

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

Control	Control ID	Question	Control Specification	Consoneus Assocsment Questions	Conso	neue Accos	sment Answers	Notes
Domain	Control ID	ID	Control Specification	Consensus Assessment Questions	Yes	No	Not Applicable	Notes
Application & Interface Security	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security	х			
Application Security		AIS-01.2	with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or	for your Systems/Software Development Lifecycle (SDLC)? Do you use an automated source code analysis tool to	х			code quality tool su apposito
		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			docker Merge request su GitLab
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development	X			INCIGE request su diceas
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment	х			
Application & Interface Security		AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed	х			
Customer Access Application &	AIS-03	AIS-02.2 AIS-03.1	regulatory requirements for customer access shall be Data input and output integrity routines (i.e., reconciliation	Are all requirements and trust levels for customers' access 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	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		х		
Application & Interface Security	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include	creasure) imperience to apprecion meriaes and	х			
Data Security / Integrity			(confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.					
			prevent improper discressive, are matter, 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			×		
Audit Planning			reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed					
			upon prior to executing any audits.					
				Do you develop and maintain an agreed upon audit plan (e.g.,				
				scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?				
		AAC-01.2			х			
				Does your audit program take into account effectiveness of implementation of security operations?				
Audit Assurance &	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed	Do you allow tenants to view your SOC2/ISO 27001 or	х			
Compliance Independent Audits		******	at least annually to ensure that the organization addresses nonconformities of established policies, standards,	similar third-party audit or certification reports?	v			VA /07 2040
		AAC-02.2 AAC-02.3	procedures, and compliance obligations.	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			VA/PT 2019 VA/PT 2019
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best	^			VAV 1 2015
		AAC-02.4		practices and guidance?	Х			pianificazione controlli
		AAC-02.5		Do you conduct internal audits at least annually? Do you conduct independent audits at least annually? Are the results of the penetration tests available to tenants.	Х			pianificazione controlli
		AAC-02.6 AAC-02.7		Are the results of the penedation tests available to tenants Are the results of internal and external addits available to bo you have a program in place that includes the ability to		x x		documentazione tecnica documentazione tecnica
Audit Assurance & 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?		x		
Resilience Business Continuity Planning		BCR-01.3	plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the	Do you provide a disaster recovery capability?	x			
- Idminiy		BCR-01.4 BCR-01.5	following: Defined purpose and scope, aligned with relevant	Do you monitor service continuity with upstream providers in the event of provider failure? Do you provide access to operational redundancy reports,	x			
		BCR-01.5	dependencies Accessible to and understood by those who will use	including the services you rely on? Do you provide a tenant-triggered failover option?	x			
		BCR-01.7	them Owned by a named person(s) who is responsible for	20 You browne a renatitatinggered railover option?		x		documentazione tecnica
			their review, update, and approval • Defined lines of communication, roles, and	Do you share your business continuity and redundancy plans with your tenants?				interna
Rucinoss Continuis	BCR-02	BCR-02.1	responsibilities - Datailed resource respondence manual work around - Duringer continuity and security incident response plans	Pare business continuity plans subject to testing at planned	v			
Business Continuity Business Continuity Management &	BCR-02 BCR-03	BCR-02.1 BCR-03.1 BCR-03.2	Business continuity and security incident response plans Data center utilities services and environmental conditions	Does your organization anniere to any international or industry	X X			Service Provider
Operational Resilience		BCR-U3.2	(e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual	Has your organization implemented environmental controls, fail-	^			
Power / Telecommunications			effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed	over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?				
	DCD Cd	BCD C++	with automated fail-over or other redundancies in the	Are information system documents (e.g., administrator and	v			solo a norress susua
Business Continuity Business Continuity	BCR-04 BCR-05	BCR-04.1 BCR-05.1	Information system documentation (e.g., administrator Physical protection against damage from natural causes	is pnysicar camage ancicipated and are countermeasures	Х	V	х	solo a persone qualificate,
Business Continuity Business Continuity	BCR-06 BCR-07	BCR-06.1 BCR-07.1	To reduce the risks from environmental threats, hazards, Policies and procedures shall be established, and	bo'you nave an equipment and datacenter maintenance		^	X	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 X	IAAS IAAS
Business Continuity Management &	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the	Do you use industry standards and frameworks to determine	^			In linea con quanto richiesto dai capitolati di gara
Operational Resilience			organization (cloud provider, cloud consumer) that must incorporate the following:	the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO				
Impact Analysis			Identify critical products and services Identify all dependencies, including processes, Parallestions by least partners, and third partners are least to continue to the continue	and RTO etc) ?				
			applications, business partners, and third party service	L		-		

			■					
		BCR-09.2	providers			x		
			Understand threats to critical products and services Determine impacts resulting from planned or unplanned	Description and the second section of the sect				
			disruptions and how these vary over time	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?				
			Establish the maximum tolerable period for disruption Establish priorities for recovery					
	202.40	202.121	Establish recovery time objectives for recumption of	Are policies and procedures established and made available				
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	Do you nave rec'nnical capabilities to ehrorce renami data	X			
Management &		BCR-11.2	supporting business processes and technical measures	Did you have documented policies and procedures		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	anising grandling as with more interest until strain countries.	x			
Retention Policy		BCR-11.5	procedures, as well as applicable legal, statutory, or	ir usnig virtuar mirastructure, uo you provide tenants with a	X			
		BCR-11.6	regulatory compliance obligations. Backup and recovery	industrial or transfer and are source and will be a fall the same and	Х			
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			Processo di progettazione
Change Control &	CCC-02	CCC-02.1	External business partners shall adhere to the same	Are policies and procedures for change management, release,	X			Processo di progettazione
Configuration		CCC-02.2	policies and procedures for change management, release,	And policies and procedures adequately enforced to ensure od you'llave'a delined quality change cohronal in resting		х		Non esiste attualmente
Change Control & Configuration		CCC-03.1 CCC-03.2	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with	ns accanientation aest no nigrano w missbills wan deration	X	x		
Management		CCC-03.3	established baselines, testing, and release standards which	Are there pondies and procedures in piace to triage and	х			Ticketing, Gitlab issue
Quality Testing		CCC-03.4	focus on system availability, confidentiality, and integrity	po viou navie controis în piace to detect sobrce codê	X			Merge request, Hash della
		CCC-03.5 CCC-03.6	of systems and services.	Are mechanisms in piace to ensure that an dedugging and	X			Merge request
Change Control &	CCC-04	CCC-04.1	Policies and procedures shall be established, and	This very charge regularies in charge and describe and regularity tree	х			Hash della release e relativo
Change Control &		CCC-05.1	Policies and procedures shall be established for managing	DO YOU HAVE POINCIES AND PROCEDURES ESCADIISHED FOR	v	x		Dick accordment 27001
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 &	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a	vo you provide a capability to identity data and nardware vo you provide a capability to identity data and nardware	х			
Information Data Security &	DSI-02	DSI-01.2 DSI-02.1	classification by the data owner based on data type, value, Policies and procedures shall be established, and	vio you inventory, tracantent, and maintain data this was to ""	v		X	
Information	23.02	DSI-02.2	supporting business processes and technical measures	can you'ensure triat data does not ringrate beyond a	X			
Data Security & Information	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that	po you unize open encifyficial frientodologies any time	X			protocollo https
Data Security &	DSI-04	DSI-03.2 DSI-04.1	traverses public networks shall be appropriately classified Policies and procedures shall be established for labeling,	Are polícies and procedures established for data idueling	x			VPN, HTTPS, autenticazione ISO 27001
Information		DSI-04.2	handling, and the security of data and objects which	To you tillow a sufuctured data-labeling standard (e.g., iso Are MeCranisMs for taber fine rifance implemented for		х		
Lifecycle	DCI OF	DSI-04.3	contain data. Mechanisms for label inheritance shall be	ploi yota flave procedures in piace to ensufe plotadiciion uaca		х		ambienti sarrati
Data Security & Data Security &	DSI-05 DSI-06	DSI-05.1 DSI-06.1	Production data shall not be replicated or used in non- All data shall be designated with stewardship, with	Are'tne responsibilities regarding data stewardship defined,	X			ambienti separati previsti ISO 27001
Data Security &	DSI-07	DSI-07.1	Policies and procedures shall be established with	Do you support the secure deletion (e.g.,	х			
Information Lifecycle			supporting business processes and technical measures implemented for the secure disposal and complete	degaussing/cryptographic wiping) of archived and backed-				
Management		DSI-07.2	removal of data from all storage media, ensuring data is	up data? can you provide a published procedure for exiting the	<u> </u>			ISO 27001, CAPITOLATI DI
Datacenter Security	DCS-01	DSI-07.2 DCS-01.1	Assets must be classified in terms of business criticality,	Do you classify your assets in terms or pusifiess chiticality,	X		x	IAAS
Asset Management		DCS-01.2	service-level expectations, and operational continuity	cro you maintain a compete inventory or all or your critical are physical security be inneters (e.g., relices, waits, others,			х	IAAS
Datacenter Security	DCS-02 DCS-03	DCS-02.1 DCS-03.1	Physical security perimeters (e.g., fences, walls, barriers,	Do you have a capability to use system geographic location			X	IAAS IAAS
Datacenter Security Equipment	DCS-03	DCS-03.1 DCS-03.2	Automated equipment identification shall be used as a method of connection authentication. Location-aware	is automáted equipment idéntification used as a metriou to			X	IAAS
Datacenter Security	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or	is authorization obtained prior to relocation or transfer of carryou provide terrants with your dissect management.			х	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	ca'ii you próvide evidence that policies, standards, and			X	IAAS IAAS
Policy	DC3-00	DCS-06.2	supporting business processes implemented, for	carrydu provide évidence that your personner and involved			x	IAAS
Datacenter Security	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and	Are ingress and egress points, such as service areas and			Х	IAAS
Datacenter Security Datacenter Security	DCS-08 DCS-09	DCS-08.1 DCS-09.1	Ingress and egress points such as service areas and other Physical access to information assets and functions by	vớ you restrict physical access to information assets and			X x	IAAS IAAS
Encryption & Key	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to	bo you nave key management policies bildoing keys to		х	^	1100
Encryption & Key		EKM-02.1	Policies and procedures shall be established for the	Do you have a capability to allow creation of unique Do you have a capability to manage encryption keys on		X		
Management Key Generation		EKM-02.2	management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key	habalf af samesta?		x		
,		EKM-02.4	generation to revocation and replacement, public key	Do you maintain key management procedures? Do you mave documented ownership for each stage of the Do you duffize any third party; open source; proprietary		х		
Encounting 9 Key	EKM-03	EKM-02.5	infrastructure, cryptographic protocol design and	Do you encrypt terraint data acress (on diskystorage) within		x		
Encryption & Key Management		EKM-03.2	Policies and procedures shall be established, and supporting business processes and technical measures	DO YOU léverage éfici yption to protect data and virtual		X		
Encryption		EKM-03.3	implemented, for the use of encryption protocols for	po you have good mentation establishing and demning your poyou have platform and data appropriate entrybuor mat		х		
Encryption & Key		EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be	4 114 16 1 14 14 14 14 14	Х	x		
Management Storage and Access		EKM-04.2 EKM-04.3	required. Keys shall not be stored in the cloud (i.e. at the		х			
Storage and Access		EKM-04.3 EKM-04.4	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? Do you nave separate key management and key usage	х	х		
Storage and Access Governance and	GRM-01	EKM-04.3 EKM-04.4 GRM-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for	Do you store encryption keys in the cloud? Do you have separate key management and key usage Do you have uccumented innormation security baselines for	x	х		
Storage and Access	GRM-01	EKM-04.3 EKM-04.4	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? Do you nave separate key management and key usage	x	х		
Governance and Risk Management Baseline Requirements		EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that	Do you store encryption keys in the cloud? Low you have separate key intangement and key usage of you have separate key intangement and key usage of you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	x	x		
Governance and Risk Management Baseline Requirements	GRM-01 GRM-02	EKM-04.3 EKM-04.4 GRM-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance	Do you store encryption keys in the cloud? Do you nave speafare key triansgement and key usage 50 you? have becumented information security desentes for Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Does your organizators risk assessments take mito account Do your conflict has a steeper seemed associated with ordard Do your conflict has a steeper seemed associated with ordard Do your conflict has a steeper seemed associated with ordard	X	x x x		
Governance and Risk Management Baseline Requirements		EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that	Do you store encryption keys in the cloud? DO you have speaked were the supplement and key usage bo you'd have uccumented information security baselines for Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Does your organizations risk assessments take into account boryour conduct has a dissessment assessments take into account Are your dentinari, organies, sind-vaccounter making.	X X X	x		
Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and Governance and	GRM-02	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (SMP)	Do you store encryption keys in the cloud? Do you nave speafare key triansgement and key usage 50 you? have becumented information security desentes for Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Does your organizators risk assessments take mito account Do your conflict has a steeper seemed associated with ordard Do your conflict has a steeper seemed associated with ordard Do your conflict has a steeper seemed associated with ordard	x x x x x	x		
Storage and Access Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and Risk Management	GRM-02 GRM-03 GRM-04	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.2	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and	Do you store encryption keys in the cloud? Do you nave speafare key triansgement and key usage So you have speafare key triansgement and key usage So you have the capability to continuously monitor and poport the compliance of your infrastructure against your information security baselines? Does your organizations risk assessments take into account Doryourconfide! have assessment assessment account are your certain, drossness, into assectated with ruition are your printing; obsenses, into assectanies ruition Doryour priority your infrastructure continuition Doryour priority your infrastructure continuition Doryour priority with your occumentation bescholding Doryour priority your infrastructure continuition.	X X X X X	x		ISO 9001 E 27001
Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and	GRM-02 GRM-03	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.2 GRM-04.1 GRM-04.5 GRM-05.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be	Do you store encryption keys in the cloud? Do you have speafare key triansgement and key usage Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you confidence of your infrastructure against your or your confidence of your infrastructure against your or your province relatines with our commensation treasure. Are your recrimical pushess, and resecutive managers Do you province relatines with our commensation treasure infinity Do seed (fiden and in the management and province in the compliance of the compliance in the compliance of	X X X X X X X X X X X X X X X X X X X	x		ISO 9001 E 27001
Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and Governance and Governance and Governance and Risk Management Governance and Risk Management Risk Management Risk Management	GRM-02 GRM-03 GRM-04 GRM-05	EKM-04.3 EKM-04.4 GRM-01.2 GRM-01.2 GRM-02.1 GRM-02.2 GRM-02.1 GRM-04.1 GRM-04.1 GRM-04.5 GRM-05.1 GRM-06.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that links assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, commented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all	Do you store encryption keys in the cloud? Do you have speafare key triansgement and key usage do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Does your organizations have assessments take mito account overyour conductions have assessments take mito account overyour conductors have assessments asked into account overyour conductors have assessments asked into account overyour certains have assessments askediated with ordata Arte your recrimical outsides, sind executive triansgers out your province relatins with concumeration treasuring out your review your minimation security managediffetit Do execution and international control provinces and province use more your information is executive provinces and province and province and province and province and province of the provinces and provinced user managed in the provinces and	X X X X X X X X X X X X X X X X X X X	x		
Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and	GRM-02 GRM-03 GRM-04 GRM-05	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.2 GRM-04.5 GRM-05.1 GRM-05.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be	Do you store encryption keys in the cloud? Do you have sparature key management and key usage Do'you'n have sparature key management and key usage Do'you'n have the capability to continuously monitor and Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Does your organization's rest assessments taken into account Doe your conduct has a deseasement assessments to over the control of the control o	X X X X X X X X X X X X X X X X X X X	x		
Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Folicy	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.2 GRM-05.1 GRM-06.3 GRM-06.3 GRM-06.3	required. Keys shall not be stored in the cloud (i.e. at the cloud baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable	Do you store encryption keys in the cloud? Do you have speafare key triansgement and key usage of you'd have use capability to continuously monitor and port the compliance of your infrastructure against your information security baselines? Uses your organizations risk assessments take mito account poryourconfulct has assessments assertine account poryourconfulct has assessments assertine account poryourconfulct has assessment assertine account poryour confulct has assessment assertine account poryour confulct has assessment assertine account poryour providences of the confunction of the confuncti	X X X X X X X X X X X X X X X X X X X	x		ISO 27001
Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and Risk Management Governance and Risk Management Folicy Governance and Governance and Risk Management Folicy Governance and Risk Management Folicy	GRM-02 GRM-03 GRM-04 GRM-05	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.2 GRM-05.3 GRM-06.3 GRM-06.3 GRM-06.5 GRM-06.5 GRM-06.5 GRM-06.5	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (SMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable A formal disciplinary or sanction policy shall be established	Do you store encryption keys in the cloud? Do you have spariare key minagement and key usage by dud have becapability to continuously monitor and Do you have the capability to continuously monitor and proport the compliance of your infrastructure against your information security baselines? Do you confide the assessment stake into account Do you confide the assessment assessment stake into account Do your confide the assessment assessment stake into account Do your confide the assessment assessment stake into account Do your confide the assessment assessment assessment Do your confide the assessment assessment assessment Do your provide the assessment assessment assessment Do your confider has assessment assessment assessment Do your not formation assessment assessment Do your mitor fination is county provide in take in orman account for your into fination accounty provide abundated by into the assessment Do you take agreement to density fyour providers abolite Do you take agreement to density for providers abolite Do you take agreement to density for providers abolite Do you do uscobse wince controls, scandards, certification is so do fination assessment or assessment or Do you do uscobse wince controls, scandards, certification is as do fination assessment assessment or prove emproyees a made assessment or prove emproyees a made assessment assessment or prove emprovees a made assessment assessment assessmen	X X X X X X X X X X X X X X X X X X X	x		ISO 27001
Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Risk Management Policy Governance and Governance and Governance and Governance and Governance and Risk Management Policy Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Governance and	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-06.3 GRM-06.5 GRM-06.5 GRM-06.5 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.2	required. Keys shall not be stored in the cloud (i.e. at the cloud baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable	Do you store encryption keys in the cloud? Do you store separate key triansgement and key usage do you'n rave separate key triansgement and key usage do you'n have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and rouse your organizations rask assessments take more account do you'n certificat, outsides, and executive managers Do you'n reviewly odi multimation asset lateful with ruisian vor you'n certificat, outsides, and executive managers Do you'n reviewly odi multimation account/your against the Do you'n reviewly odi multimation account/your against the Too vextedified with intern stantagement care or minar account feer your information security pointless and procedures made are information security and the procedures of the properties of the procedure of the properties of the procedure of the properties of the procedure of the proced	X X X X X X X X X X X X X X X	x		ISO 27001
Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and Governance and Governance and Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Governance and Risk Management Governance and	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.2 GRM-06.3 GRM-06.5 GRM-06.7 GRM-07.2 GRM-07.2 GRM-07.2 GRM-08.1 GRM-08.1 GRM-08.1 GRM-09.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that links assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable for employees who have violated security policies and Risk assessment results shall include updates to security. Ho organization's business leadership (or other accountable for employees who have violated security policies and Risk assessment results shall include updates to security. Ho organization's business leadership (or other accountable for employees who have violated security policies and Risk assessment results shall include updates to security.	Do you store encryption keys in the cloud? Do you have sparature key management and key usage Do'you'n have sparature key management and key usage Do'you'n have uncommented into management and the properties of the company of th	X X X	x		ISO 27001
Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Risk Management Policy Governance and Governance and Governance and Governance and Governance and Risk Management Policy Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Governance and	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-06.3 GRM-06.5 GRM-06.5 GRM-06.5 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.2	required. Keys shall not be stored in the cloud (i.e. at the cloud recourt of the cloud baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable A formal disciplinary or sanction policy shall be established for employees who have violated security policies and Risk assessment results shall include updates to security.	Do you store encryption keys in the cloud? Do you have sparative key management and key usage bo'you' have sparative key management and key usage bo'you' have be capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Dou's your organization's rask assessmens taken mor account to you provide the ske assessment assessmens taken mor account to your provide of the ske assessment assessmens taken mor account to your provide of the ske assessment assessmens taken mor account to your provide of the ske assessment assessmens taken mor account to your provide of the ske assessment assessment assessment the your white and outside the ske assessment	x x	x		ISO 27001
Governance and Risk Management Bovernance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Risk Management G	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-02.2 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-07.2 GRM-07.2 GRM-09.1 GRM-09.2 GRM-09.2 GRM-09.2 GRM-09.2 GRM-09.2 GRM-09.2	required. Keys shall not be stored in the cloud (i.e. at the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be creatablished and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable A formal disciplinary or sanction policy shall be established are shown by the organization's business leadership (or other accountable and Risk assessment results shall include updates to security the organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments hall be performed at least annually or at	Do you store encryption keys in the cloud? Do you have speaked to the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you provide the season that the secondar that the compliance of your provider has assessment asserting account on your confider has assessment asserting account on your provider has assessment asserting asserting and your provider has assessment asserting asserting or your provider has assessment asserting asserting or your provider has a season asserting as a provider and your provider and your provider and the transfer and provider asserting the contrast account for execution and the provider and provider and provider and provider and your telands when your point account your provider and your provider and your telands when your point account your provider and your telands when your point account your provider and your person and your provider and your person	X X X	x		ISO 27001
Governance and Risk Management Baseline Governance and Risk Management Governance and Risk Management Governance and Risk Management Policy Governance and Risk Management Risk Man	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.2 GRM-05.1 GRM-06.3 GRM-06.5 GRM-06.3 GRM-06.5 GRM-07.1 GRM-07.2 GRM-07.1 GRM-09.2 GRM-09.2 GRM-09.1 GRM-09.2 GRM-10.1 GRM-09.2 GRM-10.1 GRM-10.2	required. Keys shall not be stored in the cloud (i.e. at the cloud cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable A formal disciplinary or sanction policy shall be established for employees who have violated security policies and Risk assessment results shall include updates to security. The organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance	Do you store encryption keys in the cloud? Do you have sparaface key management and key usage by you have sparaface key management and key usage by you have sparaface key management and key usage by you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you confide this a desemble associated where usage by your confided has a desemble associated where usage or your proving the sparaface of your monitor associated where usage or your proving your monitor associated where usage or your proving your monitor about security management to be executioned and internating tenter tracer or orman account for your minimization security provinces and procedures make or your historiated internating them tracer orman account for your minimization security provinces and procedures make or your historiated internating them tracer orman account for your minimization security provinces and procedures make or your historiated to design the management in your province and procedures make or your have developed to design the indiging or your or your discount eventure. You can diagence misping or your or your discount of the provinces of the country or your provinces of the provinces of the country or your provinces of the provinces of the country or your provinces of the pr	X X X X	x		ISO 27001
Governance and Risk Management Bovernance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Risk Management G	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-06.5 GRM-06.3 GRM-06.5 GRM-06.5 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-09.2 GRM-10.2 GRM-10.3 GRM-10.3 GRM-10.3 GRM-10.4 GRM-10.3 GRM-10.4 GRM-10.3 GRM-10.4 GRM-10.4 GRM-11.1 GRM-11.2 GRM-11.1	required. Keys shall not be stored in the cloud (i.e. at the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be creatablished and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable A formal disciplinary or sanction policy shall be established are shown by the organization's business leadership (or other accountable and Risk assessment results shall include updates to security the organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments hall be performed at least annually or at	Do you store encryption keys in the cloud? Do you have speafare key triansgement and key usage of you're are papality to continuously monitor and proport the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and proport the compliance of your infrastructure against your information security baselines? Do you have seeing the seeing security baselines? Do you frow the seeing sees the second of the second o	X X X X	x x x		ISO 27001
Governance and Risk Management Bovernance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Human Resources Asset Returns	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-11 HRS-01	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.1 GRM-02.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.2 GRM-05.1 GRM-06.2 GRM-05.1 GRM-06.2 GRM-07.2 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.1 GRM-09.1 GRM-09.2 GRM-10.1 GRM-10.2 GRM-10.1 GRM-10.2 GRM-10.1 GRM-10.1 GRM-10.1 GRM-10.1 GRM-10.1 GRM-10.1 GRM-10.1 GRM-10.1 HRS-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud rovider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable for employees who have violated security policies and Risk assessment results shall include updates to security The organization's business relationships. The organization's business role or function jishall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and Upon termination of workforce personnel and/or	Do you store encryption keys in the cloud? Do you have sparaface key management and key usage by you have sparaface key management and key usage by you have sparaface key management and key usage by you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you confide this a desemble associated where usage by your confided has a desemble associated where usage or your proving the sparaface of your monitor associated where usage or your proving your monitor associated where usage or your proving your monitor about security management to be executioned and internating tenter tracer or orman account for your minimization security provinces and procedures make or your historiated internating them tracer orman account for your minimization security provinces and procedures make or your historiated internating them tracer orman account for your minimization security provinces and procedures make or your historiated to design the management in your province and procedures make or your have developed to design the indiging or your or your discount eventure. You can diagence misping or your or your discount of the provinces of the country or your provinces of the provinces of the country or your provinces of the provinces of the country or your provinces of the pr	X X X X	x x x		ISO 27001
Governance and Risk Management Boseline Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Governance and Risk Management Human Resources Asset Returns	GRM-02 GRM-03 GRM-05 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-06.5 GRM-06.3 GRM-06.5 GRM-06.5 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-09.2 GRM-10.2 GRM-10.3 GRM-10.3 GRM-10.3 GRM-10.4 GRM-10.3 GRM-10.4 GRM-10.3 GRM-10.4 GRM-10.4 GRM-11.1 GRM-11.2 GRM-11.1	required. Keys shall not be stored in the cloud (i.e. at the cloud baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable for employees who have violated security policies and Risk assessment results shall include updates to security. The application of the programization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance tevels based on risk criteria shall be established level. Acceptance tevels based on risk criteria shall be established level. Acceptance tevels based on risk criteria shall be established level. Acceptance tevels based on risk criteria shall be established level. Acceptance tevels based on risk criteria shall be established level. Acceptance tevels based on risk criteria shall be established level. Acceptance tevels based on risk criteria shall be established portion of external business relationships, all	Do you store encryption keys in the cloud? Do you have sparative key management and key usage bo'you' have sparative key management and key usage bo'you' have sparative key management and key usage bo'you' have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you'conduct'h sa' alsessement assessment take mor account Do you'conduct'h sa' alsessement'h assessement take mor account Are your actimation' dostenes, and resecutive management Do you'conduct'h sa' alsessement'h asses roman account Are your actimation's ecurity pionices and procedures manoe Do you'd nake' algerennent o't de instint'you'n proviners adultier Do you'd nake' algerennent o't de instint'you'n proviners adultier Do you'd nake' algerennent o't de instint'you'n proviners adultier Do you'd nake' algerennent o't will account o'co taken' Do you'd nake' algerennent o'n ward' a construction o'co taken' Do you'd nake' algerennent o'co management o'co Do'you'n noun'y bou'r terlants' where you'n make' hateran Do'you ple noun', a't minimirum, annuba redires o't you Do'you'n noun'y bou'r terlants' where you'n make 'hateran Do'you ple noun', a't minimirum, annuba redires o't you Do'you'n noun'y bou'r terlants' where you make 'n erice priser' Do'you'n noun'y bou'r terlants' where you'n make 'n erice priser' Do'you'n noun'y bou'r terlants' where you make 'n erice priser' Do'you'n noun'y bou'r terlants' where you'n make 'n erice priser' Do'you'n noun'y bou'r terlants' where you'n make 'n erice priser' Do'you'n noun'y bou'r terlants' where you'n make 'n erice priser' Do'you'n noun'y bou'r terlants' where you'n n	X X X X	x x x		ISO 27001
Governance and Risk Management Bovernance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Governance and Risk Management Human Resources	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-09 GRM-10 GRM-11 HRS-01	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.5 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-07.2 GRM-07.2 GRM-09.1 GRM-09.2 GRM-10.1 GRM-09.2 GRM-10.1 GRM-10.2 GRM-11.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-03.2	required. Keys shall not be stored in the cloud (i.e. at the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable of remployees who have violated security policies and Risk assessment results shall incude updates to security the organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments hall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established information of workforce personnel and/or terms for adherence to established information all presents thall incorporate provisions and/or terms for adherence to established information.	Do you store encryption keys in the cloud? Do you have spariar key minagement and key usage by your large spariar key minagement and key usage by your large spariar key minagement and key usage by you have the capability to continuously monitor and report the confinence of your infrastructure against your information security baselines? One your organizations reas assessments take mito account purpoyou confided has a sessessment aske mito account purpoyour confided has a sessessment aske mito account your your account and the secondary mind asked to your provided has a sessessment asked to be accounted to your afford material security profiled and procedures make the your afford material security profiled and procedures make the your afford material security profiled and procedures make the your profiled has a sessessment asked by the profiled profiled has a sessessment asked by the your account of a seen of your profiled has a sessessment asked by the your profiled has a sessessment asked by your pro	X X X X X X X X X	x x x		ISO 27001
Governance and Risk Management Boseline Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Policy Governance and Governance and Risk Management Governance and Risk Management Policy Governance and Risk Management Human Resources Asset Returns Human Resources	GRM-02 GRM-03 GRM-05 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.5 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-07.1 GRM-08.1 GRM-09.2 GRM-10.1 GRM-10.2 GRM-10.1 GRM-10.2 GRM-10.1 GRM-11.1 GRM-11.2 GRM	required. Keys shall not be stored in the cloud (i.e. at the cloud baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable has business relationship). Information security or sanction policy shall be established and made readily available for review by all impacted personnel and external business relationships. Information security solicies must be authorized by the organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessment results shall include updates to security. The organization's business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and Upon termination of workforce personnel and/or expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual Employment agreements shall incorporate provisions and/or terms for adherence to established information and/or terms for adherence to established information and/or terms for adherence to established information.	Do you store encryption keys in the cloud? Do you have speaked to the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you provide the season of the compliance of your infrastructure against your information security baselines? Do you provide the season of the season of the compliance of your provided the season of the season of the your control of the season of the season of the your and your provided the season of the season of the your and your provided the season of the your and your provided the season of the your and your provided the your provided they your provided the your provided they your provided the your provided they your provided	X X X X X X X X X X X X X X X X X X X	x x x		ISO 27001
Governance and Risk Management Bovernance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Governance and Risk Management Human Resources	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-09 GRM-10 GRM-11 HRS-01	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.5 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-07.2 GRM-07.2 GRM-09.1 GRM-09.2 GRM-10.1 GRM-09.2 GRM-10.1 GRM-10.2 GRM-11.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-03.2	required. Keys shall not be stored in the cloud (i.e. at the cloud rovider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data powernance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and mad readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership for other accountable A formal disciplinary or sanction policy shall be established of remployees who have violated security policies and Risk assessment results shall include updates to security the organization's business leadership for other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessment shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established into respiration of risk criteria shall be established. In programment of the programment	Do you store encryption keys in the cloud? Do you have speaked to the cloud? Do you have speaked to the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and information security baselines? Do you have the capability to continuously monitor and the control of the cont	X X X X X X X X X	x x x		ISO 27001
Governance and Risk Management Howard Risk Management Human Resources Human Resources Employment Human Resources Human Resources	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01 HRS-02 HRS-03 HRS-04 HRS-05	EKM-04.3 EKM-04.4 EKM-04.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.1 GRM-02.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.2 GRM-05.1 GRM-06.2 GRM-06.3 GRM-06.3 GRM-06.3 GRM-07.2 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.1 GRM-09.1 GRM-09.1 GRM-10.1 GRM-10.2 GRM-10.3 GRM-10.2 GRM-10.3 GRM-10.3 GRM-10.2 GRM-10.3 GRM	required. Keys shall not be stored in the cloud (i.e. at the cloud rovider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and ine management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable for employees who have violated security policies and Risk assessment results shall include updates to security The organization's business relationships. The organization's business relationships and the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and Upon termination of workforce personnel and/or expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual temployment agreements shall incorporate provisions and/or terms for adherence to established information. Roles and responsibilities for performing employment termination or change in employment procedures shall be Policies and procedures shall be established, and	Do you store encryption keys in the cloud? Do you have sparative key management and key usage Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you provide the statement of the stateme	X X X X X X X X X X X X X X X X X X X	x x x		ISO 27001
Governance and Risk Management Human Resources Ausset Returns Human Resources	GRM-02 GRM-03 GRM-05 GRM-05 GRM-06 GRM-07 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-04 HRS-05 HRS-06 HRS-06	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.5 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-07.2 GRM-07.2 GRM-07.2 GRM-08.3 GRM-09.1 GRM-09.1 GRM-10.1 GRM-10.2 GRM-10.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-04.2 HRS-04.1 HRS-04.1 HRS-05.1	required. Keys shall not be stored in the cloud (i.e. at the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable A formal disciplinary or sanction policy shall be established for employees who have violated security policies and Risk assessment results shall incude updates to security. The organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitting at least annually or at Risks shall be mitting the established information of external business relationships, all Upon termination of workforce personnel and/or expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual Employment agreements shall incorporate provisions and/or terms for adherence to established information Roles and responsibilities for performing employment termination or change in employment procedures shall be established from and or change in employment procedures shall be reformed to change in employment procedures shall be folicies and procedures shall be established formation.	Do you store encryption keys in the cloud? Do you have sparative key management and key usage Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you provide the statement of the stateme	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		ISO 27001
Governance and Risk Management Bovernance and Risk Management Governance and Governance and Governance and Governance and Governance and Risk Management Human Resources Asset Returns Human Resources Employment Human Resources Employment Human Resources	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01 HRS-02 HRS-03 HRS-04 HRS-05	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.5 GRM-07.1 GRM-06.3 GRM-07.1 GRM-07.1 GRM-08.1 GRM-08.1 GRM-09.2 GRM-09.1 GRM-10.2 GRM-10.1 GRM-10.2 GRM-10.3 GRM	required. Keys shall not be stored in the cloud (i.e. at the cloud rovider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that linfastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable for employees who have violated security policies and Risk assessment results shall include updates to security The organization's business sleadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and Upon termination of workforce personnel and/or expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual temployment agreements shall incorporate provisions and/or terms for adherence to established information Roles and responsibilities for performing employment termination or change in employment procedures shall be Policies and procedures shall be established, and	Do you store encryption keys in the cloud? Do you have speaked to the control of the cloud? Do you have the capability to continuously monitor and report the configuration of the control of the contr	X X X X X X X X X X X X X X X X X X X	x x x		ISO 27001
Governance and Risk Management Boseline Governance and Risk Management Human Resources Asset Returns Human Resources	GRM-02 GRM-03 GRM-05 GRM-05 GRM-06 GRM-07 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-04 HRS-05 HRS-06 HRS-06	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-06.5 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.5 GRM-07.2 GRM-06.3 GRM-07.2 GRM-07.2 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.2 GRM-10.1 GRM-11.2 GRM-11.1 GRM-11.2 HRS-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that filks assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and Upon termination of workforce personnel and/or expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual Employment agreements shall incorporate provisions and/or terms for adherence to established information. Roles and responsibilities for performing employment termination or change in employment procedures shall be efforted the established, and Requirements for non-disclosure or confidentiality. Roles and responsibilities for performing employment agreements for non-disclosure or confidentiality. Roles and responsibilities for performing employment agreements for non-disclosure or confidentiality. Roles and responsibilities of northerous established, and supporting business processes and technical be established, and supporting business processes and technical measures.	Do you store encryption keys in the cloud? Do you have speaked to the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you remained the speaked of the compliance of your infrastructure against your information security baselines? Do you remained the speaked of the compliance of your infrastructure against your information security baselines? Do you remained the speaked of the speaked of the compliance of your mornitation assection the speaked of the compliance of your mornitation recurry principles and procedures make only do you remained the processing of the compliance of your information in the maintaigent relative to the speaked of the compliance of your information is courtly pointed and procedures make only only of the compliance of your information is courtly pointed and procedures make only only of the compliance of your information is courtly pointed to design the fingling or your or you do used the white of your years and the court your formation security pointed to the speaked of your years and the court your formation of the court of your demander of your personnel or make the your personnel or the court of the court of your personnel or the court of your personnel or the court of your personnel or your make it bucumented, organization water or your and a speaked of your personnel or your provide or your personnel or process of your personnel or process or your personnel or pro	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		ISO 27001
Governance and Risk Management Governance and Risk Management Baseline Requirements Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Governance and Governance and Risk Management Human Resources Human	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-01.2 GRM-02.1 GRM-02.1 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.2 GRM-06.3 GRM-06.5 GRM-06.3 GRM-06.5 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-09.1 GRM-10.1 GRM-10.2 GRM-11.1 GRM-10.2 GRM-11.1 HRS-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data powernance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and ine management shall take formal action to Information security policies and procedures shall be established and mad readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership for other accountable A formal disciplinary or sanction policy shall be established of remployees who have violated security policies and Risk assessment results shall include updates to security the organization's business leadership for other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessment results shall be established unto the complex shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established, and Upon termination of workforce personnel and/or terms for adherence to established information and/or terms for adherence to established information and/or terms for adherence to established information and/or terms for adherence to established, and Pursuant to local laws, regulations, ethics, and contractual Employment agreements shall be established, and Supporting business processes and technical measures. A security awareness training program shall be established, and supporting business processes and technical measures.	Do you store encryption keys in the cloud? Do you have speaked to the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you remained the speaked of the compliance of your infrastructure against your information security baselines? Do you remained the speaked of the compliance of your infrastructure against your information security baselines? Do you remained the speaked of the speaked of the compliance of your mornitation assection the speaked of the compliance of your mornitation recurry principles and procedures make only do you remained the processing of the compliance of your information in the maintaigent relative to the speaked of the compliance of your information is courtly pointed and procedures make only only of the compliance of your information is courtly pointed and procedures make only only of the compliance of your information is courtly pointed to design the fingling or your or you do used the white of your years and the court your formation security pointed to the speaked of your years and the court your formation of the court of your demander of your personnel or make the your personnel or the court of the court of your personnel or the court of your personnel or the court of your personnel or your make it bucumented, organization water or your and a speaked of your personnel or your provide or your personnel or process of your personnel or process or your personnel or pro	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		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Boseline Governance and Risk Management Human Resources Asset Returns Human Resources	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-06.5 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.5 GRM-07.2 GRM-06.3 GRM-07.2 GRM-07.2 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.2 GRM-10.1 GRM-11.2 GRM-11.1 GRM-11.2 HRS-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that filks assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and Upon termination of workforce personnel and/or expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual Employment agreements shall incorporate provisions and/or terms for adherence to established information. Roles and responsibilities for performing employment termination or change in employment procedures shall be efforted the established, and Requirements for non-disclosure or confidentiality. Roles and responsibilities for performing employment agreements for non-disclosure or confidentiality. Roles and responsibilities for performing employment agreements for non-disclosure or confidentiality. Roles and responsibilities of northerous established, and supporting business processes and technical be established, and supporting business processes and technical measures.	Do you store encryption keys in the cloud? Do you have sparadrax key management and key usage by your love sparadrax key management and key usage by your love sparadrax key management and key usage by your love of the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Dour your conduct has a desense assessment taken mor account purpose the control of th	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		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Boseline Governance and Risk Management Human Resources Asset Returns Human Resources	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-01.2 GRM-02.1 GRM-02.1 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.2 GRM-06.3 GRM-06.5 GRM-06.3 GRM-06.5 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-09.1 GRM-10.1 GRM-10.2 GRM-11.1 GRM-10.2 GRM-11.1 HRS-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable A formal disciplinary or sanction policy shall be established for employees who have violated security policies and Risk assessment sesults shall incude updates to security. The organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitted at least annually or at Risks shall be mitted at least annually or at Risks shall be mitted at least annually or at Risks shall be mitted at least annually or at Risks shall be reformed at least annually or at Risks shall be performed at least annually or at Risks shall be performed the established and Upon termination of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual Employment agreements shall incorporate provisions and/or terms for adherence to established information Roles and responsibilities for performing employment procedures shall be established, and Requirements for non-disclosure or confidentiality. Roles and responsibilities of contractors, employees, and Policies and procedures shall be establish	Do you store encryption keys in the cloud? Do you have sparadrax key imagement and key usage Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you provide the spanning of the spanning of the providence of the compliance of your infrastructure against your information security baselines? Do you provide the spanning of the spanning of the providence of the compliance of your your providence training to spanning or your or your providence training to the providence of the your providence training to the your providence of the 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		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Baseline Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Hollow Governance and Risk Management Hollow Rovernance and Risk Management Human Resources Auman Resources Employment Human Resources Employment Human Resources Employment Human Resources Training / Awareness	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08 HRS-09	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-01.2 GRM-02.1 GRM-02.1 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.2 GRM-06.3 GRM-06.5 GRM-06.3 GRM-06.5 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-09.1 GRM-10.1 GRM-10.2 GRM-11.1 GRM-10.2 GRM-11.1 HRS-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that links assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable for employees who have violated security policies and for employees who have violated security policies and Risk assessment results shall include updates to security The organization's business relationships. The organization's business relationships and the process of the program and the established for all contractors, third-party users, and employees of the organization and mandated when appropriate established for all contractors, third-party users, and employees of the organization and mandated when appropriate established for all contractors, third-party users, and employees of the organization and mandate	Do you store encryption keys in the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your infrastructure asserting the county of the control of the county of t	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		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Boseline Governance and Risk Management Human Resources Asset Returns Human Resources	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08	EKM-04.3 EKM-04.4 EKM-04.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.1 GRM-02.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-05.1 GRM-05.1 GRM-05.1 GRM-06.2 GRM-06.3 GRM-06.3 GRM-06.3 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.1 GRM-09.1 GRM-10.1 GRM-10.1 GRM-10.2 HRS-01.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-04.1 HRS-04.1 HRS-05.1 HRS-09.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable of the component of the c	Do you store encryption keys in the cloud? Do you have sparative key imagement and key usage bo'you' have sparative key imagement and key usage bo'you' have occumented into manaton security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you's review of the statement of the sparation of the statement of the statement of the sparation of the statement of the statement of the sparation of the statement of the statement of the statement of the statement of the sparation of the statement of the statement of the sparation of the statement of	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		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Governance and Risk Management Baseline and Risk Management Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Governance and Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Human Resources Human Resourc	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-10 GRM-11 HRS-01 HRS-02 HRS-03 HRS-04 HRS-05 HRS-07 HRS-08 HRS-09	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.5 GRM-06.5 GRM-06.5 GRM-06.3 GRM-06.5 GRM-07.2 GRM-06.3 GRM-06.3 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.2 GRM-10.1 GRM-09.2 GRM-10.1 GRM-10.2 GRM-10.1 GRM-10.2 GRM-10.1 GRM-10.2 GRM-10.1 GRM-10.3 GRM	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and ine management shall take formal action to Information security policies and procedures shall be established and mad readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable A formal disciplinary or sanction policy shall be established of remployees who have violated security policies and Risk assessment results shall include updates to security The organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessment shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptane levels based on risk criteria shall be established and Upon termination of workforce personnel and/or terms for adherence to established information and/or terms for adherence to established information and/or terms for adherence to established information and responsibilities for performing employment termination or change in employment procedures shall be established, and Supporting business processes and technical measures A security avareness training and regular updates in organizational rockedures shall be established and supporting business processes and technical measures A security avareness training and regular update	Do you store encryption keys in the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your infrastructure asserting the county of the control of the county of t	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		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Governance and Governance and Risk Management Human Resources Human Reso	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08 HRS-09	EKM-04.3 EKM-04.4 EKM-04.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-05.1 GRM-06.2 GRM-05.1 GRM-06.2 GRM-06.3 GRM-06.3 GRM-07.2 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.1 GRM-09.1 GRM-09.2 GRM-11.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-04.2 HRS-04.1 HRS-05.1 HRS-06.1 HRS-07.1 HRS-07.1 HRS-08.1 HRS-09.3 HRS-09.2 HRS-09.3 HRS-09.9 HRS-09.9 HRS-09.9 HRS-09.9 HRS-09.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable of the component of the c	Do you store encryption keys in the cloud? Do you have store encryption keys in the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against 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 X X X X X X X X X X X X X X X X X		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Baseline Governance and Risk Management Human Resources Aussel Returns Human Resources Hum	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-10 GRM-11 HRS-01 HRS-02 HRS-03 HRS-04 HRS-05 HRS-07 HRS-08 HRS-09	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.5 GRM-06.3 GRM-07.2 GRM-07.2 GRM-07.2 GRM-10.1 GRM-10.2 GRM-10.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-03.2 HRS-04.2 HRS-04.2 HRS-04.1 HRS-06.1 HRS-06.1 HRS-06.1 HRS-07.1 HRS-08.2 HRS-09.3 HRS-09.1 HRS-10.1 HRS-10.1 HRS-10.1 HRS-10.1 HRS-10.1	lequired. Keys shall not be stored in the cloud (i.e. at the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that fisk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security physical policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership for other accountable. A formal disciplinary or sanction policy shall be established are only as the security and the set of the security and the security policies and Risk assessment results shall include updates to security. The organization's business leadership for other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments rall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established information and upon termination of workforce personnel and/or expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual Employment agreements shall incorporate provisions and/or terms for adherence to established information Roles and responsibilities for performing employment termination or change in employment procedures shall be established for all contractual employment procedures shall be established, and Requirements for non-disclosure or onfidentially exponsibilities of rotharctors, employees, and responsibilities for contractors, employees, and responsibilities for contra	Do you store encryption keys in the cloud? Do you have store encryption keys in the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? Do you remain a security baselines? Do you remain a security baselines? Do you remain a security baselines? Do you provide the security baselines are provided to you you remain out you will be security baselines? Do you there a security baselines? Do you there a security baselines are provided the your and the security baselines are provided to you you remain out you will be security by poncess advantated by one or you thank a security poncess advantated by one or you thank a security poncess advantated by one or you thank a security poncess advantated by one or you thank a security poncess advantated by one or you thank a security poncess advantated by one or you thank a security poncess advantated by one or you thank a security poncess advantated by one or you will be security as a security of your thank and will be security or you you will be security or you you will be security or you wi	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		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Baseline Governance and Risk Management Governance and Risk Management Governance and Governance and Governance and Governance and Risk Management Governance and Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Human Resources Acceptable Use Human Resources Hu	GRM-02 GRM-03 GRM-04 GRM-05 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08 HRS-09 HRS-09 HRS-09	EKM-04.3 EKM-04.4 EKM-04.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.1 GRM-02.1 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-05.1 GRM-06.2 GRM-05.1 GRM-06.5 GRM-06.3 GRM-06.5 GRM-07.2 GRM-06.5 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.1 GRM-09.1 GRM-09.1 GRM-10.1 GRM-10.2 GRM-10.2 GRM-10.3 GRM-10.3 GRM-10.3 GRM-10.3 GRM-10.3 GRM-10.3 GRM-10.2 GRM-10.3 GRM	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and inle management shall take formal action to information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable for employees who have violated security policies and Risk assessment results shall include updates to security The organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be until the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and Upon termination of workforce personnel and/or expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual temployment agreements shall incorporate provisions and/or terms for adherence to established information. Roles and responsibilities of performing employment termination or change in employment procedures shall be organization and mandated when appropriate, All Pursuant to local laws, regulations, ethics, and contractual policies and procedures shall be established, and supporting business processes and t	Do you store encryption keys in the cloud? Do you have store encryption keys in the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against 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 X X X X X X X X X X X X X X X X X		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Baseline Governance and Risk Management Human Resources Aussel Returns Human Resources Hum	GRM-02 GRM-03 GRM-04 GRM-05 GRM-06 GRM-07 GRM-09 GRM-10 GRM-11 HRS-01 HRS-02 HRS-03 HRS-04 HRS-04 HRS-09 HRS-09	EKM-04.3 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.5 GRM-06.3 GRM-07.2 GRM-07.2 GRM-07.2 GRM-10.1 GRM-10.2 GRM-10.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-01.1 HRS-03.2 HRS-04.2 HRS-04.1 HRS-04.2 HRS-04.1 HRS-06.1 HRS-06.1 HRS-07.1 HRS-08.2 HRS-09.3 HRS-09.1 HRS-10.1 HRS-10.1 HRS-10.1 HRS-10.1 HRS-10.1	lequired. Keys shall not be stored in the cloud (i.e. at the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that fisk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, an information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to information security physical policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership for other accountable. A formal disciplinary or sanction policy shall be established are only as the security and the set of the security and the security policies and Risk assessment results shall include updates to security. The organization's business leadership for other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments rall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established information and upon termination of workforce personnel and/or expiration of external business relationships, all Pursuant to local laws, regulations, ethics, and contractual Employment agreements shall incorporate provisions and/or terms for adherence to established information Roles and responsibilities for performing employment termination or change in employment procedures shall be established for all contractual employment procedures shall be established, and Requirements for non-disclosure or onfidentially exponsibilities of rotharctors, employees, and responsibilities for contractors, employees, and responsibilities for contra	Do you store encryption keys in the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your lower your procedure has a sessessmens take into account 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		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Baseline Governance and Risk Management Human Resources Hu	GRM-02 GRM-03 GRM-04 GRM-05 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08 HRS-09 HRS-09 HRS-09	EKM-04.3 EKM-04.4 EKM-04.1 GRM-01.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.5 GRM-06.5 GRM-06.5 GRM-06.5 GRM-06.5 GRM-07.2 GRM-06.5 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.2 GRM-10.1 GRM-09.2 GRM-10.1 HRS-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that fisk assessments associated with data powernance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and ine management shall take formal action to Information security policies and procedures shall be catablished and mad readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership for other accountable A formal disciplinary or sanction policy shall be established of remployees who have violated security policies and Risk assessment results shall include updates to security The organization's business leadership for other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessment results shall include updates to security the organization's business leadership for other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptane levels based on risk criteria shall be established and Upon termination or risk criteria shall be established and Upon termination or hange in employment procedures shall be established and Porterna for adherence to established information and responsibilities for performing employment for clarge and procedures shall be established, and supporting business processes and technical measures and responsibilities for con	Do you store encryption keys in the cloud? Do you have the capability to continuously monitor and report the configuration are occurrent uncommended to you have the capability to continuously monitor and report the configuration are over infrastructure against your information security baselines? Do you have the capability to continuously monitor and report the configurations are sensitive as a session of the configuration of the configu	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		ISO 27001 Informativa e gestione degli Informativa e gestione degli
Governance and Risk Management Baseline Governance and Risk Management Governance and Risk Management Human Resources Acceptable Use Human Resources Employment Human Resources Human Re	GRM-02 GRM-03 GRM-04 GRM-05 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08 HRS-09 HRS-09 HRS-09	EKM-04.3 EKM-04.4 EKM-04.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.2 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.5 GRM-06.3 GRM-07.2 GRM-07.2 GRM-08.1 GRM-09.2 GRM-10.1 HR-09.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that links assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and line management shall take formal action to Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable of the management propers of the component of the componen	Do you store encryption keys in the cloud? Do you have store encryption keys in the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information assessment ass	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		ISO 27001 Informativa e gestione degli Informativa e gestione degli FORMAZIONE
Governance and Risk Management Baseline Governance and Risk Management Governance and Risk Management Human Resources Acceptable Use Human Resources Employment Human Resources Human Re	GRM-02 GRM-03 GRM-04 GRM-05 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08 HRS-09 HRS-09 HRS-09	EKM-04.3 EKM-04.4 EKM-04.1 GRM-01.1 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.1 GRM-02.2 GRM-03.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-06.5 GRM-06.5 GRM-06.5 GRM-06.5 GRM-06.5 GRM-07.2 GRM-06.5 GRM-07.2 GRM-08.1 GRM-09.1 GRM-09.2 GRM-10.1 GRM-09.2 GRM-10.1 HRS-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that fisk assessments associated with data powernance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and ine management shall take formal action to Information security policies and procedures shall be catablished and mad readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership for other accountable A formal disciplinary or sanction policy shall be established of remployees who have violated security policies and Risk assessment results shall include updates to security The organization's business leadership for other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessment results shall include updates to security the organization's business leadership for other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptane levels based on risk criteria shall be established and Upon termination or risk criteria shall be established and Upon termination or hange in employment procedures shall be established and Porterna for adherence to established information and responsibilities for performing employment for clarge and procedures shall be established, and supporting business processes and technical measures and responsibilities for con	Do you store encryption keys in the cloud? Do you have the capability to continuously monitor and 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 X X X X X X X X X X X X X X X X X		ISO 27001 Informativa e gestione degli Informativa e gestione degli FORMAZIONE
Governance and Risk Management Basseline Requirements Governance and Risk Management Risk Management Governance and Governance and Governance and Governance and Risk Management Governance and Risk Management Governance and Risk Management Governance and Risk Management Hollow Management Governance and Risk Management Hollow Management Hollow Management Human Resources Acceptable Use Human Resources Human Resour	GRM-02 GRM-03 GRM-04 GRM-05 GRM-05 GRM-06 GRM-07 GRM-08 GRM-09 GRM-10 GRM-11 HRS-01 HRS-03 HRS-04 HRS-05 HRS-06 HRS-07 HRS-08 HRS-09 HRS-09 HRS-09	EKM-04.3 EKM-04.4 EKM-04.4 GRM-01.1 GRM-01.2 GRM-02.1 GRM-02.1 GRM-02.1 GRM-03.1 GRM-04.1 GRM-04.1 GRM-04.1 GRM-05.1 GRM-05.1 GRM-06.2 GRM-06.2 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.3 GRM-06.5 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-07.2 GRM-08.1 GRM-09.1 GRM-10.1 GRM-10.2 GRM-11.1 HRS-01.1	required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that infrastructure system, and network components that Risk assessments associated with data governance requirements shall be conducted at planned intervals and Managers are responsible for maintaining awareness of, An Information Security Management Program (ISMP) shall be developed, documented, approved, and Executive and ine management shall take formal action to Information security policies and procedures shall be established and mare readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable A formal disciplinary or sanction policy shall be established for employees who have violated security policies and Risk assessment results shall include updates to security The organization's business leadership (or other accountable business role or function) shall review the Aligned with the enterprise-wide framework, formal risk assessment shall be performed at least annually or at Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and Upon termination or risk criteria shall be established and Upon termination or change in employment procedures shall be established and Popularity of external business relationships, all pursuant to local laws, regulations, ethics, and contractual imployment agreements shall incorporate provisions and/or terms for adherence to established information. Roles and responsibilities for: A security awareness training program shall be established for all contravactors, third-party users, and employees of the organization and amandated when appropriate. All individuals with a	Do you store encryption keys in the cloud? Do you have store encryption keys in the cloud? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information assessment ass	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		ISO 27001 Informativa e gestione degli Informativa e gestione degli FORMAZIONE

March Marc	Identity & Access	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be	is user access to diagnostic and configuration ports restricted	Х			
And Company	Identity & Access		IAM-04.1	Policies and procedures shall be established to store and	bo you manage and store the identity of an personner who	Х			
See 1. 19. 19. 19. 19. 19. 19. 19. 19. 19.		1444.05				Х	l.		COMPETENZE
Mary						x	^		
March Marc			IAM-06.2			X			
Company		IAM-07		The identification, assessment, and prioritization of risks	Does your organization conduct third-party unauthorized	Х			
March Marc			IAM-07.2						
March Marc	Third Party Access					v			
March Marc	Identity & Access	IAM-08	IAM-08.1			X			
March Marc	Management								
March Marc									
March Marc		IAM-09				X V			
March Marc		IAM-10				X			
March Marc	Management					х			gestione incidenti di
March Marc	User Access Reviews					Х			
Marchael	Idontitu 9 Accoss	1004.11			yeur tananta, if inconcentrate assess may have been allowed to				COMUNICAZIONE AL
March Marc		IAIVI-11			is any charlige in user access status interfued to include				
Part		IAM-12				Х			
Part						X			
Proceedings Process	User ID Credentials				DO You Have a Policy Enforcement Point Capability (e.g.,	Х	v		IDENTITY PROVIDER IN
March Marc							x		
Mary			IAM-12.6			х			
Section						X			LDAP, SSO AZIENDALI
March Marc						x			
Management March						X			
West				Account credential and/or identity store minimization or		Х			
March Marc	Identity & Access		IAM-13.1			Х			
March	Infrastructure &		IVS-01.1			Y	IX.		
Company Comp			110 02.2			^	x		
Authoritions of the control of the c			113 02.4	compliance obligations and providing unique user access	Are audit logs centrally stored and retained?	Х			
Security (1997) 1992 1992	Intrusion Detection		110 02.0						
The color of the									
Secretary 19 (1997) 19 (19					And changes made to virtual macmines, or moving or an				
Marchael		IVS-03				х			
March		IVS-04		The availability, quality, and adequate capacity and				х	
Section of the control of the contro					. ,	V		х	
And section (1997) 1999 1999 1999 1999 1999 1999 1999					rs system perrormance monitorea ána tanéa in order to	X			SAR SUI SERVIZI (VAA) E
Security (1997) Wheel to security (1997) W		IVS-05						х	S. J. SO. SERVICE (VIVI) E
Security (Controlled in Controlled in Contro	Infrastructure &		IVS-06.1	Network environments and virtual instances shall be				х	
Comment of the Commen								X	
Section of the components of t								X X	
Missachura Mis		IVS-07	IVS-07.1			Х			
Security of the control of the contr		IVS-08	IVS-08.1			х			
March Marc			IVS-08.2				х		
Minimum		11/5-00	IVS-08.3			X			
			IVS-09.2			X			
Tresposations & 19-20 (19-20) The content was access a supported from the following of the content of the conte	Security		IVS-09.3			Х			
Service of the control of the contro	Segmentation		IVS-09.4			Х			
Nominations (1961) (1961) (1962) (196	Information 0	11/0 40	IVS-09.5		Green serior en la contraction de la contraction	X			
Interpretative (1962)	Intrastructure &		172-10.1	Secured and encrypted communication channels shall be		^			
The comments of the comments o	Virtualization		IVS-10.2	used when migrating physical servers, applications, or data		X			
Security 19-12 1	Infrastructure &	IVS-11	IVS-11.1		por you'resther personner access to an hypervisor time.	X X			
Interspectability & 197.01 PP-013. The provider and sea of early deathly give to provide a consistent of early give to provide a consistent of e	Infrastructure &	140 11	IVS-11.1 IVS-12.1	Access to all hypervisor management functions or Policies and procedures shall be established, and	ne policies aria procedures éstabilismeu ana metrafilisms	X X			
Visual Interceptability Visual Prof. Prof. 1 Prof. Prof. 2 Prof.	Infrastructure & Virtualization	140 11	IVS-11.1 IVS-12.1 IVS-12.2	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures	pot you'reschec peisonhier access to an nypervisor " Are poinces and procedures established and mechanisms Are poinces and procedures established and mechanisms	X X			
Interogeneithy & IPV01 PV01 PV01 PV01 PV01 PV01 PV01 PV01	Infrastructure & Virtualization Security	IVS-12	IVS-11.1 IVS-12.1 IVS-12.2 IVS-12.3	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments,	DO you'rescher peisonlier access to an myperosion' whe poinces and procedures estabilished and methanisms were poincies and procedures estabilished and methanisms were poincies and procedures estabilished and methanisms were poincies and procedures estabilished and methanisms but your network architecture diagrams cleanly identify ingin-	X X	X		
Interceptability & IPP-G31 PPG-11 PPG-12 PPG	Infrastructure & Virtualization Security Infrastructure &	IVS-12	IVS-11.1 IVS-12.1 IVS-12.2 IVS-12.3 IVS-13.1	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high- risk environments and data flows that may have legal	od you'rescher, peisonine access to an nyperosoti ner ponces and procedures estationiste and metrianisms ner ponces and procedure's estationiste and metrianisms ner ponces and procedure's estationiste and metrianisms ner ponces and procedure's estationiste and metrianisms ou you metvion a architecture's dearning centry memory in do you'mignement rechinic affirmeastics and apply dereitsemment of you'mignement rechinic affirmeastics and apply dereitsemment.	X X	X X		
Processing Processor Services of the control of the	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability &	IVS-12 IVS-13 IPY-01	IVS-11.1 IVS-12.1 IVS-12.2 IVS-12.3 IVS-13.1 IVS-13.2 IPY-01.1	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting husiness processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high- risk environments and data flows that may have legal The provider shall use open and published APIs to ensure	od you'reschor, peisonine adoes to an insperiodor in the policies and procedures established and medicinisms are poincies and procedures established and medicinisms are poincies and procedures established and medicinisms are poincies and procedures established and infectanisms to your network actinitecture diagrams cleanly deprive to you imprement rechinical measures and apply developed to you do publism and to all a reas available from established to you do publism and to all a reas available from established to the procedure of the procedure of the procedure of the total procedure of the procedure of the procedure of the total procedure of the procedure of the total procedure of the procedure of the total procedure of the total procedure of the total	X X X X	X X		
Participating Policy (IPP-OL) Improved the processor of the control of the contro	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability &	IVS-12 IVS-13 IPY-01 IPY-02	IVS-11.1 IVS-12.1 IVS-12.2 IVS-12.3 IVS-13.1 IVS-13.2 IPY-01.1 IPY-02.1	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high- risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to	ody out rescher, personline access to an insperiodor are poinces affer processors is solidanted and meteralismiss are poinced and processors is solidanted and meteralismiss are poinced and processor is established after international are poinced after processor in the processor in the processor is a processor in the processor i	X X X X X	X X		PDF, XLS, CSV
Intergrepatibility IPPOSI 19POS 19P	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability &	IVS-12 IVS-13 IPY-01 IPY-02	IVS-11.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-13.1 IVS-13.1 IVS-13.2 IPY-01.1 IPY-02.1 IPY-03.1	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high- risk environments and data flows that may have legal The provider shall use open and published APIs to ensure all structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions	ody out rescher, personitier access to an insperiodor. Are pointes arise processore s'estamistier au meterialismis in a report processore s'estamistier au meterialismis in a processore s'estamistier a'internationismis in a processor a consideration and a processor a consideration and	X X X X X	X X		PDF, XLS, CSV
The provider and use in deciding recognition of multiple control of the provider and use in deciding recognition of multiple control of the provider and use in deciding recognition of the provider and use in deciding recognition of the provider and use in the provider and use in deciding recognition of the provider and use in deciding recognition of the provider and use in the provider a	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Portability Portability	IVS-12 IVS-13 IPY-01 IPY-02	IVS-11.1 IVS-12.1 IVS-12.2 IVS-12.3 IVS-13.1 IVS-13.2 IPY-01.1 IPY-02.1 IPY-03.1 IPY-03.2	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high- risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer	ody out restrict personities access to an insperiodothic access to an insperiodothic access and protection es estationated and mechanisms are poincies and protectiones estationated and mechanisms are poincies and protectiones estationated and interchanisms are poincies and protectiones estationated and interchanisms are poincies and protection and p	X X X X X	x x		PDF, XLS, CSV
Virtuation (Proc. 2) and a comment entroprehability of the comment	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & I	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03	IVS-12.1 IVS-12.2 IVS-12.2 IVS-12.3 IVS-13.1 IVS-13.2 IPY-01.1 IPY-02.1 IPY-03.1 IPY-03.2 IPY-03.3 IPY-04.1	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high- risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application The provider shall use secure (e.g., non-clear text and	oby our testinct personities access to an insperioritimate and in the position of the procedure is established and mechanisms were pounces and procedure's established and mechanisms were pounced and procedure's established and mechanisms were pounced and procedure's established and mechanisms were pounced and procedure's established and apply development of your implement recinition and apply development of your problement and the procedure's and apply development is distributed by plottings and the procedure's rate and provide problement and procedure's rate. See distributed on the procedure's rate and provide provide politices and procedure's rate. See distributed on the provide politices and procedure's rate. See vice there is usual import, usual seed politices and procedure's rate. See vice there is usual import, usual seed procedure's rate, see vice there is usual import, usual seed procedure's rate, see vice there.	X X X X X X X X X X X X X X X X X X X	x x		PDF, XLS, CSV
Mobile Security MOS-01	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03	IVS-11.1 IVS-12.1 IVS-12.2 IVS-12.3 IVS-13.1 IVS-13.1 IVS-13.2 IPY-01.1 IPY-02.1 IPY-03.3 IPY-03.3 IPY-04.1 IPY-04.2	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal the provider shall use open and published APIs to ensure AII structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the	oby our testinct personities access to an insperioritimate and in the position of the procedure is established and mechanisms were pounces and procedure's established and mechanisms were pounced and procedure's established and mechanisms were pounced and procedure's established and mechanisms were pounced and procedure's established and apply development of your implement recinition and apply development of your problement and the procedure's and apply development is distributed by plottings and the procedure's rate and provide problement and procedure's rate. See distributed on the procedure's rate and provide provide politices and procedure's rate. See distributed on the provide politices and procedure's rate. See vice there is usual import, usual seed politices and procedure's rate. See vice there is usual import, usual seed procedure's rate, see vice there is usual import, usual seed procedure's rate, see vice there.	X X X X X X X X X X X X X X X X X X X	X X		PDF, XLS, CSV
Mobile Security MOS-08 MOS-081. The POVD polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polity of the polity and supporting warreness training clearly with the polity of the polity of the polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polity and supporting warreness training clearly with the polity of the polit	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03	IVS-12.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-13.1 IVS-13.1 IVS-13.2 IPY-03.1 IPY-03.2 IPY-03.3 IPY-04.2 IPY-04.2 IPY-04.2	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization	not you'restrict personities acteus to an inpervotor " Are pointes and procedure is electionistic and meterinamisms were pointed and procedure's electionistic and meterinamisms were pointed and procedure's electionistic and infectionisms were pointed and procedure's electionistic and infectionisms were pointed and procedure's electionistic and infectionisms work pointed and infectionistic and infectionisms work pointed and infectionistic and purpose under provide provide political and procedure's rich self-vice and so dissoluctoriety customer under advantable vinte acteur and provide provide political and procedure's rich self-vice and so and provide political and procedure's rich self-vice and provide provide political provide provide political provide provide political provide provide pr	X X X X X X X X X X X X X X X X X X X	X X		PDF, XLS, CSV
Mobile Security MOS-06 MOS-03.1 The provider shall have a documented papication short in the security of the security MOS-06 MOS-06.1 The provider shall have a documented papication short in the security of the security MOS-06 MOS-06.1 The provider shall have a documented papication short in the security of the security MOS-06 MOS-06.1 The provider shall have a documented papication which is security MOS-06 MOS-06.1 The provider shall have a documented papication short in the security of the security MOS-06 MOS-06.1 The company shall have a documented papication which is security MOS-06 MOS-06.1 The company shall have a documented application which is security MOS-06 MOS-06.1 The company shall have a documented application which is security MOS-06 MOS-06.1 The company shall have a documented application which is security most than the security of the security MOS-06 MOS-06.1 The company shall have a documented application which is security most than the security of the security MOS-06 MOS-06.1 The mobile devices and access that the security MOS-06 MOS-06.1 The mobile device policy shall require the use of all the security MOS-18 MOS	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Portability Interoperability & Portability Interoperability & Portability Virtualization	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-04	IVS-11.1 IVS-12.1 IVS-12.2 IVS-12.3 IVS-13.1 IVS-13.2 IPY-03.1 IPY-03.1 IPY-03.2 IPY-04.1 IPY-04.2 IPY-05.2 IPY-05.2	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal. The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized entework protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented	ody out restrict personities access to an insperiodor access real and access to an insperiodor access and protectiones estationised and mechanisms are poincies and protectiones estationised and mechanisms are poincies and protectiones estationised and international access and protectiones estationised and international access and international access and international access and appropriate access and object to access and appropriate access and object access and appropriate access and	X X X X X X X X X X X X X X X X X X X			PDF, XLS, CSV
Mobile Security MOS-06 MOS-05.1 All Could based services used by the company's mobile because with some provider half have a documented mobile device with the company's mobile because with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented applied device with the company that have a documented and endorsed the company that have a documented and endorsed through the clark of the company that have a documented and endorsed through the clark of the company that have a documented and enforced through the clark of the company that have a documented and enforced through the clark of the company that have a documented and enforced through the clark of the company that have a documented and enforced through the clark of the company that have a documented and enforced through the clark of the company that have a documented and enforced through the clark of the company that have a documented and enforced through the clark of the company that the compan	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability Interoperability & Portability Interoperability & Portability Virtualization Mobile Security	NS-12 NS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01	IVS-12.1 IVS-12.1 IVS-12.2 IVS-12.3 IVS-13.1 IVS-13.1 IPY-03.1 IPY-03.1 IPY-03.3 IPY-04.1 IPY-04.2 IPY-05.3 IPY-05.3 IPY-05.3 IPY-05.3	Access to all hypervisor management functions or policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high- risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile	ody out restrict personities access to an insperiodor in a reponder after processors is solidanted an interfaminist and pointed after processors is solidanted and interfaminist are pointed after processor is established and interfaminist are pointed after interfaminist and power of the processor in a confidence and processor in a confidence and processor in a confidence and apply obe interested to you processor and to add a confidence and a processor in a confidence and in a confidence and a confidence and processor in a confidence and proc	X X X X X X X X X X X X X X X X X X X	х		PDF, XLS, CSV
Mobile Security MOS-06 MOS-061 All Couls based services used by the company's mobile Mobile Security MOS-07 MOS-08	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Portability Portability Portability & Portability & Portability & Portability & Portability & Mobile Security Mobile Security Mobile Security	NS-12 NS-13 IPY-01 IPY-02 IPY-03 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02	195-31.1 195-32.1 195-32.2 195-32.2 195-31.3 195-31.3 197-03.1 197-03.2 197-03.3 197-04.2 197-05.2 197-05.3 197-05.3 197-05.3 197-05.3 197-05.3 197-05.3	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure AII structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile	Let you trestice personities access to an insperiodor. And poincies and professiones established and metralismisms are poincies and professiones established and metralismisms are poincies and processories established and metralismisms are poincies and processories established and indicate in the processories established and and appropriet established to you metablished and the processories and appropriet established and and appropriet established and appropriet established and appropriet established and and appropriet established appropriet established and appropriet established appropriet established and appropriet established and appropriet established appropriet.	X X X X X X X X X X X X X X X X X X X	x x		PDF, XLS, CSV
Mobile Security MOS-10 MOS-101 An investment of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of his make a documented galgatication of the company of	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability Interoperability & Portability Virtualization Mobile Security Mobile Security Mobile Security Mobile Security	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-02	195-11.1 195-12.1 195-12.1 195-12.2 195-12.2 195-13.1 197-03.1 197-03.2 197-03.3 197-04.2 197-05.2 197-05.3 197-05.2 197-05.3 197-05.2 197-05.3 197-05.2 197-05.3	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high- risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting	not you'restrict personities actess to an insperiodor actes of the processor of stationard and meta-raininisms are poincies and processor is estationard and meta-raininisms are poincies and processor is estationared and interchanisms are poincies and processor is estationared and interchanisms are poincies and processor is estationared and interchanisms are poincies and interchanisms only you return a consideration and processor in the processor is only you provide the processor in the processor is only you provide politicisms and processor in expectationary to you provide politicisms and processor is the processor is the processor in the processor in the processor is only you provide politicisms and processor is the processor in the processor is the processor in the processor is the processor in the processor in the processor is the processor in the processor in the processor is the processor in the processor in the processor is the processor in the processor in the processor is the processor in the processor	X X X X X X X X X X X X X X X X X X X	X X X		PDF, XLS, CSV
Mobile Security M05-10 M05-11 M05-11 M05-11 M05-12 M05-12 M05-12 M05-13 M05-15	Infrastructure & Virtualization Security Infrastructure & Virtualization Virtualization Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Portability Interoperability & Portability Virtualization Mobile Security	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05	IVS-31.1 IVS-32.2 IVS-32.2 IVS-32.2 IVS-13.1 IVS-13.2 IPY-03.1 IPY-03.1 IPY-03.2 IPY-03.3 IPY-04.1 IPY-05.2 IPY-05.5 IPY-05.5 IPY-05.5 IPY-05.3 IPY	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been The company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented mobile device	ody out rescher, personitier access to an insperiodor are poinces after processors a steadoins fed and meteralisms are poinces after processors a steadoins fed and meteralisms are poinces after processors a steadoins fed and interchanisms are poinces after processors a steadoins fed and interchanisms are poinces after processors as a steadoins fed and interchanisms are poinces after poince and appropriet processors of the processor and appropriet processors of the processors and appropriet processors of the processors and appropriet processors and approved to processors and appropriet processors and appropriet processors and appropriet processors and appropriet processors and approved to processors approved to processors approved to processors and approved to processors approved t	X X X X X X X X X X X X X X X X X X X	x x x x		PDF, XLS, CSV
Mobile Security MOS-99	Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Portability Portability & Portability Wirtualization Mobile Security	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06	IVS-11.1 IVS-12.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-12.2 IVS-13.3 IVS-13.3 IVS-13.1 IVS-13.2 IVS-13.3 IVS-13.1 IVS-0.3.1 IVS-0.3.2 IVS-0.3.2 IVS-0.3.2 IVS-0.3.2 IVS-0.3.2 IVS-0.3.3 IVS-0.4.1 IVS-0.5.2 IVS-0.5.2 IVS-0.5.3 IVS-	Access to all hypervisor management functions or policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All Structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use a nutualization formats (e.g., OVF) to help ensure interoperability, and shall have documented hart-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting the BYOD policy and supporting awareness training clearly. The provider shall have a documented policy prohibiting the BYOD policy and supporting awareness training clearly.	not you'restrict personities access to an insperiodor access more process. The access to an insperiodor access more process and process establishment arm enterialments are poments and process establishment arm enterialments are poments and process establishment and interior anisms are poments and process and interior anisms are possible and interior anisms are possible and interior anisms and provide process and process and appropriet and process and appropriet and process and appropriet process and access and appropriet process and access and appropriet process and process and process and appropriet process and appropriet process and process and approprie	X X X X X X X X X X X X X X X X X X X	x x x x x		PDF, XLS, CSV
Mobile Security MoS-19.1 MOS-19.1 MOS-19.1 The mobile device management solution shall be for mobile security most and the mobile device policy shall regime the use of mobile Security MoS-19.2 MOS-19.2 The mobile device policy shall regime the use of mobile Security MOS-19.2 MOS-19.2 The mobile device policy shall regime the use of mobile Security MOS-19.2 MOS-19.2 The mobile device policy shall regime the use of mobile Security MOS-19.2 MO	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Portability Portability Virtualization Mobile Security	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-06 MOS-06 MOS-07	IVS-31.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-13.3 IVS-13.3 IPV-03.1 IPV-03.2 IPV-03.3 IPV-04.1 IPV-05.2 IPV-05.3 IPV	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments. Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal the provider shall use open and published APIs to ensure AII structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (trenart) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile memory and the standard virtualization of most leg, over the provider shall have a documented policy prohibiting the 8YOD policy and supporting awareness training clearly the provider shall have a documented mobile device. All cloud-based services used by the company's mobile The company shall have a documented application.	ody out restrict personities access to an insperiodor are pomose and processors is stocknished our metaminisms are pomose and processors is stocknished our metaminisms are pomosed and processors is stocknished our metaminisms are pomosed and processors is a stocknished our metaminisms are pomosed and processors and processors and processors and processors of the process	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		PDF, XLS, CSV
Mobile Security MOS-12 MOS-12 MOS-12 MOS-13 MOS-14 MOS-14 MOS-14 MOS-15 MOS-16 MOS-17 MOS-18 MOS-19	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Virtualization Mobile Security Mobile	IVS-12 IVS-13 IPV-01 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06 MOS-07 MOS-08 MOS-07 MOS-08	IVS-11.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-12.2 IVS-13.3 IPY-01.1 IPY-03.1 IPY-03.1 IPY-03.3 IPY-04.1 IPY-04.2 IPY-05.2 IPY-05.2 IPY-05.2 IPY-05.1 IPY-05.0 IPY	Access to all hypervisor management functions or policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting the BYOD policy and supporting awareness training clearly. The provider shall have a documented mobile device. All cloud-based services used by the company's mobile The company shall have a documented application. The BYOD policy shall define the device and eligibility.	not you'restrict personities actess to an insperiodor and process and processors established and metalinams are poncies and processors established and metalinams are poncies and processors established and metalinams are poncies and processors established and indicatanisms are poncies and processors established and and another control of the control	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		PDF, XLS, CSV
Mobile Security MoS-12 MOS-12 of built-in security controls on mobile devices (e.g., 4) Mobile Security MoS-13 MOS-13 The PTOD policy includes clarifying language for the expectation of privacy, requirements for highland to the mobile devices of an included to the privacy from the mobile devices are configured to MoS-13 MOS-13 MOS-14 BYOD analytor company owned devices are configured to MoS-16 MOS-16 MOS-16 MOS-16 MOS-16 Password policles, applicable to mobile devices are configured to MoS-16 MOS-16 MOS-16 Password policles, applicable to mobile devices are configured to MOS-16 MOS-16 MOS-16 Password policles, applicable to mobile devices are configured to MOS-16 MOS-16 MOS-16 Password policles, applicable to mobile devices are configured to MOS-17 MOS-17 The mobile device policy shall require the BYOD uses of MOS-18 MOS-19 MOS-20	Infrastructure & Virtualization Security Infrastructure & Virtualization Virtualization Interoperability & Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Virtualization Mobile Security	IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 IPY-05 MOS-01 MOS-02 MOS-03 MOS-06 MOS-06 MOS-07 MOS-08 MOS-09	IVS-11.1 IVS-12.2 IVS-12.2 IVS-12.3 IVS-13.1 IVS-13.2 IVS-13.1 IVS-13.2 IVS-13.1 IVS-13.2 IVS-01.1 IPV-03.1 IPV-03.1 IPV-03.2 IPV-03.2 IPV-03.2 IPV-03.3 IPV-04.1 IPV-05.1 IPV-05.2 IPV-05.3 IPV-05.3 IPV-05.3 IMOS-02.1 MOS-02.1 MOS-06.1 MOS-06.1 MOS-07.1 MOS-09.1 MOS-09.1 MOS-09.1 MOS-09.1 MOS-09.1	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify highrisk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented list of approved application stores has been The company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented application. The BYOD policy shall idefine the device and eligibility. An inventory of all mobile device usued to store and access.	ody out rescher, personities access to an insperiodor are pomose affective and insperiodors as solidantification internationals are pomose affective processors solidantification internationals are pomosed affective and international are pomosed affective and international control you retain a metal and international are pomosed affective and only you present a first processor and apply obesitive and to you have a first processor and apply obesitive and to you have processor and to all an available or international solidantification and an apply obesitive and to you have policies and procedurely rescaled a first processor and apply of the area in a significant and a policies and procedurely rescaled a first procedurely rescaled and apply of the area of the processor and apply of the area and processor and apply of the area and apply of the apply of the area and apply 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		
Mobile Security MOS-13 MOS-131 MoS-14 MOS-141 MOS-152 MOS-153 MOS-153 MOS-153 MOS-153 MOS-154 MOS-154 MOS-154 MOS-154 MOS-162 MOS-163 MOS-164 MOS-164 MOS-164 MOS-164 MOS-165	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization Mobile Security	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-06 MOS-07 MOS-09 MOS-09 MOS-10 MOS-11	IVS-311 IVS-312 IVS-312 IVS-312 IVS-312 IVS-312 IVS-313 IVS-	Access to all hypervisor management functions or policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high- risk environments and data flows that may have legal the provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Adocumented list of approved application stores has been the company shall have a documented policy prohibiting The BYOD policy and supporting awareness training clearly The provider shall have a documented policy prohibiting the BYOD policy shall define de device and application the BYOD policy shall define the device and eligibility An inventory of all mobile devices used to store and access A centralized, mobile device management solution shall be	not you'restrict personities access to an insperiodor. Are pointes and processors is established and metarinamisms are pointed and processors is established and metarinamisms are pointed and processors is established and interchanisms are pointed and processors is established and interchanisms are pointed and interchanisms are pointed and interchanisms are possible and interchanisms are possible and interchanisms or you you insperience interchanisms and apply one processors into you you implement rechinical interactive and apply one interchanisms or you provide politicis after processors into processors. The service interactive are usually provide process into processors into processors. The service interactive are usually provide politicis after processors. The service interactive are usual implor, to auto according into a service interactive and politicisms are usual interactive. The service interactive are usual interactive and according to a consumer to one of the processors are usual interactive. The service interactive are usual interactive and according to a consumer and according to the processors. The service interactive are usual interactive and according to the processors are usual interactive. The service is a consumer are usual interactive and according to the processors are usual interactive and according to the processors. The processors are usual interactive and according to the processors are usual interactive and according to the processors are usual interactive and according to the processors. The processors are usual interactive and according to the processors are usual interactive and according to the processors. The processors are usual interactive and according to the processors are usual interactive and according to the processors. The processors are usual interactive and according to the processors are usual interactive and according to the processors. The processors are usual interactive and according to the processors are usual interactive and according to the processors and accordin	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		
Mobile Security MOS-14 MOS-151 MOS-151 Changes to mobile device a per confluence to Mobile Security MOS-15 MOS-151 Changes to mobile device operating systems, patch levels MOS-162 MOS-16	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Virtualization Mobile Security	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-06 MOS-07 MOS-09 MOS-09 MOS-10 MOS-11	IVS-111 IVS-12.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-12.3 IVS-13.2 IVS-13.2 IVS-13.1 IVS-13.2 IVS-0.3.1 IVS	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been The company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented mobile device All cloud-based services used by the company's mobile The Company shall have a documented and eligibility. An inventory of all mobile device used to store and access A centralized, mobile device management solution shall be The mobile device policy shall require the use of	ody out restrict personities access to an insperiodor in a proposition are pounces and processors is statistical and instructional and instruction are pounces and processors is statistical and interchanisms are pounces and processors is established and interchanisms are pounces and processors is established and interchanisms are pounces and processors in a processor in a process	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		
Mobile Security MOS-15 MOS-15.1 Changes to mobile device operating systems, patch levels, most according to the security MOS-16 MOS-16.1 Password some security events in a timely manner. Encoded Reporting Security MOS-17 MOS-17.1 The mobile device policy all requires the POS Duser to MOS-18.1 Most according to the security MOS-18.1 Most according to the security MOS-19 MOS-19.2 Most according to the security MOS-18 MOS-18.2 MOS-18.2 MOS-18.2 MOS-18.2 MOS-18.3 MOS-18.3 All mobile devices permitted for use through technical device policy and large application to recognize the security MOS-19 MOS-19.3 Most according to the security MOS-20 MOS-20.2 Most according to the security	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Portability Portability Virtualization Mobile Security Mobile	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-06 MOS-07 MOS-09 MOS-09 MOS-09 MOS-09 MOS-10 MOS-11 MOS-12	IVS-311 IVS-321 IVS-321 IVS-322 IVS-322 IVS-32 IVS-32 IVS-32 IVS-32 IVS-33 IVS-32 IVS-33 IVS-3	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile Adocumented Interportation of the provider shall be as a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented application stores has been The company shall have a documented application. The BYOD policy shall define the device and eligibility An inventory of all mobile devices used to structure and access A centralized, mobile device management solution shall be The mobile device policy shall require the use of The mobile device policy shall propibility for the BYOD policy included califying language for the	ody out reschere personnier abeets to an reppersoon are ponness after processors a steadorn for an enterfaments are ponness after processors a steadorn for a first processor and a first rescharations are ponness and processors a steadorn for a first processor and a first rescharations are ponness after processors and a provide a first processor and a provide processor and a provide processor and a provide processor and a provide processor and a processor and a provide provide and a provide provide and a provide provide and a provide provide provide and a provide provide and a provide provide provide and a provide provide provide provide provide and a provide provide provide and a provide provide provide provide provide and a provide provide provide provide provide and a provide p	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		
Mobile Security MoS-16 MoS-16 MoS-16 MoS-16 MoS-17 MoS-17 MoS-17 MoS-17 MoS-17 MoS-17 MoS-18 MoS-18 MoS-18 MoS-18 MoS-18 MoS-18 MoS-18 MoS-18 MoS-19 MoS-20	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Portability Portability Portability & Virtualization Mobile Security Lapidoperabile Security Lapidope	IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 IPY-05 MOS-01 MOS-02 MOS-03 MOS-06 MOS-06 MOS-07 MOS-08 MOS-09 MOS-01 MOS-11 MOS-11	IVS-11.1 IVS-12.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-12.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-0.3 I	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization (latform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting The BYOD policy and supporting awareness training clearly. The provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented application in the BYOD policy shall define the device and eligibility. An inventory of all mobile device used to store and access A centralized, mobile device policy shall grequire the use of the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e	ody out restrict personnier access to an insperiodor in expension are poinces and processors is stocknished an uniternamisms are poinces and processors is stocknished an uniternamisms are poinces and processors is stocknished and uniternamisms are poinces and processors is established and uniternamisms are poinces and processors and internamisms are poinces and processors and approprietion of your insperiment certain affirmensives and approprietion of your processors and approprietion of your processors and approprietion and in the processor and approprietion and in the processor and approprietion a	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		
Mobile Security MOS-17 MOS-18 MOS-19 M	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Portability Portability & Portability & Portability & Portability & Portability & Portability & Virtualization Mobile Security Joilbreoking and Mobile Security Legal Mobile Security Mobile Security Legal Mobile Security Mobile Security Legal Mobile Security Mobile Secu	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-07 MOS-08 MOS-09 MOS-11 MOS-12 MOS-13	IVS-311 IVS-312 IVS-312 IVS-312 IVS-312 IVS-312 IVS-313 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal the provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as in industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented application The provider shall have a documented application the EVOD policy and supporting awareness training clearly. The provider shall have a documented application the EVOD policy shall define the device and eligibility. An inventory of all mobile device used to store and access A centralized, mobile device management solution shall be the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices. The BYOD policy includes clarifying language for the expectation of privacy, requirements for illigation, even the proper should be application of the probable device policy shall grow the circumvention of built-in security controls on mobile devices in the BYOD and/or company owned devices are continued to the spectation of privacy, requirements for illigation, even the proper shall application of the probable device policy shall grow the circumvention of built-in security controls on mobile device and continued to the application of the probable de	ody out reschect personities access to an impervation are poinces after processors is stockinshed and meteralismiss are poinces after processors is stockinshed and international are poinces after poince and poi	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		
Mobile Security MoS-17 Policy MOS-17 MoS-17 Policy MOS-17 MOS-17 MOS-17 Policy MOS-17 MOS-17 MOS-17 MOS-18 MOS-19 MOS-20	Infrastructure & Virtualization Security Infrastructure & Virtualization Virtualization Unteroperability & Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Virtualization Mobile Security Mobile Securi	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06 MOS-07 MOS-09 MOS-11 MOS-12 MOS-13	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-131 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify highrisk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented list of approved application stores has been The company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile device usued to store and access. A centralized, mobile device policy shall require the use of the mobile device policy shall prophibit the circumvention of built-in security controls on mobile devices (e.g., the BYOD policy produced scaffying language for the expectation of privacy, requirements for Ittigation, e.BYOD and/or company wowed devices are configured to Changes to mobile device and services are configured to Changes to mobile device and services are configured to Changes to mobile device and services are configured to	ody out restrict personities access to an insperiodor in a report possibility of the control of	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		
Mobile Security MoS-12 MoS-13 MoS-13 MoS-14 MoS-15 MoS-15 MoS-15 MoS-16 MoS-17 MoS-17 Mobile Security MoS-18 MoS-19 MoS-20 MoS-2	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Portability & Virtualization Mobile Security Mobil	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06 MOS-07 MOS-09 MOS-11 MOS-12 MOS-13	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-131 IVS-03.1 IVS-03.1 IVS-03.1 IVS-03.1 IVS-04.1 IVS-05.1 IVS-05.1 IVS-05.1 IVS-05.3 IVS-06.1 IVS-05.3 IVS-06.1 IVS-06.3 IVS-06.1	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as nidustry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented district of approved application stores has been The company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile device used by the company's mobile. The company shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile device used to store and access. A centralized, mobile device policy shall require the use of The mobile device policy shall prophibit the circumvention of built-in security controls on mobile devices (e.g., The BYOD policy includes clarifying language for the expectation of privacy, requirements for iligation, e. BYOD and/or company owned devices are configured to Changes to mobile device porenting systems, patch levels, Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on	ody out reschect personnier access to an insperiodor are poinces affortive outcomes establishment and metrafinants are poinces affortive outcomes establishment and metrafinants are poinces after procedure's establishment and metrafinants are poinces after procedure's establishment and infrinternaments are poinces after procedure's establishment and infrinternaments are poinces after procedure's establishment and provide mental oby you be interned to you implement recinitural interastives and apply oberitives and oby you provide and so you provide printers after procedure's received and apply oberitives and so you provide printers after procedure's received and apply oberitives and so you provide poinces after procedure's received and apply oberitives and to you provide protices after procedure's received and apply of the received and appl	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		
Mobile Security MOS-18. MOS-19. MOS-20. MOS-20	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Potability & Virtualization Mobile Security Posswords	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-06 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-14	IVS-11.1 IVS-12.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-12.2 IVS-12.3 IVS-13.1 IVS-13.2 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-0.3	Access to all hypervisor management functions or policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All Structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recoppised virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented have documented ist of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile devices used to store and access cantralized, mobile device supports of the use of The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device and provider shall be advantaged to mobile devices, shall be documented and enforced through technical controls on all company devices or devices and provides or devi	ody out restrict personnier acteus for an impervation are poinces and processors is statistically an international acteus from the formation and processors is extensional or an international acteus from the formation and processors is extensional or an international acteus from the formation and processors in the processors in the processor in the proc	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		
Mobile Security MoS-19 MoS-19 MoS-19 MoS-19 MoS-19 MoS-19 MoS-20	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Portability & Portability Portability Virtualization Mobile Security Passwords	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-06 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-14	IVS-311 IVS-312 IVS-312 IVS-312 IVS-32 IVS-32 IVS-33	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented application for the SPOD policy shall define the device and eligibility. An inventory of all mobile devices used to structured and cases a centralized, mobile device management solution shall be The mobile device policy shall require the use of The mobile device policy shall prohibit the circumvention of built-in security controls on mobile the circumvention of built-in security controls on mobile devices (e.g., The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-BYOD and/or company owe devices approved for FVOD users to Memoria and controls on a company devices or device support of Policy or the provider shall be an advantage to mobile device operating systems, patch levels, assowed policies, applicable to mobile devices, shall be adocumented and enforced through technical controls on all company devices or device supported	ody out restrict personnier access to an imperiodor access processions in the control of the procession of the control of the	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		
Mobile Security Mobile Sec	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Portability & Portability Portability Virtualization Mobile Security Passwords	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-06 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-14	IVS-11.1 IVS-12.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-12.2 IVS-12.3 IVS-13.2 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-0.3	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify highrisk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented application. The BYOD policy and supporting equire the use of the company shall have a documented application of privacy, requirements for litigation, e. BYOD policy includes clarifying language for the provider's homobile device policy shall require the use of the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices are configured to Changes to mobile device policy shall prequire the use of the mobile device policy shall prequire the use of the mobile device policy shall prequire the use of the mobile device policy shall prequire the use of the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices, shall be documented and enforced thorgets of shall require the BYOD user to perform	ody out rescher, personitier abcets to an impervation are poinces and professionates and meta-infinishms are poinces and professionate distances and are relectionates are poinces and professionate distances and are relectionates are poinces and professionate distances and are relectionates are poinces and professionates and since the original solution in the original solution and apply oberhave meta-oby objections and solution and apply oberhaves meta-oby objections and solution and solution and solution and solution are solutionated and solution and solution are solutionated and solution and solution are solutionated and solution and solution are solutionated and solution are solutionated and solution and solution and solution are solutionated and solution and sol	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		
MoS-19.2 storing and accessing company information shall allow for Mobile Security Putches MOS-20.3 allowed for use or access on a BYOD-enabled device. MOS-20.2 allowed for use or access on a BYOD-enabled device. Security Indident SEF-01. SEF-01.1 SEF-02.2 supporting business processes and technical measures implemented, to triage security-related events and ensure implemented, to triage security-related events and ensure implemented, to triage security-related events and ensure implemented. SEF-02.3 supporting business processes and technical measures implemented. SEF-03.4 series and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure implemented, to triage security-related events and ensure implemented security incident response ghan? X Security Incident SEF-03.3 SEF-03.1 series in a timely manner. Information security events shall be reported through medical formation security events shall be reported through medical formation security events shall be reported through medical formation security events shall be reported through medical fined communications shannels in a timely manner. Information security events shall be reported through medical fined communications shannels in a timely manner. Information security events shall be reported through medical fined communications shannels in a timely manner. Information security events shall be reported through medical fined communications shannels in a timely manner. Information security events shall be reported through medical fined communications shannels in a timely manner. Seponse particularly required for the presentation of evidence to support incident in a timely manner. Seponse particularly required for the presentation of evidence to support incident in a timely manner. In the process particularly required for the presentation of evidence to support in the process particularly recorded to the papicable legical action subject to the relevant jurisdictio	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability & Wirtualization Mobile Security Passwords	IVS-12 IVS-13 IPV-01 IPV-01 IPV-02 IPV-03 IPV-04 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-07 MOS-07 MOS-08 MOS-09 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-16	IVS-311 IVS-321 IVS-321 IVS-322 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented policy prohibiting the EVIC of the provider shall have a documented policy prohibiting. The EVIC policy shall define the device and eligibility An inventory of all mobile devices used to structure that use of the mobile device policy shall require the use of the mobile device policy shall prohibit the circumvention of built-in security controls on mobile the circumvention of built-in security controls on mobile devices and access A centralized, mobile device anagement solution shall be He mobile device policy shall graquite the use of the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices and access A centralized, mobile device operating systems, patch levels, Password policies, applicable to mobile devices are configured to Changes to mobile device operating systems, patch levels, Password policies, applicable to mobile devices,	ody out restrict personnier actes to an impervation are pointes after processors is stationarely an internationary are pointes after processors is stationarely an internationary are pointes after processors is stationarely and internationary are pointes after processors is stationarely and internationary are pointes after processors is stationarely and internationary are pointed and internationary are pointed and internationary are processors and apply oberines and only oby objuditionary after a distribution and apply objects and internationary objects and internationary objects and internationary objects and internationary objects are processors as a stationary objects and internationary objects and international areas and internationary objects and internationary 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		
MoS-20.2 MOS-20.2 MOS-20.2 Security Incident SEF-01 SEF-01.4 Points of contact for applicable regulation authorities, Security Incident SEF-02.3 Septiment of their responsibility and incident management, a Septiment SEF-03.3 Security Incident SEF-03.4 Septiment SEF-03.4 Septiment SEF-03.4 Security Incident Management, E-Discovery, & Cloud Forensics Security Incident Management, E-Discovery, & Cloud Forensics Septiment SEF-03.4 Septiment SEF-03.4 Septiment SEF-03.5 SEF-03.5 Septiment SEF-03.5 SEF-03	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization Mobile Security Posswords Mobile Security Posswords Mobile Security Posswords Mobile Security Policy Remote Wije	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-06 MOS-07 MOS-08 MOS-09 MOS-11 MOS-12 MOS-12 MOS-13 MOS-14 MOS-15 MOS-16	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-132 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All Structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as cruel, e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an enustry-recoppited virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented hartimalware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly The provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented application The company shall have a documented application and the BYOD policy shall define the device and eligibility. An inventory of all mobile devices used to store and access centralized, mobile device sues to store and access centralized, mobile device policy shall enquire the use of The mobile device policy shall enquire the use of The mobile device policy shall enquire the second policy. Providers of mobile devices used to store and access centralized, mobile device application or problements for iligation, e. BYOD policy includes clarifying language for the expectation of privacy, requirements for iligation, e. BYOD and/or company owned devices are	not you'restrict personities access to an insperiodor in a proposed in the protection is statistical and instructional instruction in the protection is statistical and interchanisms are pomere's indicators and interchanisms are power in a protection in the protection of	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		
Security Incident SEF-01 SEF-01.1 Points of contact for applicable regulation authorities, Security Incident SEF-02 SEF-02.1 Points of contact for applicable regulation authorities, Security Incident SEF-03 SEF-03.2 Security Incident SEF-03 SEF-03.2 Security Incident SEF-03 SEF-03.2 Security Incident SEF-03.2 Security Incident SEF-03.3 SEF-03.2 Security Incident SEF-03.3 SEF-03.3 SEF-03.3 SEF-03.3 SEF-03.3 SEF-03.3 SEF-03.3 SEF-03.3 SEF-03.3 SEF-03.4 SEF-03.4 SEF-03.4 SEF-03.5	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Policy & Legal Interoperability & Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Virtualization Mobile Security Policy Mobile Security Policy Mobile Security Policy Mobile Security Remote Wijee Mobile Security Remote Wijee Mobile Security Remote Wijee Mobile Security Robile Security Remote Wijee Mobile Security Robile Security Remote Wijee Mobile Security Robile Security Remote Wijee Mobile Security Mobile Security Remote Wijee Mobile Security Remote Wijee Mobile Security Mobile Security Mobile Security Remote Wijee Mobile Security Remote Wijee Mobile Security Remote Wijee Mobile Security Mobile Security Remote Wijee Mobile	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-06 MOS-07 MOS-08 MOS-09 MOS-11 MOS-12 MOS-12 MOS-13 MOS-14 MOS-15 MOS-16	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-131 IVS-03.1 IVS-03.1 IVS-03.1 IVS-03.1 IVS-03.1 IVS-04.1 IVS-05.1 IVS-121 IVS-121 IVS-131 IVS-132 IVS-131	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as nidustry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented anti-malware awareness training, specific to mobile a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented apolicy prohibiting. The BYOD policy shall adefine the device and eligibility. The provider shall have a documented apolicy prohibiting. The BYOD policy shall define the device and eligibility. An inventory of all mobile device used to store and access A centralized, mobile device policy shall require the use of The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e. BYOD and/or company owned devices and reconstitution shall be application or the service policy shall require the BYOD user to perform backups of data, prohibit the crusage of naproved application sores, and require the use of anti-All mobile device policy shall require the BYOD user to perform backups of data, prohibit the crusage of anaproved application sores, and re	not you'restrict personities actess to an insperiodor in a proposed in the protection is statistical and instruction and in the protection is statistical and interferansistic are pointed and protection is established and interferansistic are pointed and protection is established and interferansistic are pointed and interferansistic are possible and interferansistic are protected and interferansistic are protected and interferansistic are protected and interferansistic are protected and interferance in the protection of the prote	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		
Security Indeent SEF-02 SEF-02.1 Policies and procedures shall be established, and supporting business processes and technical measures processes. SEF-02 supporting business processes and technical measures processes and technical measures. SEF-03 security principlent security events and supporting business processes and technical measures. SEF-03 supporting business processes and technical measures are supported business. SEF-03 supporting business processes and technical measures are supported business. SEF-03 supporting business processes and technical measures are supported business. SEF-03 supporting business processes supported business processes supported business processes and technical measures are supported business. SEF-03 supporting business an	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization Mobile Security Passwords Mobile Security Possords	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06 MOS-07 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-12 MOS-13 MOS-14 MOS-15 MOS-15 MOS-16	IVS-11.1 IVS-12.1 IVS-12.1 IVS-12.2 IVS-12.2 IVS-12.2 IVS-12.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-13.3 IVS-0.3	Access to all hypervisor management functions or policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All Structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (trenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as consultant-vrecopined virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented hard-malware awareness training, specific to mobile A documented its of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented mobile device. All cloud-based services used by the company's mobile. The mobile device policy shall require the use of The BYOD policy shall define the device and eligibility. An inventory of all mobile devices used to store and access a centralized, mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall require the use of all company devices or devices approved for BYDD usage, The mobile device policy shall require the use of an accompany devi	ody out reschere personnier access to an impervation are pointess after processors a stationaries and internationaries are pointess after processors as a stationaries and internationaries are pointess after processors and approprietive and oby doubt and a risk of an area available on reduces in a fine of a processor and approprietive and is object to design a stationaries and approprietive and is object to design a stationaries and approprietive and is object to design a stationaries and approprietive and is object to design a stationaries and approprietive and is object to design and a stationaries and approprietive and is object to design and a stationaries and approprietive and is object to design and a stationaries and a stationarie	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		
Security Incident SEF-03.2 Septional pellemented, to triage security-related events and ensure forensics SEF-03.3 Implemented, to triage security-related events and ensure timely and thorough incident management, as per timely and thorough incident management with a management and external business reasonsings to you hincident communication channels for workforce personnel and external business reasonsings to you hincident communication channels for workforce personnel and external business reasonsings to you hincident communication channels for workforce personnel and external business reasonsings to you hincident communication channels for workforce personnel and external business reason	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Virtualization Mobile Security Passwords Mobile Security Passwords Mobile Security Policy Mobile Security Patches Mobile Security Patches	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-03 MOS-04 MOS-05 MOS-07 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-14 MOS-15 MOS-15 MOS-16 MOS-16 MOS-17	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been The company shall have a documented policy prohibiting. The SYOD policy and supporting awareness training clearly. The provider shall have a documented application to the SYOD policy shall indefine the device and eligibility. An inventory of all mobile devices used by the company's mobile. The company shall have a documented application. The SYOD policy shall define the device and eligibility. An inventory of all mobile devices used to store and access A centralized, mobile device policy shall require the use of The mobile device policy shall require the use of the mobile device policy shall require the use of the MOD and an endorsed through technical controls on all company devices or devices approved for BYOD usage to the proposed professor of the provider shall would be device saperating vystems, patch levels, Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage to rehapproved application, and require the use of an	ody out restrict personities access to an imperiodor in a processor is solitorities and in the contraction of the processor is solitorities and intrinctional interest processor is solitoritied and interest intrinsic and processor is extended after international size poincies and processor is extended after international processor in the processor is extended after international processor in the	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		
Discovery, & Cloud SEF-0.3 implemented, to triage security-related events and ensure forensics SEF-0.3 implemented, to triage security-related events and ensure timely and thorough incident management, as per SEF-03.1 Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely mananer information security events in a timely mananer information security events in a timely mananer report forensic procedures, including chain of custody, are required for the presentation of evidence to support required for the presentation of evidence to support specific	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Portability & Policy	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-04 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-07 MOS-07 MOS-08 MOS-07 MOS-10 MOS-11 MOS-12 MOS-12 MOS-13 MOS-14 MOS-15 MOS-16 MOS-17 MOS-18 MOS-19 MOS-17	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly The provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented application for the Evolution of the BYOD policy shall define the device and eligibility. An inventory of all mobile devices used to structure and access A centralized, mobile device management solution shall be the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices or and access A centralized, mobile device aperating systems, patch levels, Password policies, applicable to mobile devices for the expectation of privacy, requirements for litigation, e-BYOD and/or company owned devices are configured to Changes to mobile device operating systems, patch levels, Password policies, applicable to mobile devices shall be d	only out restrict, personities access to an impervation are pounted and processors is stationarily and international and processors is established and international and processors in the processor is established and an advantage in the control processor in the processor is an advantage in the desired and international international and inte	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		
Forensics SEF-024 timely and thorough incident management, as per Security Incident SEF-03 SEF-03.1 workforce personnel and external business relationships war workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Security Incident SEF-04 SEF-04.1 Proper forensic procedure, including that in of custody, are required for the presentation of evidence to support of support of the presentation of evidence to support of the presentation of evidence of evidence to support of the presentation of evidence of the pr	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability & Virtualization Mobile Security Passwords Mobile Security Passwords Mobile Security Passwords Mobile Security Pactices Mobile Security Pactices Security Pactices Security Incident Security Indident Security Indident	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-04 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-07 MOS-07 MOS-08 MOS-07 MOS-10 MOS-11 MOS-12 MOS-12 MOS-13 MOS-14 MOS-15 MOS-16 MOS-17 MOS-18 MOS-19 MOS-17	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify highrisk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented. Anti-malware awareness training, specific to mobile. A documented ist of approved application stores has been The company shall have a documented opplicity protects. The provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile device policy shall prequire the use of the mobile device policy shall prequire the use of the mobile device policy shall prequire the use of the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices are configured to the BYOD policy produced scaffying language for the expectation of privacy, requirements for Ittigation, e.BYOD and/or company owned devices are configured to perform backups of data, prohibit the runage of unapproved application stores, and equire the YoU ou ser to perform backups of data, prohibit the usage of unapproved application stores, and equire the YoU ou s	only out restrict, personities access to an impervation are pounted and processors is stationarily and international and processors is established and international and processors in the processor is established and an advantage in the control processor in the processor is an advantage in the desired and international international and inte	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		
Security Incident SEF-03 SEF-04 SEF-04 SEF-04 SEF-04 SEF-04 SEF-04 SEF-05 SE	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization Mobile Security Passwords Mobile Security Mobile Security Passwords Mobile Security Mobile Security Passwords Mobile Security Mobile Security Mobile Security Patches Mobile Security Indident Security Indident Security Indident Security Indident Security Indident Security Indident	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-04 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-07 MOS-07 MOS-08 MOS-07 MOS-10 MOS-11 MOS-12 MOS-12 MOS-13 MOS-14 MOS-15 MOS-16 MOS-17 MOS-18 MOS-19 MOS-17	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-132 IVS-131 IVS-132 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented policy prohibiting the EVIC of the provider shall have a documented policy prohibiting. The EVIC policy and supporting awareness training clearly. The provider shall have a documented policy prohibiting the EVIC of the provider shall have a documented policy prohibiting. The EVIC policy shall define the device and eligibility An inventory of all mobile devices used to store and cacess A centralized, mobile device management solution shall be the mobile device policy shall require the use of the mobile device policy shall require the use of the mobile device policy shall require the use of the mobile device policy shall require the use of the mobile device policy shall require the use of the expectation of privacy, requirements for litigation, e-BYOD and/gr. company owned devices are configured to Changes to mobile device appread for 8700 usage, The mobile devices or device operati	ody out restrict personnier access to an impervation are poinces after processors estationated and metarinisms are poinces after processors and appropriate and opportunity of the processor of the proces	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		
Discovery, & Cloud shall Consent and/or contractually agree to report all information security events in a timely manner information security events shall be reported through needfined communications shannels in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely mann	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization & Wobile Security Mobile Security Possords Mobile Security Mobile	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-07 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-15 MOS-16 MOS-17	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as not use, non-clear trutualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented list of approved application stores has been The company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile device used by the company's mobile. The company shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile device used to store and access A centralized, mobile device management solution shall be The mobile device policy shall require the use of The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices per on the proposed proposed proposed proposed proposed proposed profession provides on problemented solution shall be Parabolic device policy shall prohibit the circumvention of built-in security controls on mobile devices, shall be documented application store, and require the BYOD usage to the proposed proposed proposed	ody out restrict personnier acteurs for an imperiodor in expense processor as indivined and metalianisms are pomices and processor as isotationally an international in a processor as indivined and international interpretational processor as indivined and international interpretation of your relevant and international interpretation of your intervent and international interpretation of your intervent international interpretation of your implement recinitural interactives and apply obelienes in doctor of your processor and the processor and interpretation of your processor and processor and interpretation of your processor and your processor a	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		
Forensics information security events in a timely manner. Information security events that libe reported through crediting date of the presentations channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Security Indident SEF-04 SEF-04.1 SEF-04.2 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-04.4 SEF-04.5 SEF-05.5 SEF-05.4 Metanism shall be up to in place to monitor and quantity.	infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability Policy & Legal Interoperability & Portability Portability Wirtualization Mobile Security Passwords Mobile Security Patches Mobile Security Patches Mobile Security Patches Security Incident Security I	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06 MOS-07 MOS-07 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-15 MOS-16 MOS-17	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been The company shall have a documented policy prohibiting. The SYOD policy and supporting awareness training clearly. The provider shall have a documented opicity prohibiting. The SYOD policy shall redefine the device and eligibility. An inventory of all mobile devices used by the company's mobile The company shall have a documented application. The SYOD policy shall define the device and eligibility. An inventory of all mobile devices used to store and access A centralized, mobile device management solution shall be The mobile device policy shall require the use of The mobile device policy shall require the use of the MOD policy shall device operating systems, patch levels, Password policies, applicable to mobile devices (e.g., The BYOD policy policy ball clarify the systems and require the use of anti-All mobile device policy shall require the support of the properation of privacy, requirements for litigation, e-BYOD and endorred through technical controls on all company devices or devices approved to BYOD usage to report by shall	ody out restrict personnier acteurs for an imperiodor in expense processor as indivined and metalianisms are pomices and processor as isotationally an international in a processor as indivined and international interpretational processor as indivined and international interpretation of your relevant and international interpretation of your intervent and international interpretation of your intervent international interpretation of your implement recinitural interactives and apply obelienes in doctor of your processor and the processor and interpretation of your processor and processor and interpretation of your processor and your processor a	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		
Information security events shall be reported through Information security events	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Potability & Virtualization Mobile Security Passwords Mobile Security Mobile Security Passwords Mobile Security Mobile Security Passwords Mobile Security Indient Mobile Security Indient Management, E-Discovery, & Clouforensies Security Indient	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06 MOS-07 MOS-07 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-15 MOS-16 MOS-17	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify highrisk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an endury-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented application. The BYOD policy and supporting awareness training clearly. All cloud-based services used by the company's mobile. All cloud-based services used by the company's mobile. All cloud-based services used by the company's mobile. The provider shall have a documented application shall be the company shall have a documented application shall be The mobile device policy shall require the use of the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices see go. BYOD and/or company owned devices are configured to perform backups of atta, prohibit the usage of the expectation of privacy, requirements for liti	ody out restrict personnier access to an impervation are pointes after processors estationated and metarfinants are pointes after processors estationated and interferancement of your imperment recinitional measurement and appropriate and object your processors are considered and appropriate and object your processors are considered and appropriate and	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		
Security Incident SEF-04 SEF-04.1 Proper forensic procedures, including chain of custody, are legislated by companion of custody, and a capability of supporting in the custom of custody and a capability of supporting in the custom of custody and a capability of supporting in the custom of custody. At a capability of supporting in the custom of custody, and capability of supporting in the custom of custody. At a capability of supporting in the custom of custody, and capability of supporting in the custom of cust	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization Wobile Security Mobile Security Possords Security Incident Mobile Security Incident Mobil	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06 MOS-07 MOS-07 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-15 MOS-16 MOS-17	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile Andocumented list of approved application stores has been The company shall have a documented policy prohibiting. The SYOD policy and supporting awareness training clearly. The provider shall have a documented application stores has been The company shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile devices used by the company's mobile The company shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile devices used to store and access A centralized, mobile device management solution shall be The mobile device policy shall require the use of The mobile device policy shall require the use of The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-BYOD and/or company ower devices appreciated by the company son all company devices or device appreciation submit on the supporting business processes	ody out restrict personnier actes to an impervation are pointes after processors is stationared an internationary are pointed and processors is stationared and internationary are pointed and processors is stationared and internationary are pointed and processors is established and internationary are pointed and processors is established and internationary are pointed and processors in a processor and apply oberiners and pointed and processors are apply oberiners and pointed and processors are apply oberiners and processors from a statistic or an apply oberiners and processors from a statistic or an apply of processors are apply of an apply of a processor and apply of a processor ana	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		
Security Indeent SEF-04 SEF-04. Proper foreign procedures, including chain or custory, at Management, E- Discovery, & Cloud SEF-04. Polymer foreign procedures, including chain or custory, at Cloud SEF-04. SEF-04. Polymer foreign procedures, including chain or custory, at Cloud SEF-04. SEF-04. SEF-04. A diter an information security incident. Upon notification, or with the control of the contro	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization Wobile Security Mobile Security Possords Security Incident Mobile Security Incident Mobil	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06 MOS-07 MOS-07 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-15 MOS-16 MOS-17	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify highrisk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented mobile device. All cloud-based services used by the company's mobile. The EYOD policy and supporting awareness training clearly the provider shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile device sused to store and accessing company shall have a documented application. The BYOD policy shall require the use of the mobile device policy shall require the use of the mobile device policy shall propible the crumwention of hult-in security controls on mobile devices specification shall be The mobile device policy shall require the use of anti-All mobile device policy shall require the use of anti-All mobile device policy shall require the use of anti-All mobile devices permitted for use through the company BYOD p	ody out reschere personnier access to an impervation are poinces and processores selections and an international some poinces and processores selections and appropriate the object of the processor selection and appropriate the object of the processor selection and appropriate and object of the	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		
Discovery, & Cloud SEF-04.3 potential legal action subject to the relevant jurisdiction Forensics SEF-04.4 after an information security incident. Upon notification Security Incident SEF-05 SEF-05.1 Mechanisms shall be our in obace to monitor and quantity Ory formation are quantity the types, volumes, and a continuous	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability Policy & Legal Interoperability & Portability & Virtualization Mobile Security Passwards Wipe Mobile Security Packer Wipe Mobile Security Packer Wipe Mobile Security Packer Wipe Mobile Security Incident Management, E-Discovery, & Cloud Forensies Incident Reporting Incident Incident Reporting Incident In	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-03 MOS-04 MOS-05 MOS-07 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-15 MOS-15 MOS-15 MOS-16 MOS-17 MOS-18 MOS-18 MOS-19	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-123 IVS-132 IVS-133 IVS-133 IVS-133 IVS-133 IVS-133 IVS-133 IVS-133 IVS-133 IVS-133 IVS-033 IVS-03. IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify highrisk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile device usued to store and access A centralized, mobile device policy shall prequire the use of the mobile device policy shall prequire the use of the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices, shall be the company shall have a documented application shall be The mobile device policy shall prequire the use of the mobile device policy shall prequire the true of the expectation of privacy, requirements for litigation, e.BYOD and/or company owned devices are configured to perform backups of data, prohibit the circumvention of built-in security controls on mobile devices, shall be normally and thorough incident management soluti	ody out restrict personnier actes to an impervation are pointes after processors is stationarely an internationary are pointes after processors is stationarely an internationary are pointes after processors is stationarely and apply objective arms oby you implement recent internationary and apply objective arms oby you implement recent internationary and apply objective arms oby you provide under the objective arms of your processors are stationary or an apply objective arms of your processors are stationary or an apply of the objective arms of your provide customer from a stationary or provide and an apply objective arms of your provide policies after procedurely recently after the your provide consumers (recently objective arms objective arms objective and a consumer or consumers of your provide consumers or consumers of your provide anti-rhalware training specific to more your provide anti-rhalware training specific to my your arms of your provide anti-rhalware training specific to my your arms of your provide anti-rhalware training specific to my your arms of your provide anti-rhalware training specific to my your your arms of your provide anti-rhalware training specific to my your your arms of your provide and your provide and your provide anti-rhalware training specific to my your your arms of your provide and your your provide and your provide and your provide and your your provide 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 X X X X X X X X X X X X X X		
Forensics SEF-04.4 after an information security incident. Upon notification, Journal of the security incident SEF-05 SEF-05.1 Mechanisms shall be out in place to monitor and quantify of your monitor and quantify or your monitor and your monitor a	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization Mobile Security Passwords	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-03 MOS-04 MOS-05 MOS-07 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-15 MOS-15 MOS-15 MOS-16 MOS-17 MOS-18 MOS-18 MOS-19	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting husiness processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile A documented list of approved application stores has been the company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly The provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly The provider shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly the provider shall have a documented mobile device. All cloud-based services used by the company's mobile. The company shall have a documented application to the BYOD policy shall define the device and eligibility. An inventory of all mobile devices used to store and access A centralized, mobile device management solution shall be the mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices and access A centralized, mobile device operating systems, patch levels, Password policies, applicable to mobile devices (e.g., The BYOD policy shall define the device operating systems, patch levels, Password policies, applicable to mobile devices, shall be doc	ody out restrict personnier access to an impervation are poinces after processors estationated and metarlinisms are poinces and processors and processors and provide and processors are possible of the processor of the processors and apply oberinary and processors are processors and apply oberinary and apply ob	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		
	infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization Mobile Security Passwords 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	IVS-12 IVS-13 IPY-01 IPY-02 IPY-03 IPY-04 IPY-05 MOS-01 MOS-02 MOS-03 MOS-03 MOS-04 MOS-05 MOS-07 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-15 MOS-15 MOS-15 MOS-16 MOS-17 MOS-18 MOS-18 MOS-19	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-131 IVS-132 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-131 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify highrisk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented list of approved application stores has been The company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented policy prohibiting. The BYOD policy shall alter device and eligibility. An inventory of all mobile device used by the company's mobile. The company shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile devices used to store and access A centralized, mobile device policy shall require the use of The mobile device policy shall prequire the use of The mobile device policy shall require the use of The mobile device policy shall prohibit the curamyen shall have a documented application. The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e. BYOD and/or company owned devices are configured to the promise device policy shall prohibit the curamyen shall have a document of the proposed policy shall carrier the systems and servers allowed for use or access on a BYOD-enabl	ody out reschere personnier abeets to an impervation are poincies and professioners designation and an international size poincies and professioners designated and international size poincies and professioners designated data international size poincies and professioners designated data international size poincies and professioners designated data international size poincies and operational data international	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		
Management, E SEF-05.2 the types, volumes, and costs of information security when you share safety south into the security with your share safety south in the security with your share safety south into the security with your share safety safety south into the security with your share safety	Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Interoperability & Interoperability & Interoperability & Portability & Virtualization & Virtualizatio	IVS-12 IVS-13 IPV-01 IPV-02 IPV-03 IPV-04 IPV-04 IPV-05 MOS-01 MOS-02 MOS-03 MOS-06 MOS-07 MOS-08 MOS-09 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-16 MOS-17 MOS-18 MOS-17 MOS-18 MOS-19 MOS-19 MOS-19 MOS-10 MOS-10	IVS-111 IVS-121 IVS-121 IVS-121 IVS-122 IVS-122 IVS-122 IVS-123 IVS-132 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-132 IVS-131 IVS-132 IVS-031 IVS-	Access to all hypervisor management functions or Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal The provider shall use open and published APIs to ensure All structured and unstructured data shall be available to Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (treant) requirements for service-to-service application. The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the The provider shall use as nicutery-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented Anti-malware awareness training, specific to mobile. A documented district of approved application stores has been The company shall have a documented policy prohibiting. The BYOD policy and supporting awareness training clearly. The provider shall have a documented policy prohibiting. The BYOD policy shall define the device and eligibility. The provider shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile devices used by the company's mobile. The company shall have a documented application. The BYOD policy shall define the device and eligibility. An inventory of all mobile device suesd to store and access. A centralized, mobile device management solution shall be The mobile device policy shall require the use of The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices, shall be the Shop policy policy hall carify the yes provided shall promote the second providers of the systems and servers allowed for use or access on a BYOD-enabled device. Policy shall carify the yes palled and proced tures approved for BYOD usage to per	ody out restrict personnier access to an impervation are poinces after processors estationated and methodinans are poinces after processors estationated and processors are poinces after processors and apply oberities and objoint processors and apply oberities and objoint poinces after processors and apply oberities and objoint processors and apply objoint apply objoint and animal processors and apply objoint apply objoint and animal processors and apply objoint	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		

				DO YOU INSPECT AND ACCOUNT FOR DATA QUARRY EFFORS AND				
Supply Chain		STA-01.1	Providers shall inspect, account for, and work with their			x		
Management,		STA-01.2	cloud supply-chain partners to correct data quality errors	vo yoʻu uesigii anu impiemerit controis to initigate anu	x			
Supply Chain	STA-02	STA-02.1	The provider shall make security incident information	Do ýou make security incluent information available to all	x			
Supply Chain	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical	Dố you conect capacity and tise data for air l'elevant "		x		
Management,		STA-03.2	and virtual) application and system-system interface (API)			^		
Transparency, and			designs and configurations, and infrastructure network and					
Accountability				Do you provide tenants with capacity planning and use				
Network /			systems components, shall be designed, developed, and					
Infrastructure			deployed in accordance with mutually agreed-upon service	reports.				
Services			and capacity-level expectations, as well as IT governance			x		
Supply Chain	STA-04	STA-04.1	The provider shall perform annual internal assessments of	DO YOU PERIORITI ATTITUAL INTERNAL ASSESSITIENTS OF	x			
Supply Chain	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers	DO YOU SEIECT AND INTONICOL DUISOUTCEU PROVIDERS III			х	
Management,		STA-05.2	and customers (tenants) shall incorporate at least the	they are in compliance with applicable legislation?			x	
Transparency, and		STA-05.3	following mutually-agreed upon provisions and/or terms:		v		^	
Accountability		STA-05.4	Scope of business relationship and services offered (e.g.,	Does legal counsel review all third-party agreements?	<u>^</u>			IAAS
Third Party				DO YOU have the Capability to recover data for a specific	^			IAAS
Agreements		STA-05.5	customer (tenant) data acquisition, exchange and usage,	DO YOU have the capadinty to restrict the storage or		х		
		STA-05.6	feature sets and functionality, personnel and infrastructure	can you provide the prifysical location/geography or storage		х		
		STA-05.7	network and systems components for service delivery and	cán you provide the physical location/geography of storage		х		
		STA-05.8	support, roles and responsibilities of provider and			х		
		STA-05.9	customer (tenant) and any subcontracted or outsourced	Do you andw tenants to define acceptable geographical		x		
		STA-05.10	business relationships, physical geographical location of	Are systems in place to monitor for privacy predictes and		x		
		STA-05.11	hosted services, and any known regulatory compliance	DO YOU ANDW TENANTS TO OUT OUT HAVING THEM		x		
		STA-05.12	considerations)	do you provide the client with a list and cobies or air		x		
Supply Chain	STA-06	STA-06.1	Providers shall review the risk management and	DO YOU TEVIEW THE TISK MANAGEMENT AND GOVERNATICE	v	^		
Supply Chain	STA-07	STA-00.1		Are policies and procedures established, and supporting	, , , , , , , , , , , , , , , , , , ,			
			Policies and procedures shall be implemented to ensure	bo you have the ability to measure and address non-	X			
Management,		STA-07.2	the consistent review of service agreements (e.g., SLAs)	canfyou manage service-rever connects or anconstituencies	X			
Transparency, and		STA-07.3	between providers and customers (tenants) across the	DO YÖÜ PÍOVIQE LENANCS WICH ÖNGONIG VISIONICY AND TEPOTCING	X			
Accountability		STA-07.4	relevant supply chain (upstream/downstream). Reviews	Do you make standarus-based information security metrics	Х			
Supply Chain Metrics		STA-07.5	shall be performed at least annually and identify non-			x		
			conformance to established agreements. The reviews	66 you provide customiers with ongoing visionity and		x		
		STA-07.7	should result in actions to address service-level conflicts or	DO YOUR DATA MANTAGEMENT POINCIES AND PROCEDURES ADDRESS		х		
		STA-07.8	inconsistencies resulting from disparate supplier	Do you review all service level agreements at least annually?	x			ISO 9001/27001
Supply Chain	STA-08		- 1	Do you review all service level agreements at least annually? Do you assure reasonable mormation security across your	X X			ISO 9001/27001
Supply Chain	STA-08	STA-08.1	Providers shall assure reasonable information security	Do you review all service level agreements at least annually? Do you assure reasonable information security across your boes your annual review include an partners/timu-party?	X X			ISO 9001/27001
Management,		STA-08.1 STA-08.2	Providers shall assure reasonable information security across their information supply chain by performing an		x x x			ISO 9001/27001
Management, Supply Chain	STA-08 STA-09	STA-08.1 STA-08.2 STA-09.1	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate	bóes your annuai review includé an partners/tilird-party	X X X	x		ISO 9001/27001
Management, Supply Chain Management,	STA-09	STA-08.1 STA-08.2 STA-09.1 STA-09.2	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality,	oo you mandate ahndar mormation security reviews and	x x x	X X		ISO 9001/27001
Management, Supply Chain Management, Threat and		STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and	búes your annuai review includé an partners runnu party ? Do you mandate arindar informátion sécurity reviews and Do you have extel na tumo party services und comments.	X X X			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability	STA-09	STA-08.1 STA-08.2 STA-09.1 STA-09.2	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures	búes your annuai review includé an partners runnu party ? Do you mandate arindar informátion sécurity reviews and Do you have extel na tumo party services und comments.	x x x			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management	STA-09	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on	odes your annual review include an partnersy tillide party of the party services through the party of the par	x x x			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability	STA-09	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures	Lodes youth annual release include an partners or mid-party or you will not part you have a wild a mornisher security modes for or of your factor and think partners security modes for or you faither annual programs that support or Do you ensure that security threat detection systems using senatures, lists, or behavioral patterns are updated across	x x x			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management	STA-09	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on	Does you'd annual review include an partnersy mind-party to you'd manuase ain'd annual and security reviews and bodyou'f nave excellent him of party Services of thought of you riske annumanware programs mais support or Do you niske annumanware programs mais support or Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best	x x x			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and Irinfarstructure network and systems	Lobes youth annual release include an partners or mid-party or spot manual artification manual release which are more securely release and of your favore external time plates secured to the other or or your labor and are released to your labor and the programs that support or or you make a security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	x x x			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and	STA-09	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT intrastructure network and systems.	Does you'd annual review include an partnersy methoparty to you'd manuage ainhidia morifiation selecting relevant and bo'glor flaver extending manuage ainhidia morifiation selecting relevant to you'd relevant the relevant the relevant support or boy you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X X X			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and Infrastructure network and systems. Policies and procedures shall be established, and supporting processes and technical measures	Loves you'd annual review include an partnersymmid yarty on you'd manuale airluid miorifiacion security reviews and body'dor frave external miorifiacion security reviews cando to you riske anomaniware programs trials support or on you riske anomaniware programs trials support or on you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	x x x x			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Molicious Software Threat and Vulnerability Management	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT intrastructure network and systems.	Lodes youth annual release include an partnersy mind-party to you from a middle mind minds an extensive shows from ord/your faster extensive modes from ord/your faster extended minds and the minds of the control of t	x x x x x x x x x x x x x x x x x x x			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability Management Vulnerability / Patch	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and Infrastructure network and systems. Policies and procedures shall be established, and supporting processes and technical measures	Does you'd annual review include an partnersy methoparty to you'd manuage airluida miorifiation security reviews and boryou'f have external thing plarity Services Chilodic with the partnership of the par	X X X X X X X			ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Molicious Software Threat and Vulnerability Management	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.1 TVM-02.2 TVM-02.3	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices (i.e., issued workstations, laptops, and mobile devices) and II infrastructure network and systems Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within implemented, for timely detection of vulnerabilities within	Lodes youth annual release include an partnersy mind-party to you from a middle mind minds an extensive shows from ord/your faster extensive modes from ord/your faster extended minds and the minds of the control of t	x x x x x x x x x x x x x x x x x x x	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability Management Vulnerability / Patch	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.1 TVM-02.2 TVM-02.4 TVM-02.4 TVM-02.4	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices (i.e., issued workstations, laptops, and mobile devices) and Irinfarstructure network and systems Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., infrastructure network and system components (e.g.,	Does you'd annual review include an partnersy methoparty to you'd manuage airluida miorifiation security reviews and boryou'f have external thing plarity Services Chilodic with the partnership of the par	X X X X X X X X X X X X X X X X X X X	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability Management Vulnerability / Patch	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.1 TVM-02.2 TVM-02.3 TVM-02.4	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (le., issued workstations, laptops, and mobile devices (le., issued workstations, laptops, and mobile devices) and II infrastructure network and systems. Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to	Does you'd annual review include an partnersy methoparty to you'd manuage airluida miorifiation security reviews and boryou'f have external thing plarity Services Chilodic with the partnership of the par	X X X X X X X X X	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability Management Vulnerability / Patch	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.1 TVM-02.2 TVM-02.4 TVM-02.4 TVM-02.4	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices (i.e., intrastructure network and systems Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A	Does you'd annual review include an partnersy methoparty to you'd manuage airluida miorifiation security reviews and body of fasee extended in a manuage airluida miorifiation security through the property of the property o	X X X X X X X X X	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability Management Vulnerability / Patch	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.1 TVM-02.2 TVM-02.4 TVM-02.4 TVM-02.4	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices (i.e., issued workstations, laptops, and mobile devices) and II infantanturiar network and systems Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls of arisk-based model for prioritizing remediation of identified	Lobes youth annual release include an partners or mid-party to you will be added a middle more security security to you will be a middle more and the company security security of the company to you will be a middle more	X X X X X X X X	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability / Patch	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.1 TVM-02.2 TVM-02.4 TVM-02.4 TVM-02.4	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and Infrastructure network and systems. Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be enanaged	Does you'd annual review include an partnersy methoparty to you'd manuage ain'd annun'fadorn's decurry reviews and bu'g'or fraise ekternat hintor partny services chindse." Do you in'aive anun manuare priograms fund support on Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices? Do you conduct network rayer vomeratumy scans regularly buy you conduct network rayer vomeratumy scans regularly buy you conduct network rayer vomeratumy scans to your denote: application/rayer vomeratumy scans to your denote: application/rayer vomeratumy scans to your denote: application/rayer vomeratumy scans to your denote call of periangly system-sayer vomeratum. The your make user essues or Younteratumy scans availation to buy your naise user essues or your parcur vomeratum cas across amor	X X X X X X X X	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability / Patch	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.1 TVM-02.2 TVM-02.4 TVM-02.4 TVM-02.4	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and I'infrastructure network and systems Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and systems components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed unrough a change management process for all vendor-	Lodes youth annual release include an partners or mid-party or you will all the partners of th	X X X X X X X X X	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability / Patch	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.1 TVM-02.2 TVM-02.4 TVM-02.4 TVM-02.4	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems. Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendors supplied patches, configuration changes, or changes to the applied patches, configuration changes, or changes to	Does you'd annual review include an partnersy methoparty to you'd manuage ain'd annun'fadorn's decurry reviews and bu'g'or fraise ekternat hintor partny services chindse." Do you in'aive anun manuare priograms fund support on Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices? Do you conduct network rayer vomeratumy scans regularly buy you conduct network rayer vomeratumy scans regularly buy you conduct network rayer vomeratumy scans to your denote: application/rayer vomeratumy scans to your denote: application/rayer vomeratumy scans to your denote: application/rayer vomeratumy scans to your denote call of periangly system-sayer vomeratum. The your make user essues or Younteratumy scans availation to buy your naise user essues or your parcur vomeratum cas across amor	X X X X X X X X X	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability Management Vulnerability / Patch	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.1 TVM-02.2 TVM-02.4 TVM-02.4 TVM-02.4	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems. Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerabilities assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to reganization's internally developed software. Upon	Lodes youth annual release include an partners or mid-party or you will all the partners of th	X X X X X X X X	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Molicious Software Threat and Vulnerability Management Vulnerability Management Vulnerability / Fatch Management	STA-09 TVM-01 TVM-02	STA-08.1 STA-09.2 STA-09.2 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.2 TVM-02.2 TVM-02.4 TVM-02.5 TVM-02.6	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices (i.e., issued workstations, laptops, and mobile devices and TI infrastructure network and svetems Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies	Lodes youth annual release include an partnersy methoparty to you manual release include an partnersy methoparty to you have been annual to you consuct network anyour you have been annual to you consuct network anyour volume annual you you think the results of you have any work and you have been anyour anyour work and anyour work and definited weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	X X X X X X X X X	x		ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Vulnerability Management Management Management Threat and	STA-09 TVM-01	STA-08.1 STA-08.2 STA-09.1 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.2 TVM-02.2 TVM-02.5 TVM-02.6	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices (i.e., issued workstations, laptops, and mobile devices) and Infrastructure network and systems. Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerabilities assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritzing remediation of identified ulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies Policies and procedures shall be setablished, and	Lodes youth annual release include an partners or mid-party or you will all the partners of th	X X X X X X X X X X X X X X X X X X X	x	X	ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Molicious Software Threat and Vulnerability Management Vulnerability Management Vulnerability Threat and Vulnerability Threat and Vulnerability	STA-09 TVM-01 TVM-02	STA-08.1 STA-09.2 STA-09.2 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.2 TVM-02.2 TVM-02.4 TVM-02.5 TVM-02.6	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices (i.e., issued workstations, laptops, and mobile devices and TI infrastructure network and svetems Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies	Lodes youth annual release include an partnersy methoparty to you manual release include an partnersy methoparty to you have been annual to you consuct network anyour you have been annual to you consuct network anyour volume annual you you think the results of you have any work and you have been anyour anyour work and anyour work and definited weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	X X X X X X X X X	x	X	ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Management Threat and Vulnerability Threat and Vulnerability Management	STA-09 TVM-01 TVM-02	STA-08.1 STA-08.2 STA-09.1 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.2 TVM-02.2 TVM-02.5 TVM-02.6	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices (i.e., issued workstations, laptops, and mobile devices) and Infrastructure network and systems. Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerabilities assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritzing remediation of identified ulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies Policies and procedures shall be setablished, and	Lodes youth annual release include an partnersy methoparty to you manual release include an partnersy methoparty to you have been annual to you consuct network anyour you have been annual to you consuct network anyour volume annual you you think the results of you have any work and you have been anyour anyour work and anyour work and definited weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	X X X X X X X X X X X X X X X X X X X	x	X	ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Molicious Software Threat and Vulnerability Management Annagement Annagement Annagement Vulnerability / Patch Management Threat and Vulnerability / Patch Management	STA-09 TVM-01 TVM-02	STA-08.1 STA-08.2 STA-09.1 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.2 TVM-02.2 TVM-02.5 TVM-02.6	Providers shall assure reasonable information security across their information supply chain by performing an Thrid-party service providers shall demonstrate compliance with information security and confidentiality. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (le., issued workstations, laptops, and mobile devices (le., issued workstations), laptops, and mobile devices (le., issued workstations), laptops, and the laptops, laptop	Does you annot review include an partners remety and party to you will all the property of the partners of the	X X X X X X X X X	x	X	ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Management Threat and Vulnerability Threat and Vulnerability Management	STA-09 TVM-01 TVM-02	STA-08.1 STA-08.2 STA-09.1 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.2 TVM-02.2 TVM-02.5 TVM-02.6	Providers shall assure reasonable information security across their information supply chain by performing an Third-party service providers shall demonstrate compliance with information security and confidentiality, Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and I.Infarstancture network and systems. Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies. Policies and procedures shall be established, and supporting business processes and technical measures.	Lodes youth annual release include an partnersy methoparty to you manual release include an partnersy methoparty to you have been annual to you consuct network anyour you have been annual to you consuct network anyour volume annual you you think the results of you have any work and you have been anyour anyour work and anyour work and definited weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	X X X X X X X X	x	X	ISO 9001/27001
Management, Supply Chain Management, Threat and Vulnerability Management Antivirus / Malicious Software Threat and Vulnerability Management Management Threat and Vulnerability Threat and Vulnerability Management	STA-09 TVM-01 TVM-02	STA-08.1 STA-08.2 STA-09.1 STA-09.1 STA-09.2 TVM-01.1 TVM-01.2 TVM-02.2 TVM-02.2 TVM-02.5 TVM-02.6	Providers shall assure reasonable information security across their information supply chain by performing an Thrid-party service providers shall demonstrate compliance with information security and confidentiality. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (le., issued workstations, laptops, and mobile devices) and II infrastructure network and systems. Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A six-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between	Does you annot review include an partners remety and party to you will all the property of the partners of the	X X X X X X X X X	x	X	ISO 9001/27001

© 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.cloudsecurityalliance.org.subject to the following: (a) the Consensus Assessments Initiative Questionnaire v3.0.1 may be used solely for your personal, informational, non-commercial use; (b) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be modified or altered in any way; (c) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be redistributed; and (c) 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 v3.0.1 (2013.) 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.