOS-20.1 SEF-01.1 SEF-02.1	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, Policies and procedures shall be established, and	od you'navie a poncy triat requires a root odéin's to perhimit but you navie a pilote, trian requires a root odéin's to perhimit but you navie a poncy trian requires a root ous as it ou sea anno odes your in province reinfolk white of colipionate oara wipe those's your in province reinfolk white of colipionate oara wipe too your income oevices have the raises a almaine as county od your income oevices have the raises a almaine as economy object income oevices have the raises a single as our object you'n briton pointsy cashing the systems and service object your aroot pointsy specify officials in order of object your amount was placed in the source of object you manual massive and points or confact with no cash	x	X X X X X X X X		
Management, E- Drovewy, & Cloud Control of the responsibility and, if required, shad content and/or control trailing are to report incidents in a timely manner, information security events in a timely manner adhering to applicable spat, statutory, or regulatory completable spat, statutory, or regulatory completed on spationing spationing management, see spationing spatial spat	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident Security Incident	MOS-18 MOS-19 MOS-20 SEF-01	MOS-16.3 MOS-17.1 MOS-17.2 MOS-18.1 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.1 MOS-20.2 SEF-01.1 SEF-02.2	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, Policies and procedures shall be established, and supporting business processes and technical measures	od you'navie' a poncy' mat requires or our defer'to perithmin but you nake a plinky mat requires of our users to promot but you make a poncy mat requires or our owns to use a number of the your nake a poncy mat requires or our owns to use a number of the your nake a promot our	x	X X X X X X X X X X X X X X X X X X X		
blad Consent and/or contractually agree to report all informations security reviews in a timely manner in a finely manner in the contractual and agree to report all information security reviews in a timely manner information security reviews shall be reported through a security incident the protect through a security incident the protect protection of the protection of	Mobile Security Remote Wipe Mobile Security Security Pathes Mobile Security Users Security Incident Security Incident Management, E- Discovery, & Cloud Forensics	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1 MOS-19.1 MOS-19.2 MOS-20.1 MOS-20.2 SEF-01.1 SEF-02.2 SEF-02.2 SEF-02.3	all company devices or devices approved for BVOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a 8YOD-enabled device. Points of contact for applicable regulation authorities, 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	od you have a poncy mar requires arrow odés to perhimit bu your have a pincy mar requires arrow oses to promot bu you make a pincy mar requires arrow oses to promot outs you make a poncy mar requires arrow oses to too sea to too sea must be your make a poncy mar requires arrow oses pour if provide reindre wijed of conporate data wipe fourly your in provide tentione wiged of conporate data wipe for your mount devices have the haves a damage secondary out your mount devices have the systems at mars offers obes your for you planty adapt you fire systems at mars offers obes your for you planty adapt you mark systems at mars offers obes your marman massiffs and points or conflact want occar out your mage mar massiffs and points or conflact want occar out your marman massiffs and points or conflact want occar out you margan and the secondary incident response plan?	X	X X X X X X X X X X X X X X X X X X X		
information security events in a timely manner. Information security events with all per porter than the sequence of the content of the conte	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident Security Incident Management, E- Discovery, & Cloud Forensics Security Incident	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.1 MOS-20.1 SEF-02.1 SEF-02.2 SEF-02.2 SEF-02.4 SEF-03.1	all company devices or devices approved for BYOD usage, 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-	od you have a poncy mar requires a roo users to promot bu you have a pincy mar requires roto users to promot to you have a poncy mar requires roto users to use anno- users you if you have reindle while or conjourate data wipe bously your in provide reindle while of conjourate data wipe bously your in provide reindle while of conjourate data wipe bously your in provide reindle while of conjourate data wipe bously of the policy tally the systems and set of its bouse youth at 100 pinky cally in the systems and set off is obes you have a documented security incident response plan? Or you have a formation of the provident of the provident in Or you have a formation of the provident in the your Or you have a formation of the provident provident in Tax with the provident in the provident in Tax with	X X	X X X X X X X X X X X X X X X X X X X		
Security Incident Management, E SEF-041 SF-052 required for the presentation of evidence to support Security Incident SEF-053 SF-053 and SEF-053 security incident SEF-054 security incident SEF-055 SF-055 security incident SEF-055 SF-055 SF-055 security incident SEF-055 SF-055 SF-055 security incident SEF-055 SF-055	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Security Incident Security Indent Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.1 MOS-20.1 SEF-02.1 SEF-02.2 SEF-02.2 SEF-02.4 SEF-03.1	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 one Workforce personnel and external business relationships shall be informed of their responsibility and, if required shall consent and/or contractually agree to report all	od you rianki a poncy man requires en our oddes to perhom be you rake a plincy man requires show users to promot or you want a poncy man requires or our own to use a nor outs you rinch a poncy man requires or our own to use a more outs you in you want or man was to be outside to the outside outside the outside outside the outside outside the outside outsid	x x	X X X X X X X X X X X X X X X X X X X		
SECUTIVE INCIDENT SEP-04.2 SEP-04.3 Proper fromerics procedures, including chain of custody, are what a process of the region of the preventation of evidence to support for the preventation of evidence to support formations. SEP-04.3 SEP-04.3 SEP-04.3 SEP-05.4 SEP-05.4 SEP-05.4 SEP-05.5 SEP-05.4 SEP-05.5 SEP-05.4 SEP-05.5 SEP-05.4 SEP-05.5 SEP	Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.1 MOS-20.1 SEF-02.1 SEF-02.2 SEF-02.2 SEF-02.4 SEF-03.1	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices permitted for user to result of the company BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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.	od you rianki a poncy man requires a rou od 68° to perhom bor you nake a pôncy man requires a rou od 68° to perhom bor you nake a pôncy man requires a rou odes no use a numerous you riank a requires a rou odes no use a numerous you ri provide reintoe whigh of coloporate out a wipe to you not you was a remainded by the rough of the coloporate out a wipe to you moune oevices raise's dire areas, a samaone security of your moune oevices raise's dire areas, a samaone security of your moune oevices raise's dire areas, a samaone security of your moune oevices raise's life samaone security of your moune oevices raise's life samaone security of your around your pours, you pendy net of the samaone security of your rough of your security in coleent requirements much your your public around your security in coleent requirements much your your publish a rouge samor reportionse plans in une your working of your security in coleent response plans' in rough your security in coleent response plans' in your your your publish in rough your security in coleent response plans' in rough your security in coleent response plans' in rough your security in coleent response plans' in your your your your publish in rough your security in coleent response plans' in your your your your your your your your	x	X X X X X X X X X X X X X X X X X X X		
Security Indeent Management, Transparency, and Accountability Helmon STA032 STA033 STA043 STA043 STA043 STA043 STA043 STA043 STA054 STA055 STA	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Security Indident Security Indident Management, E- Discovery, & Cloud Forensics Security Incident Management E- Discovery, & Cloud Forensics Incident Management E- Discovery, & Cloud Forensics Incident Reporting	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-01.1 SEF-02.2 SEF-02.3 SEF-02.3 SEF-03.2	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices permitted for user through the company BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 is a timely manner. Information security events shall be reported through nardefined communications. Annoels in a timely manner.	od you riawie a poncy mar requires or our odéth' to perhàmic be you naée a plinky mar requires of our ousers ou promour but you marke a poncy mar requires or our ousers ou promour ousers out promour ousers out you not not out the promour ousers out promour ousers out in the promour out of your mome uservices nave vite naves a donator security out you mome uservices nave vite naves a donator out of your mome uservices nave vite naves a donator out of your mome uservices nave vite naves a donator out of your mome uservices nave vite naves vite should be plantly calling the should be refer to both your moment massified and your plantly out of your moment massified and your plantly out of your moment of your moment of your moment of your moment of your plantly out your plantly out of your plantly out of your plantly out your your plantly out your your plantly out your your your your your your your your	x x	X X X X X X X X X X X		
Serious Serious Serious Serious Serious Mechanisms shall be put in place to motive and quantify in eight. Serious Security indefent. Upon nortification, on the post of place in a serious treatment and separation with X y or you with the post of place in a serious treatment and serious treatments and serious treatments and serious treatments of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the provider shall perform a nortical place in the post of the	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Security Indident Security Indident Management, E- Discovery, & Cloud Forensics Security Incident Management E- Discovery, & Cloud Forensics Incident Management E- Discovery, & Cloud Forensics Incident Reporting	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.1 MOS-19.2 MOS-19.1 MOS-20.2 SEF-02.1 SEF-02.2 SEF-02.3 SEF-02.4 SEF-03.2	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a 870D-enabled device. Points of contact for applicable regulation authorities, 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 Wortforce 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 in a timely manner. Information security events in a timely manner. Information security events in a timely manner.	odyouriavie'a poncy mar requires or our odété to perhimitor your index a plincy mar requires or our outsets ou promou to your water against or our outsets ou promou to your water against or our outsets our promou to your index promous entered with some or outsets our outsets our outsets our outsets our outsets outsets our outsets ou	x x	X X X X X X X X X X X X X X X X X X X		
Monagement, Serios Seri	Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Security Incident Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Incident Reporting Security Incident Management, E- Discovery, & Cloud Forensics Incident Reporting Security Incident Management, E- Discovery, & Cloud	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.2 SEF-01.1 SEF-02.3 SEF-02.3 SEF-03.2 SEF-03.2	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices onnecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a 8YOD-enabled device. Points of contact for applicable regulation authorities, 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 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 manager. Information security events is a timely manager. Information security events shall be reported through neadefined communications channels in a timely manager. Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support poetnatil legal action subject to the relevant jurisdiction.	odynorianie a poncy mar requines a rou osies to perhimitoro marker a pinicy mar requines a rou oses s co promoc do you marker a poncy mai requines a rou oses s co promoc do you marker a poncy mai requines a rou oses you in the provide reinnote while of comparate cara when the poncy of the provides reinnote while of comparate cara when the poncy of the provides reinnote while of comparate provides when the provides reinnote was a result of the poncy of the poncy of the provides a rough a rough of the poncy specify rein artists a rain and office of the poncy of the poncy of the provides rough a rough of the poncy of the pon	x x	X X X X X X X X X X X X X X X X X X X		
Supply Chain STA-01 STA-03 The provider shall inspect, account for, and work with their objects and account for, and work with their objects and account for an experiment control of the provider shall make security incident information and providers and accountability for the providers and considerations, and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and infrastructure network and objects of the providers and considerations and considerations and infrastructure network and objects of the providers and considerations and	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Security Incident Security Incident Management, E- Discovery, & Cloud Forensics Incident Reporting Security Incident Management, E- Discovery, & Cloud Forensics Fo	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.1 MOS-20.2 SEF-01.1 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.2	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 in a timely manner. Information security events in a timely manner. Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action security incident. Upon notification, after an information security incident. Upon notification,	od you rianki a poncy mar requires a roor users to promote the boy you rake a plinely mar requires a roor users to promote the you rounked a point, you are required as roor users to promote the your rake a point of a roor users to use announced to you rake a point of provide reintitle which or copy and a roor users to you are the reintitle which or copy and a roor user when the your room to what is reintitle which is drawn a sharp or you will show the provide raintitle which is drawn a sharp or your roor points y specify rate sizes the washington or your roor points y specify rate sizes the roots of rate are to your manual massified and points or confact curring conditions of your around point you realist the roots of rate are to your manual massified and points or confact curring conditions or your provide a roor points y specify in the specific points or confact curring control your restore your receiver your receiver hy norder response plan? The work of your root and the root of the your roo	x x	X X X X X X X X X X X X X X X X X X X		
STR-02 STR-02 STR-03 Business critical or customer (tenant) impacting (physical may stream) and infrastructure network and systems components, that be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as Tig overance with mutually agreed-upon service and capacity-level expectations, as well as Tig overance and capacity-level expectations and capacity of the time and ti	Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Security Incident Security Incident Management, E- Discovery, & Cloud Forensics Security Incident	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.1 SEF-02.1 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.2 SEF-03.2 SEF-04.4 SEF-04.4 SEF-04.4 SEF-04.4	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall mobile devices onnecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through increditions communications, channels in a timely manner. Information security events shall be reported through confeding the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, after an information security events to revolute to the relevant jurisdiction after an information security incident. Upon notification, after an information security incident. Upon notification, after an information security events to the relevant jurisdiction after an information security events to the commitment and under the commitment an	odyourianter a poncy man requires a rour oddes to perform boryourianter a pointy train requires a rour oddes to perform to yournate a poncy main requires a rour oddes to use a number of your rours a poncy main requires a rour oddes to use a number of your rife provide feminite while of your or care when the your rours are provided to the your rouns are when your rouns are when your rouns are when the your rouns are when your rouns are when your rouns are your rouns and your rouns are your rouns and your rouns are your rouns and your rouns and your rouns are your rouns and your rouns are your rouns and your rouns are your rouns and your your part and your rouns and your rouns are requirementers more your your publish a rouns a more pophissionness your comment and your resident your security incident response plans in rouns your publish a rouns and response plans in rouns your publish a rouns and response your response your security incident response plans in rouns your published a rouns and response your recording to the your security incident response plans in rouns your rouns your mount and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yours your mounter response pain comply with mount in user of your your incident response your mounter response pain comply with mount in which is actively to your your rouns of supporting in gradually your your your reset of supporting in gradually when your reset or your your rouns are discussed in mountain or yet your security in rouns in the your your rouns and a reset or tenants cause your mounter of your your your rouns and advanced to your your rouns and a rouns and your your your and a state or your your your your your your your y	x x	X X X X X X X X X X X X X X X X X X X		
STA-03 ST	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-04	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-01.1 SEF-02.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.2 SEF-04.4 SEF-04.2 SEF-04.5 SEF-04.5 SEF-04.5 SEF-04.5 SEF-05.5 SEF-05.5	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices permitted for user through the company BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 is a timely manner. Information security events shall be reported through nardefined communications. Channels in a timely manner. Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support openation and the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon nortification, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security the types, volumes, and costs of information security entered and the security providers shall intent the constitution of the cost of the cost of the cost	od you riable a poincy mar requires or our oddes to perhami- tor you rabe a poincy mar requires or our observation or our own and our you make a poincy mar requires or our own as our promout of you you make a poincy mar requires or our own account of the provide reinties which our own account of your mount overview frames where the rest of animal or our you minotine to evices have the areas of animal or our your minotine to evices have the areas of animal or our your minotine to evices have the areas of animal or our your minotine to evices have the areas of your minotine to your point, you pointly the systems and use evices your be out your manufactor contains or contains a more your your points and our your minotine to your animal or your animal or your animals of your animals of your your your your your your animals of your animals of your your your own and your your your own your your your own your your animals of your animals. They your animals of your animals. Your your animals of your your animals. Your your your your your your your your y	x x	X X X X X X X X X X X X X X X X X X X		
Accountability Transparency, and	Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Security Incident Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, E- Supply Chain Management,	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-04	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-01.1 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.2 SEF-04.3 SEF-04.4 SEF-04.5 SEF-04.5 SEF-04.1 SEF-04.1 SEF-04.1 SEF-05.1 SEF-05.1 SEF-05.1 SEF-05.1	all company devices or devices approved for BYOD usage, The mobile device policy shall require the BYOD user to perform backups of data, profibit the usage of unapproved application stores, and require the use of anti-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices onnecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 in a timely manner. Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support poential legal action subject to the relevant jurisdiction after an information security events in the relevant jurisdiction after an information security incident. Upon notification, Mechanisms shall be put in pleate to monitor and quantify the types, volumes, and costs of information security broviders shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors	od you riaw's a poncy man requires or our oddes' to perform to you rake a plincy man requires or our observations of the properties of the	x x	X X X X X X X X X X X X X X X X X X X		
Accountability Network / who when the designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as if governance supply Chain STA-04 STA-04. STA-05.1 Supply Chain STA-05 STA-05.1 Supply Chain STA-05 STA-05.1 Supply Chain STA-05.2 STA-05.2 STA-05.2 STA-05.5 STA-0	Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Security Patches Mobile Security Users Security Indident Security Indident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, Supply Chain	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-04 SEF-05 STA-01 STA-02	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.2 SEF-01.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.2 SEF-03.2 SEF-04.3 SEF-04.3 SEF-04.5 SEF-04.3 SEF-04.1 SEF-05.1	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 Workforce personnel and external business relationships shall consent and/or contractually agree to report all information security events shall be reported through mandafinad communications. channels in a timely manner. 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, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security the types, volumes, and costs of information security Providers shall make security incident information.	od you riaw's a poncy man requires or our oddes' to perform to you rake a plincy man requires or our observations of the properties of the	x x	X X X X X X X X X X X X X X X X X X X		
deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and capacity-level expectations and	Mobile Security Remote Wipe Mobile Security Security Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, E- Supply Chain Management,	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-04 SEF-05 STA-01 STA-02	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.2 SEF-01.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.2 SEF-03.2 SEF-04.3 SEF-04.3 SEF-04.5 SEF-04.3 SEF-04.1 SEF-05.1	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for the BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 Workforce personal 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 is nat timely manner. Information security events in a timely manner. Information security events in a timely manner. 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, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security roviders shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors The provider shall make security incident information Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API)	od you riaw's a poncy man requires or our oddes' to perform to you rake a plincy man requires or our observations of the properties of the	x x	X X X X X X X X X X X X X X X X X X X		
Services Supply Chain STA-04 STA-05 STA-07 S	Mobile Security Remote Wipe Mobile Security Security Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, E- Supply Chain Management, E- Supply Chain Management, Tansparency, and Management, Tansparency, and Management, Tansparency, and Management, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-04 SEF-05 STA-01 STA-02	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.2 SEF-01.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.2 SEF-03.2 SEF-04.3 SEF-04.3 SEF-04.5 SEF-04.3 SEF-04.1 SEF-05.1	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through mandfined communications. channels in a timelu manner. 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, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors The provider's shall make security incident information Business-critical or customer (tenant) impacting (physical designs and configurations, and infrastructure network, and essential configurations, and infrastructure network, and essential configurations, and infrastructure network, and essential configurations, and infrastructure network, and e	odyou riankir a ponicy man requires a rour oddin's to perhomi- boryou riankir a ponicy man requires a rour oddin's to perhomi- tory you make a ponicy man requires a rour oddin to use a min- urboryou may round required by the or opporate or a round per- turboryou may round remained by the or opporate or a round per- turboryou mound resided by the or opporate or a round per- turboryou mound resided by the or opporate or a round per- ducing the or opporate or opporate or opporate or opporate or of the or opporate or of the opporate or of the opporate or of the opporate or object you and the or opporate	x x	X X X X X X X X X X X X X X X X X X X		
Supply Chain STA-05 STA-07 STA	Mobile Security Remote Wipe Mobile Security Security Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, E- Supply Chain Management, E- Supply Chain Management, Tansparency, and Management, Tansparency, and Management, Tansparency, and Management, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-04 SEF-05 STA-01 STA-02	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.2 SEF-01.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.2 SEF-03.2 SEF-04.3 SEF-04.3 SEF-04.5 SEF-04.3 SEF-04.1 SEF-05.1	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall mobile devices onnecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through another of their responsibility and, if required, shall consent and/or contractually agree to report all information security events shall be reported through another an information security events shall be reported through another and information security events and intended and another an information security providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors the provider shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors the provider shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors the provider shall inspect, account for, and don't with their doud supply-chain partners to correct data quality errors the provider shall inspect, account for, and don't with their doud supply-chain partners to correct data quality	odyou riankir a ponicy man requires a rour oddin's to perhomi- boryou riankir a ponicy man requires a rour oddin's to perhomi- tory you make a ponicy man requires a rour oddin to use a min- urboryou may round required by the or opporate or a round per- turboryou may round remained by the or opporate or a round per- turboryou mound resided by the or opporate or a round per- turboryou mound resided by the or opporate or a round per- ducing the or opporate or opporate or opporate or opporate or of the or opporate or of the opporate or of the opporate or of the opporate or object you and the or opporate	x x	X X X X X X X X X X X X X X X X X X X		
STAOS. Staophy Chain Standard Providers shall review the risk management, and support, old and state state shall review the risk management. STAOS. Staophy Chain Metrics Staophy Chain Me	Mobile Security Remote Wige Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Indident Security Indident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, Indident Management Managem	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.2 MOS-9.2 MOS-20.2 SEF-02.3 SEF-02.1 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.2 SEF-04.4 SEF-03.1 SEF-04.5 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.1 SEF-05.1 SEF-05.1 SEF-05.3 SEF-05.2 SEF-05.3 SEF-05.3 SEF-05.3 SEF-05.3 SEF-05.3	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices sometting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a 8YOD-enabled device. Points of contact for applicable regulation authorities, 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 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 is a timely manner. 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 providers shall be put in place to monitor and quantify the types, volumes, and costs of information security providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors. The provider shall make security incident information advised to result information security providers shall make security incident information 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 g	odynomianie a poncy man redulines strout osiles for performit boryour nake a poncy man redulines strout osies to promote the organization of the provide reinforce and the production of the provides and the prov	x x	X X X X X X X X X X X X X X X X X X X		
Accountability That Party Agreements STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.10 STA-07.5 STA-07.6 STA-07.7 STA-07.8 STA-07.8 STA-07.8 STA-07.5 STA-07.5 STA-07.5 STA-07.5 STA-07.7 STA-07.8 STA-07.8 STA-07.8 STA-07.8 STA-07.8 STA-07.8 STA-07.8 STA-07.7 STA-07.7 STA-07.7 STA-07.7 STA-07.7 STA-07.7 STA-07.7 STA-07.7 STA-07.8 STA-07.7 STA-07.7 STA-07.8 STA-07.8	Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Supply Chain Management, Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-01.1 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.1 SEF-03.2 SEF-04.4 SEF-04.5 SEF-04.5 SEF-04.5 SEF-04.1 SEF-05.2 STA-01.1 STA-03.2	all company devices or devices approved for BYOD usage, 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- All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for the BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 in a timely manner. Information security events in a timely manner. 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 inclient. Jop no motification, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security revoiders shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors The provider shall passe caurity incident information Business-critical or customer (tenant) impacting (physical and only incident information. The provider shall make security incident information acqually and the control of the control of the analyse of the control of the control of the analyse of an analyse	odyon-inteke a poncy man redulines or our odeks to perhomi- boryon after a pfinely man redulines or our odeks to perhomi- boryon after a pfinely man redulines or our owns or our own our you make a proper your redulines or our owns or our own outset your in provide reintities which our opporate our ampe- tory don'in thous reduced a miner or remove variation of our of your moune usevices favor our remove variation of our of your moune usevices favor our remove variation of your of your moune usevices favor our remove variation of your of your moune usevices favor our remove variation of your object your brut up binery calmy the systems and services of uboxyour manumassity's any pitch's our our outs your own your own your your your your your your your your	x x	X X X X X X X X X X X X X X X X X X X	у,	
STA-05.5 STA-05.5 Customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure of STA-05.6 STA-05.6 STA-05.6 Customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure of STA-05.6 STA-05.6 Customer (tenant) and any support, roles and responsibilities of provider and usage, feature sets and functionality, personnel and infrastructure of STA-05.5 Under the consideration of STA-05.5 Links of Sta-05.10 STA-05.5 Links of Sta-05.10 STA-05.5 Links of Sta-05.10 STA-05.5 STA-05.5 STA-05.5 STA-05.6 STA-05.5 STA-05.5 STA-05.6 STA-05.5 STA-05.5 STA-05.5 STA-05.6 STA-07.5 STA-07.5 STA-07.5 STA-07.5 STA-07.5 STA-07.6 Customer (tenant) and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAS) STA-07.5 STA-07.5 STA-07.6 STA-07.5 STA-07.6 STA-07.7 STA-07.6 Customer (tenant) and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAS) standard st	Mobile Security Remote Wige Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Indident Security Indident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Transparency, Cloud Management, E- Supply Chain Management, Supply Chain Management, Supply Chain Supply Chain Management, Supply Chain Management, Supply Chain Supply Chain Supply Chain Supply Chain Management, Supply Chain Supply Chain Supply Chain Supply Chain Supply Chain	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.1 SEF-03.2 SEF-04.1 SEF-04.1 SEF-04.1 SEF-05.1 SEF-05.1 SEF-05.2 SEF-05.2 SEF-05.3 SEF-05.3 SEF-04.2 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.3 SEF	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 is a timely manner. Information security events shall be reported through manufactions, channels in a timely manner. 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, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors. The provider shall make security incident information adoption and system-system interface (API) designs and configurations, and intersurutial required for the device of the providers and adoption and system-system interface (API) designs and configurations, and intersurutial relevance and event and systems components, shall be designed, developed, and deployed in acco	odyourisativa poncy mart requires a rour ositiva to perhimit boryourisativa poncy mart requires a rour ositiva to promote the operation of the operation operation of the operation operation of the operation operation operation of the operation op	x x	X X X X X X X X X X X X X X X X X X X	X	
STA-05.6 STA-05.7 STA-05.7 STA-05.8 STA-05.7 STA-05.8 STA-05.7 STA-05.8 STA-05.10 STA-05.5 10 STA-05.5 10 STA-05.5 10 STA-05.5 10 STA-05.5 10 STA-05.10 STA-07.8 ST	Mobile Security Remote Wige Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Indident Security Indident Management, E- Discovery, & Cloud Forensics Security Incident Management E- Discovery, & Cloud Forensics Security Indident Management, E- Supply Chain Management, Supply Chain Management, Supply Chain Management, Supply Chain Supply Chain Management, Supply Chain Management John Managemen	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-01.1 SEF-02.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.5 SEF-02.5 SEF-02.5 SEF-03.1 SEF-03.2 SEF-03.1 SEF-03.2 SEF-04.1 SEF-04.2 SEF-05.2 SEF	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through and the story of the story	odyourisativa poncy mart requires a rour ositiva to perhimit boryourisativa poncy mart requires a rour ositiva to promote the operation of the operation operation of the operation operation of the operation operation operation of the operation op	x x	X X X X X X X X X X X X X X X X X X X	X X X	
STA05.8 support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced of outsourced outsourced of outsourced outso	Mobile Security Remote Wige Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, Transparency, and Accountability Network, Supply Chain Management, Transparency, and Accountability Network, Transparency, and Accountability Management, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.2 MOS-9.2 MOS-20.2 SEF-02.3 SEF-02.1 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.2 SEF-03.3 SEF-04.4 SEF-03.1 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.1 SEF-05.1 SEF-05.1 SEF-05.1 SEF-05.2 SEF-05.3	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through neadsfined communications channels in a timely manner. Information security events is a timely manner. Information security events the relevant jurisdiction after an information security events the relevant jurisdiction after an information security incident to custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident information security Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors. The provider shall make security incident information accurity Providers shall mappet account for, and work with their cloud supply-chain partners to correct data quality errors. The provider shall make security incident information accurity provider information security provider information security provider information security prov	odyooriawira poncy mar requires a roor oddes to perhomi- boryoomake a põincy mar requires a roor oddes to perhomi- boryoomake a põincy mar requires a roor oddes to promote oddes potent il provide fenince wijet of comporare oara wijet oddes potent il provide fenince wijet of comporare oara wijet oddes potent il provide fenince wijet of comporare oara wijet oddes potent il provide fenince wijet of comporare oara wijet oddes potent il provide fenince wijet of comporare oara wijet oddes potent il provide fenince wijet of comporare oara wijet oddes potent il provide fenince wijet of comporare oara wijet oddes your lator poincy pacenty mit oddes vandadorino oddes your lator poincy pacenty mit oddes vandadorino oddes your lator poincy pacenty mit oddes rooks vinta are oddes your lator poincy pacenty mit oddes rooks vinta are oddes your on our poincy pacenty mit oddes repostate plant oddes your lator poincy pacenty mit oddes repostate plant oddes your lator poince pacenty mit oddes repostate plant in revery for cested your security incident response plant revery for cested your security incident response plant oddes workdoor personnel and external business partners to revery for motion personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? oues your mounem response pain comply with mitous time ose or are your capacite of supporting meganorim mous yruces your mounem response pain comply with mitous time oue or over your form in the patentity of the patentity of the providence of the providence of the patentity of the	x x	X X X X X X X X X X X X X X X X X X X	X	IAAS
STA05.8 STA05.9 STA05.9 STA05.9 STA05.10 STA0	Mobile Security Remote Wige Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, Transparency, and Accountability Network, Supply Chain Management, Transparency, and Accountability Network, Transparency, and Accountability Management, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.2 MOS-18.2 MOS-19.2 MOS-9.2 MOS-20.2 SEF-02.3 SEF-02.1 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.2 SEF-03.3 SEF-04.4 SEF-03.1 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.1 SEF-05.1 SEF-05.2 SEF-05.3 SEF-	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall Mobile devices connecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 is a timely manner. Information security events shall be reported through nondefined communications: channels in a Linnaly manner. Information security events is a timely manner. Information security events is not the relevant jurisdiction after an information security events in the relevant jurisdiction after an information account of the relevant jurisdiction after an information security events in the relevant jurisdiction after an information account of the relevant jurisdiction after an information security incident information account of the provider shall be put in place to monitor and quantify the types, volumes, and costs of information security providers shall be put in place t	odyourisate a poncy man requires strour oxides for perform to be your nake a poncy man requires strour oxides to promote the your nake a poncy man requires to our oxides to the your nake a poncy man requires to our oxides to o	x x	X X X X X X X X X X X X X X X X X X X	X	IAAS
STA-05.10 STA-05.51 host of services, and any known regulatory compliance considerations) Supply Chain STA-05.12 Supply Chain STA-07.51 STA-07.51 STA-07.51 STA-07.55 STA-07.55 STA-07.55 STA-07.55 STA-07.55 STA-07.55 STA-07.55 STA-07.6 STA-07.75 STA-07.75 STA-07.76 S	Mobile Security Remote Wige Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, Transparency, and Accountability Network, Supply Chain Management, Transparency, and Accountability Network, Transparency, and Accountability Management, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-01.1 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.2 SEF-03.1 SEF-03.2 SEF-04.1 SEF-04.2 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.2 STA-01.1 STA-03.2 STA-03.2 STA-03.2 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices sometime to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through information security events shall be reported through information security events shall be reported through readefined communications. Annanck in a timely manner. Information security events shall be reported through readefined communications. Annanck in a timely manner. 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, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security. Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality error to report the provider shall make security incident information security in cident information security. The provider shall make security incident information security in cident information security in cident information security in cident information security in cident informati	odyon-inteke a poncy mar redulines a truor usdes the perhami- boryon inteke a policy trian redulines a truor usdes to promise to boryon inteke a policy trian redulines a truor usdes to promise to your area of more water than the provide refinite whigh of comparate cara whigh the provides are transported by the provides and the	x x	X X X X X X X X X X X X X X X X X X X	X	IAAS
Supply Chain STA-05.12 considerations) over the considerations of STA-05.12 considerations over the consideration over the consideration over the cons	Mobile Security Remote Wige Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Incident Reporting Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, I- Transparency, and Accountability Network, Infrastructure Services Supply Chain Management, Transparency, and Accountability Network, Transparency, and Accountability Network, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.1 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-02.3 SEF-02.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.1 SEF-03.3 SEF-04.4 SEF-03.1 SEF-04.1 SEF-04.1 SEF-04.1 SEF-05.1 SEF-05.2 SEF-04.2 SEF-04.3 SEF-05.3 SEF	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall mobile devices onnecting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 is a timely manner. Information security events shall be reported through continuous contractually agree to report all information security events in a timely manner. Information security events in a timely manner. 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 providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors. The providers shall make security incident information security providers shall make security incident information 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. The providers shall perform annual internal assessments of Supply chain agreements (e.g., SLAs) between	odyourianter a poncy man requires a rour oxides to perform to be your anter a poncy man requires a rour oxides to perform to your nate a poncy man requires a rour oxides to the source and to you make a poncy man requires a rour oxides to use a number sour if provide reintote while of compared to a care when the your and the provides reintote while of compared to a compared to your moune userices have the anterior while the contract of your moune userices have the anterior and and only of your moune userices have the restore a share and the oxides and your district or poncy place if you be shared to be your moune userices have the shared to be your moune massible also places to remove the your mention massible also places to remove the your mount massible and points to remove unrocare to your have a documented security incident response plans in your your publisher a rouse and response plans in remove your publisher a rouse and response plans in your your publisher a rouse and response plans in your your publisher a rouse and response plans in your your publisher a rouse your mounter and external business partners to report incidents in a timely manner adhering to popilicable legal, statutory, or regulatory compliance obligations? Does your mounter response pain comply your incident response pain comply your indicatent response and your your your your your your your your	x x	X X X X X X X X X X X X X X X X X X X	X X X	IAAS
Supply Chain STA-06 STA-06 STA-07 STA	Mobile Security Remote Wige Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Incident Reporting Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, I- Transparency, and Accountability Network, Infrastructure Services Supply Chain Management, Transparency, and Accountability Network, Transparency, and Accountability Network, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.1 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.2 SEF-04.4 SEF-04.5 SEF-04.5 SEF-05.2 SEF-05.3 SEF	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for some storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through a shall be information security events is a timely manner. Information security events shall be reported through a required for the presentation of evidence to support optential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors. The provider shall make security incident information security providers and inspect, account for, and work with their cloud supply-chain partners to correct data quality errors the provider shall make security incident information. Business-critical or customer (tenant) inpacting (physical and corfigurations, and infrastructure network and systems components, shall be designed, developed, and deplo	odyon/ranke a poncy man requires servor oxides to perhimitory or make a poncy man requires a root oxides to perhimitory out make a poncy main requires a root oxides to use annework a poncy main requires a root oxides to use annework a poncy main requires a root oxides to use annework a poncy main requires a root oxides to use a new oxides pour rif provide reintox which or oxides a root oxides to use a root oxide to the policy to use a root oxide to the policy to use a root oxide to the policy to use the root oxides to use oxides a root oxide to the policy to policy to use the root oxides to the root oxides to use oxides a root oxide to the root oxides to the root oxides to use oxides a root oxide to the root oxides to root oxi	x x	X X X X X X X X X X X X X X X X X X X	X	IAAS
Supply Chain Management, STA-07 STA-07.2 STA-07.2 STA-07.2 STA-07.3 STA-07.2 STA-07.5 STA-07.5 STA-07.5 STA-07.7 STA-07.7 STA-07.7 STA-07.7 STA-07.7 STA-07.7 STA-07.8 STA-07.8 STA-07.8 STA-07.7 STA-07.7 STA-07.7 STA-07.8 STA-07.8 STA-07.8 STA-07.8 STA-07.7 STA-07.8 STA-07.	Mobile Security Remote Wige Mobile Security Remote Wige Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Incident Reporting Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, I- Transparency, and Accountability Network, Infrastructure Services Supply Chain Management, Transparency, and Accountability Network, Transparency, and Accountability Network, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.3 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.1 MOS-20.1 MOS-20.1 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.1 SEF-04.4 SEF-04.2 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.2 STA-05.3 STA-05.3 STA-05.3 STA-05.5	all company devices or devices approved for BYOD usage, The mobile device policy shall require the BYOD user or perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for the SYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 in a timely manner. Information security events in a timely manner. 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, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors. The provider shall make security incident information. Business-critical or customer (tenant) impacting (physical and ovirtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and usage feature sets and functionality, personnel and infrastructure etwork and systems components for	odyourisele a poncy man requires en or oddes to perform to be your select a poncy man requires or or oddes to perform to be your select a poncy man requires or or oddes to the select and to you nave a poncy man requires or or oddes to use announced to you nave a poncy man requires or or oddes to use announced to your more uservice share the select and select and to you never the select and you have a documented security incident response pain of your or you have a documented security incident response pain or you you have a documented security incident response pains must you you have a documented security incident response pains must you you have a documented security incident response pains must you you never your security incident response pains must you you never your security incident response pains must you you never your security incident response pains must you you you have a documented security incident response pains must you you you have an or several possess your security incident response pains must you you you want you security incident response pains must you you you you want you you want you you want you you want you	x x	X X X X X X X X X X X X X X X X X X X	X	IAAS
Management, SIA07.2 In consistent review of service agreements (e.g., SL45) to strong provides and customers (tenants) across the review of service agreements (e.g., SL45) to strong provides and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews STA07.4 STA07.5 STA07.6 STA07.6 STA07.7 STA07.7 STA07.8 ST	Mobile Security Remote Wipe Mobile Security Security Mobile Security Security Patches Mobile Security Security Incident Security Incident Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, I- Supply Chain Management, I- Supply Chain Management Supply Chain Management Accountability Network Infrastructure Services Supply Chain Management Accountability Network Infrastructure Services Supply Chain Management I ransparency, and Accountability Intrasparency, and Accountability Intra Party Agreements	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-03 STA-04 STA-05	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.1 MOS-20.2 SEF-01.1 SEF-02.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.2 SEF-04.1 SEF-03.2 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.5 SEF-04.3 SEF-05.5 SEF	all company devices or devices approved for BYOD usage, The mobile device policy shall require the BYOD user to the mobile device policy shall require the BYOD user of mapproved application stores, and require the use of anti-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall clarify the systems and servers allowed for use or accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through information security events is a timely manner. Information security events shall be reported through manafedinad communications. channels in a timely manner. 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, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security the contractual pagnation and system-system interface (API) designs and configuration and system-system interface (API) designs and configurations, and infrastructure network and sypication 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 cause	odyon rawie a poncy man redulines serour osies to perhimitory or make a poncy man redulines serour osies to promote the object of the perhimitory of the perhimitory of the perhimitory of the perhitory of the pe	x x	X X X X X X X X X X X X X X X X X X X	X X X	IAAS
Accountability STA-07.4 relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-standard supply chain Metrics STA-07.5 shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least annually and identify non-standard supplements. The reviews shall be performed at least	Mobile Security Remote Wipe Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Incident Reporting Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 STA-01 STA-02 STA-03 STA-05 STA-05 STA-05	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.2 MOS-19.1 MOS-19.1 MOS-20.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.2 SEF-03.1 SEF-03.2 SEF-04.3 SEF-05.2 STA-05.2 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.9 STA-05.11 STA-05.12 STA-05.12 STA-05.11 STA-05.11 STA-05.12 STA-05.11 STA-05.12 STA-05.11 STA-05.11 STA-05.11	all company devices or devices approved for BYOD usage, The mobile device policy shall require the BYOD user to the mobile device policy shall require the BYOD user of mapproved application stores, and require the use of anti-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices sometime to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through information security events shall be reported through manafelinad communications. Annance in a timely manner. Information security events shall be reported through readefined communications. Annance in a timely manner. 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, Mechanisms shall be put in place to monitor and quantify the types, youlmes, and costs of information security? Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors. The provider's shall make security incident information. Business-ritical or customer (tenant) impacting (physical and ovirtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components for service delivery and support, roles and functionality, personned a	odyouriantie a poncy man requires a rour oxides to perform to be your anter a promot make a pinky trant requires a rour oxides to perform to be your anter a promot make a pinky trant requires a rour oxides to trous anter over your make a poncy make requires a rour oxides to trous anter oxides your in provide reintox make the rours oxides your in provide reintox make the rours oxides your in provide reintox make the rours oxides your oxides and the rours of your mount oxides rained the rained the rours of your mount oxides a rour reintox variation of your oxides and the provides and the rours of your mount oxides and your points your points your points your points your points your points of the rour oxides your brough your point your points your points of the rour oxides your brough your point your points your points of the rour oxides your points your points your points your points your points or your points your points or your points your points your points or your points your your points your points your points your your points your your points your your points your your points or your your points your your points your your points your your points your your your your your your your your	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X	IAAS
Supply Chain Metrics STA-07.5 STA-07.6 STA-07.6 STA-07.6 STA-07.8 Inconsistencies resulting from disparate supplier Do you review all service level agreements at least annually? X STA-07.8 STA-07.8	Mobile Security Remote Wipe Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Security Indident Management, E- Discovery, & Cloud Forensics Security Indident Management, E- Discovery, & Cloud Forensics Security Indident Management, E- Supply Chain Management, E- Supply Chain Management, Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services Supply Chain Supply Chain Management, Transparency, and Accountability Train Party Agreements Supply Chain Supply Chain Supply Chain Management, Supply Chain Management, Supply Chain Management, Supply Chain Management, Management, Management, Management, Management, Management, Management, Management,	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 STA-01 STA-02 STA-03 STA-05 STA-05 STA-05	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.1 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.2 SEF-02.3 SEF-02.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.4 SEF-03.1 SEF-03.2 SEF-03.3 SEF-04.4 SEF-03.1 SEF-04.1 SEF-04.1 SEF-04.2 SEF-04.3 SEF-05.1 SEF-05.1 SEF-05.3 SEF-05.2 SEF-05.3 SEF	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for some storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through a shall be information security events shall be reported through candidated normanical final rehannels. In a timely manner. Information security events in a timely manner. Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support optential legal action subject to the relevant jurisdiction, Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors. The provider shall make security incident information 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 systems components (tenants) shall incorporate at least the following mutually agreed upon service and capacity-	odyouriantie a poncy man requires a rour oxides to perform boryouriantie a pointy man requires a rour oxides to perform to oryournate a poncy man requires a rour oxides to the oxide and oxide a poncy man requires a rour oxides to the oxide and oxide a round oxide a round oxide and oxide a round oxide a round oxide and oxide a round oxide a roun	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X	IAAS
STA-07.8 STA-07.8 STA-07.8 STA-07.8 Inconsistencies resulting from disparate supplier Do you'review all service level agreements at least annually? X ISO 9001/27001	Mobile Security Remote Wipe Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, Transparency, and Accountability Transparency, and Accountability Agreements Supply Chain Management, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 STA-01 STA-02 STA-03 STA-05 STA-05 STA-05	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.2 SEF-03.1 SEF-03.2 SEF-03.3 SEF-04.4 SEF-03.1 SEF-03.2 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.2 STA-01.1 STA-05.2 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.6 STA-05.9 STA-05.9 STA-05.9 STA-05.9 STA-05.9 STA-05.9 STA-05.11 STA-05.2 STA-05.11 STA-05.2 STA-05.11 STA-05.2 STA-05.11 STA-05.2 STA-05.11 STA-05.2 STA-05.11 STA-05.2 STA-05.5 STA-05.6 STA-05.5 STA-05.5 STA-05.5 STA-05.6 STA-05.5 STA-05.7 STA-07.3	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through an activity of the shall be reported through a required for the presentation of evidence to support optential legal action subject to the relevant jurisdiction after an information security evident in place to monitor and quantify the types, volumes, and costs of information security providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality error for providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality error 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, and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and usage, feature sets and functionality, personnel and infrastructure netw	odyonisale a poncy man requines actor oxides to perithmit bodyon rake a poncy man requines actor oxides actor oxides to promor over the poncy man requires actor oxides to the oxides actor oxides actor oxides to the oxides actor oxides to the oxides actor oxides to the oxides actor o	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	XXX	IAAS
STA-07.8 inconsistencies resulting from disparate supplier Do you review all service level agreements at least annually? X ISO 9001/27001	Mobile Security Remote Wipe Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, Transparency, and Accountability Transparency, and Accountability Agreements Supply Chain Management, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 STA-01 STA-02 STA-03 STA-05 STA-05 STA-05	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.1 MOS-20.2 SEF-01.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.1 SEF-03.2 SEF-03.1 SEF-03.2 SEF-03.3 SEF	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices sonnecting to corporate networks or storing and accessing company information shall allow for the BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 in a timely manner. 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, Mechanisms shall be put in place to monitor and quantify the types, youlmes, and costs of information security providers shall inspect, account for, and work with their cloud supply-chain inpartners to correct data quality errors. The provider shall make security incident information. 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, personnel and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutual	odyourisely a poncy man requires en our oxides to perform to be your safe a poincy trait requires to rou oxides to perform to be your safe a poincy trait requires to rou oxides to the oxides a poincy main requires to rou oxides to use announced to your safe a poincy main requires to rou oxides to use announced to your moune oxides refer to the whole of the provides remove whether of the provides remove the performance oxides to your moune oxides raised that the performance oxides to your moune oxides raised that the performance oxides to your moune oxides raised that the performance oxides to your moune oxides raised that the performance oxides to your moune oxides raised that the your performance oxides to your moune oxides and your performance oxides to your management oxides to your have a documented security incident response plans from your your publisher a rouse and response plans from the your your performance oxides to your management oxides to your management oxides to your management oxides to your management oxides to your have predefined communication channels for workforce personnel and external business partners to report incidents in a timely management adherent exposition plans from the report incidents in a timely management adherent oxides partners to your substance of their expositions from your your workford oxides to your management response partners that your your your mounter response partners do your short oxides and your workford oxides to your management oxides to your short oxides to your management oxides to your workford oxides to your your your your your your your you	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	XXX	IAAS
Supply Chain STA-08 STA-08 I Providers shall assure reasonable information security	Mobile Security Remote Wipe Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, Transparency, and Accountability Transparency, and Accountability Agreements Supply Chain Management, Transparency, and Accountability	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 STA-01 STA-02 STA-03 STA-05 STA-05 STA-05	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.1 MOS-18.2 MOS-19.1 MOS-20.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.2 SEF-04.4 SEF-04.2 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.2 STA-05.2 STA-05.5 STA-05.5 STA-05.5 STA-05.5 STA-05.10 STA-05.10 STA-05.12 STA-07.3 STA-07.3 STA-07.4 STA-07.3 STA-07.4 STA-07.3 STA-07.4 STA-07.5 STA-07.5 STA-07.3 STA-07.6	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices sometting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 is a timely manner. Information security events shall be reported through information security events is a timely manner. Information security events is a timely manner. Information security events shall be reported through manafedinad romunications. Channels in a timely manner. 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 information security the types, volumes, and costs of information security the device of the provider shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors the provider shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors the provider shall make security incident information security methods and support, roles and configurations, and infrastructure network and systems components for service delivery and support, roles and responsibili	odyonisale a poncy man requines actor oxides to perform to do you make a poncy man requines actor oxides to you sees a up romain to do you make a poncy man requines actor oxides you required to your make a poncy man required actor oxides you required you required to your make a poncy man required your provide remote which or oxides you recover act when you you make be evides amony make the down and you will not you make a constraint of the systems and seeding you you will not polity cathly rich systems and seeding you you will study polity cathly rich systems and seeding you you will study polity cathly rich systems and seeding you you manuam massons and sport oxides to consider a your your manuam massons and you you will study polity cathly rich systems and you you will study polity cathly rich systems and you you will not you you will not you you will not you you will not you you have a documented security incident response plans in you you you will not you you will not you you will not you you will not you will not you you will not you you will not you you will not you will not you you will not you you will not you will not you you you will not you will not you will not you you you will not you will not you you will not you you will not you you will not you required you you will not you you you you will not you	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X	IAAS
	Mobile Security Remote Wipe Mobile Security Remote Wipe Mobile Security Security Patches Mobile Security Users Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Incident Reporting Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Discovery, & Cloud Forensics Security Incident Management, E- Supply Chain Management, Transparency, and Accountability Third Party Agreements Supply Chain Management, Transparency, and Accountability Third Party Agreements	MOS-18 MOS-19 MOS-20 SEF-01 SEF-02 SEF-03 SEF-03 SEF-03 SEF-04 SEF-05 STA-01 STA-02 STA-04 STA-05 STA-07	MOS-16.3 MOS-17.1 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-17.2 MOS-18.2 MOS-19.1 MOS-19.2 MOS-20.2 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-02.3 SEF-03.1 SEF-03.2 SEF-03.1 SEF-03.2 SEF-04.4 SEF-03.1 SEF-03.2 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-04.3 SEF-05.2 SEF-04.3 SEF-05.2 SEF	all company devices or devices approved for BYOD usage, 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-All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall mobile devices permitted for user through the company BYOD program or a company-assigned mobile device shall should device someting to corporate networks or storing and accessing company information shall allow for The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. Points of contact for applicable regulation authorities, 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 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 shall be reported through information security events shall be reported through information security events in a timely manner. Information security events is a timely manner. Information security events shall be reported through readefined communications. Annance in a timely manner. 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, Mechanisms shall be put in place to monitor and quantity the types, volumes, and costs of information security the types, volumes, and costs of information security the expension of vidence to support potential legal action subject to the relevant jurisdiction and carriant language and unspert, according to the provider shall make security incident information. Business-ritical or customer (tenant) inpacting (odynomianie a ponicy man redulines servor osless for perithmit boryour nake a ponicy man redulines a toro osses to promote the organization of the provide reinforce and the organization of the organization	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X	

				Does your annual review include an partners/third-party	L.			
Management,		STA-08.2	across their information supply chain by performing an	Do you mangate ahnuar mormation security reviews and	X			
Supply Chain		STA-09.1	Third-party service providers shall demonstrate	po you make the marting party services comount		Х		
Management,		STA-09.2	compliance with information security and confidentiality,	po you have external time party services conduct		х		
Threat and		TVM-01.1	Policies and procedures shall be established, and	Do you have anti-maiware programs that support or	x			
Vulnerability		TVM-01.2	supporting business processes and technical measures	Do you ensure that security threat detection systems using				
Management			implemented, to prevent the execution of malware on	signatures, lists, or behavioral patterns are updated across				
Antivirus / Malicious			organizationally-owned or managed user end-point	all infrastructure components as prescribed by industry best				
Software			devices (i.e., issued workstations, laptops, and mobile	practices?				
			devices) and IT infrastructure network and systems	II.	X			
Threat and		TVM-02.1	Policies and procedures shall be established, and	DO YOU CONDUCT NETWORK-TAYER VUINERABILITY SCANS REGULARLY DO YOU CONDUCT Application-rayer vulnerability scans	x			
Vulnerability		TVM-02.2	supporting processes and technical measures		x			
Management		TVM-02.3	implemented, for timely detection of vulnerabilities within	DO you'conduct local operating system layer vuliler admity	х			
Vulnerability / Patch		TVM-02.4	organizationally-owned or managed applications,	wnryou mlake the results or Vurier autitry's cans available to		х		
Management		TVM-02.5	infrastructure network and system components (e.g.,	DO you nave a capability to paten vulnerabilities across all of	х			
		TVM-02.6	network vulnerability assessment, penetration testing) to					
			ensure the efficiency of implemented security controls. A					
			risk-based model for prioritizing remediation of identified	Do you inform customers (tenant) of policies and procedures				
			vulnerabilities shall be used. Changes shall be managed	and identified weaknesses if customer (tenant) data is used as				
			through a change management process for all vendor-	part the service and/or customer (tenant) has some shared				
			supplied patches, configuration changes, or changes to the	responsibility over implementation of control?				
			organization's internally developed software. Upon					
			request, the provider informs customer (tenant) of policies		x			
Threat and	TVM-03	TVM-03.1	Policies and procedures shall be established, and	is mobile code authorized before its installation and use,			x	
Vulnerability		TVM-03.2	supporting business processes and technical measures					
Management			implemented, to prevent the execution of unauthorized					
Mobile Code			mobile code, defined as software transferred between					
			systems over a trusted or untrusted network and executed	Is all unauthorized mobile code prevented from executing?				
			on a local system without explicit installation or execution					
			by the recipient on organizationally-owned or managed				x	

by the recipient. on organizationally-owned or managed

© Copyright 2014-2019 Cloud Security Alliance - All rights reserved. You may download, store, display on your
computer, view, print, and link to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire CAIQ
Version 3.0.1" at http://www.coloudsecurityalliance org subject to the following: (a) the Consensus Assessments Initiative
Questionnaire v3.0.1 may be used solely for your personal, informational, non-commercial use; (b) the Consensus
Assessments Initiative Questionnaire v3.0.1 may not be redistributed; and (d) the trademark, copyright or other notices may not be
removed. You may quote portions of the Consensus Assessments Initiative Questionnaire v3.0.1 as permitted by the Fair
Use provisions of the United States Copyright Act provided that you attribute the portions to the Cloud Security Alliance
Cloud Consensus Assessments Initiative Questionnaire 3.0.1 (2014). If you are interested in obtaining a license to this
material for other usages not addressed in the copyright notice, please contact info@cloudsecurityalliance.org.