CAIQv3.f

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Conse	nsus Assess	ment Answers	Notes
Application &	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed,	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your	Yes	No	Not Applicable	
Interface Security Application Security		AIS-01.2	developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Systems/Software Development Lifecycle (SDLC)?		x		
		AIS-01.3		Do you use an automated source code analysis tool to detect security defects in code prior to production? Do you use manual source-code analysis to detect security defects in code prior to aroduction?	x	x		
		AIS-01.4		uo you use manuai source-cobe analysis to betect security betects in cobe prior to production r Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		x		
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	х			
Application & Interface Security Customer Access		AIS-02.1 AIS- 02.2	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	x			
Requirements				Are all requirements and trust levels for customers' access defined and documented?	x			
Application & Interface Security Data Integrity	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or	Does your data management policies and procedures require audits to verify data input and output integrity routines?		x		
		AIS-03.2	- misuse.	A Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	x			
Application & Interface Security Data Security / Integrity	AIS-04	AIS-04.1	hádise and procedures that be established and materiative in support of data sensity to textel (confidentiality, merginy, and exability) excess and an analysis of the sensitive sensitive sensitives in an analysis system interfaces, juridiction, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRANP, CAESARS)?		x		
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 reviewing the	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?		х		
Audit Planning		AAC-01.2	effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Does your audit program take into account effectiveness of implementation of security operations?		x		
Audit Assurance & Compliance	AAC-02	AAC-02.1 AAC-02.2	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports? Do you conduct network penetration tests of your cloud service infrastructure at least annually?		x		
Independent Audits		AAC-02.3	established policies, standards, procedures, and compliance obligations.	Do you conduct network penetration tests of your cloud service infrastructure at least annually? Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and exidance?		x		
		AAC-02.4 AAC-02.5		Do you conduct internal audits at least annually? Do you conduct independent audits at least annually?	x x			
Audit Assurance &	AAC-03	AAC-02.6 AAC-02.7 AAC-03.1	Organizations shall create and maintain a control framework which	Are the results of the penetration tests available to tenants at their request? Are the results of internal and external audits available to tenants at their request?	x		x	
Compliance Information System Regulatory Mapping			captures standards, regulatory, legal, and statutory requirements relevant for their business eaces. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?		x		
Business Continuity Management &		BCR-01.1 BCR-01.2	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all human business and the stablished of the stable of	Does your organization have a plan or framework for business continuity management or disaster recovery management?			x	
Operational Resilience Business Continuity		BCR-01.3	business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:	Do you have more than one provider for each service you depend on? Do you provide a disaster recovery capability?	x			
Planning		BCR-01.4	Defined purpose and scope, aligned with relevant dependencies Accessible to and understood by those who will use them	Do you monitor service continuity with upstream providers in the event of provider failure?		х		
		BCR-01.5 BCR-01.6	Owned by a named person(s) who is responsible for their review, update, and approval Defined lines of communication, roles, and responsibilities	Do you provide access to operational redundancy reports, including the services you rely on? Do you provide a tenant-triggered failover option?	x	x		
		BCR-01.7	Detailed recovery procedures, manual work-around, and reference information Method for plan invocation	Do you provide a tenane-origine for anover opcom	^		x	
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intensity or upon significant organizational or environment dramps. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?			x	
Business Continuity Management & Operational Resilience Power / Telecommunications	BCR-03	BCR-03.1 BCR-03.2	Data center utilities services and environmental conditions (e.g., water, power, temportarius and humidity conditions, lacdor internet connectivity) shall be secured, monitored, maintained, and tatefa for continual effectiveness at planned intervals to ensure protection from multihorized interception or damage, and designed with automated fail- over or other redundancies in the event of planned or unplanned disruptions.				x	
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	x			Le informazioni sono fornite dal service provider
Business Continuity Management & Operational Resilience Environmental Risks		BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberter attacks, including (Fer, flood, atmosphere) celetrical discharge, solar induced geomagnetic storm, wind, earthquake, tsurami, toppiosion, nuclear accident, volonia cativity, biological harad, civil umrest, mudidle, tectonic activity, and other forms of natural or ma- made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical damage anticipated and are countermeasures included in the design of physical protections?			x	
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, ternadoes, earthquakes, hurricanes, etc.)?		x		
Business Continuity Management & Operational Resilience	BCR-07	BCR-07.1 BCR-07.2	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?			x	informazioni a carico del service provider informazioni a carico del
Resilience Business Continuity Management & Operational	BCR-08	BCR-08.1	support personnel. Protection measures shall be put into place to react to natural and man- made threats based upon a geographically-specific business impact assessment.	Do you have an equipment and datacenter maintenance routine or plan? Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?		x	x	service provider informazioni a carico del service provider
Resilience Business Continuity	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the					
Management & Operational Resilience Impact Analysis		BCR-09.2	impact of any disruption to the organization (cloud provider, cloud consume) that must incorporate the following: • Identify ortical products and services • Identify all dependencies, including processes, applications, business pathers, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. orticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?			x	
Business Continuity	BCR-10	BCR-10.1	and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within ther maximum tolerable period of disruption • Estimate the resources reaulined for resumption Policies and proceedures shall be established, and supporting business	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?		x		
Management & Operational Resilience Policy	BCR-11	BCR-11.1	Processing of polycobiols and we subdime, and supporting goal may be approximately and approximately appropriate participant delivery and support of the organization's IT capabilities supporting delivery and support of the organization's IT capabilities supporting delivery and support of the organization's IT capabilities supporting acceptable standards (Le., TIL vi and COBIT S). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	x		×	
Business Continuity Management & Operational	BCK-11	BCR-11.2	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	x		x	
Resilience Retention Policy		BCR-11.3	policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business	x]

		BCR-11.4	incorporated as part of business continuity planning and tested accordingly for effectiveness.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	х			
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	х			
		BCR-11.6 BCR-11.7		Does your cloud solution include software/provider independent restore and recovery capabilities? Do you test your backup or redundancy mechanisms at least annually?	x			
Change Control &	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business	bo you care four backup or redundancy mechanisms as reduction daily.	~			
Configuration Management			processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual					
New Development / Acquisition			applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?			x	
			authorized by the organization's business leadership or other accountable					
			business role or function.					
Change Control & Configuration	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	х			
Management		CCC-02.2	developers within the organization (e.g., ITIL service management processes).	Are policies and procedures adequately enforced to ensure external business partners comply with change management			×	
Development				requirements?			~	
Change Control & Configuration	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines.	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	х			
management		CCC-03.2 CCC-03.3	testing, and release standards which focus on system availability,	Is documentation describing known issues with certain products/services available? Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service	х			
Quality Testing		CCC-03.4	confidentiality, and integrity of systems and services.	offerings?	х			
		CCC-03.4 CCC-03.5	-	Do you have controls in place to ensure that standards of quality are being met for all software development? Do you have controls in place to detect source code security defects for any outsourced software development activities?	x		x	
		CCC-03.6						Gestito dal software di
et	000.04		Policies and procedures shall be established, and supporting business	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	х			sviluppo
Change Control & Configuration	CCC-04	CCC-04.1	processes and technical measures implemented, to restrict the installation					
Management Unauthorized			of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices)	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	x			
Software			and IT infrastructure network and systems components.					
Change Control &	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks					
Configuration			associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual)					
Production Changes			applications and system-system interface (API) designs and configurations.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	x			
			 Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all 	тока приз сароплоника интиги.				
			changes directly correspond to a registered change request, business- critical or customer (tenant), and/or authorization by, the customer					
		CCC-05.2	(tenant) as per agreement (SLA) prior to deployment.	Do you have policies and procedures established for managing risks with respect to change management in production environments?		x		
		CCC-05.3		Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	х			
Data Security &	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the					
Information Lifecycle Management			data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	х			
Classification		DSI-01.2	-					
				Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	х			L
Data Security & Information Lifecycle		DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document,					
Management Data Inventory /			and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and					
Flows			virtual) applications and infrastructure network and systems components	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services'				
			and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to	Do you inventory, document, and maintain data nows for data that is resident (permanent or temporary) within the services applications and infrastructure network and systems?	х			
			address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk.					
			provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.					
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?		x		
Data Security & Information	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?			х	
Lifecycle Management		DSI-03.2	activity, unauthorized disclosure, or modification in such a manner to					
E-commerce Transactions			prevent contract dispute and compromise of data.	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	х			
Data Security &	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the					
Information Lifecycle Management			security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that				
Handling / Labeling /			containers for data.	contain data?			х	
Security Policy								
		DSI-04.2		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?			x	
Data Security &	DSI-05	DSI-04.3 DSI-05.1	Production data shall not be replicated or used in non-production	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			х	
Information Lifecycle			environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is					
Management Nonproduction Data			affected, and must comply with all legal and regulatory requirements for	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	х			
			scrubbing of sensitive data elements.					
Data Security &	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned					
Information Lifecycle		00.00.1	responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	x			
Management								
Data Security & Information Lifecycle		DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	x			
Management Secure Disposal			and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.					
Secure Disposar		DSI-07.2	recoverable by any comparer forenale means.	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	х			
Datacenter Security	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?			x	
Asset Management		DCS-01.2	expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical					
			locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned			x	
			-8	ownership?			^	
Datacenter Security Controlled Access		DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication				
Points			desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., rences, waiis, parriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?			х	
Datacenter Security	DCS-03	DCS-03.1		Do you have a capability to use system geographic location as an authentication factor?			x	
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 technologies may be used to	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment			x	
Identification Datacenter Security	DCS-04	DCS-04.1	validate connection authentication integrity based on known equipment Authorization must be obtained prior to relocation or transfer of	location?			~	
Offsite Authorization			hardware, software, or data to an offsite premises.	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?			х	
Datacenter Security	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of					
Offsite Equipment			equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders					
			recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory	Can you provide tenants with your asset management policies and procedures?			х	
			for reuse and deployment or securely stored until it can be destroyed.					
Datasa da C	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business					
Datacenter Security Policy	DCS-06	DCS-06.1	processes implemented, for maintaining a safe and secure working					
			environment in offices, rooms, facilities, and secure areas storing sensitive information.	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?			x	
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies,				
Data da fina	DCS-07		haven and approximate course	standards, and procedures?			х	
Datacenter Security Secure Area	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor			x	
Authorization			personnel are allowed access.	egress and ingress points?			^	
Datacenter Security	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where					
Unauthorized Persons Entry			unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises,			x	
			facilities to prevent unauthorized data corruption, compromise, and loss.	monitored, controlled and isolated from data storage and process?			^	
Datacenter Security	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support					
User Access			personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?			х	
Encryption & Key	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there					
Management Entitlement			shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	х			
Encryption & Key	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of	Do you have a capability to allow creation of unique encryption keys per tenant?	x			
Management Key Generation		EKM-02.2	cryptographic keys in the service's cryptosystem (e.g., lifecycle	Do you have a capability to manage encryption keys on behalf of tenants?		x		
key Generation		EKM-02.3 EKM-02.4	management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used,	Do you maintain key management procedures? Do you have documented ownership for each stage of the lifecycle of encryption keys?		x		
		EKM-02.5	access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?		x		
Encryption & Key	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business					
Management Encryption			processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers,	Do you encrypt tenant data at rest (on disk/storage) within your environment?		х		
		EKM-03.2	databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and				
			applicable legal, statutory, and regulatory compliance obligations.	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?		х		
		EKM-03.3		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?		х		

Encryption & Key	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?		x		
Management Storage and Access		EKM-04.2 EKM-04.3	open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but	Are your encryption keys maintained by the cloud consumer or a trusted key management provider? Do you store encryption keys in the cloud?		x x		
Governance and Risk	GRM-01	EKM-04.4 GRM-01.1	maintained by the cloud consumer or trusted key management provider. Baseline security requirements shall be established for developed or	Do you have separate key management and key usage duties? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating	x	х		
Management Baseline		GRM-01.2	acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that	systems, routers, DNS servers, etc.)? Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information	^			
Requirements			comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be	security baselines?		x		
Governance and Risk Management Risk Assessments		GRM-02.1 GRM-02.2	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?		х		
Risk Assessments		GRM-02.2	 Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure Compliance with defined retention periods and end-of-life disposal 	Do you conduct risk assessments associated with data governance requirements at least once a year?		x		
Governance and Risk Management	GRM-03	GRM-03.1	 Commission with defined referition periods and end-of-life disposal Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to 	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of		x		
Management Management			their area of responsibility.	policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees, area or responsibility?		*		
Governance and Risk Management		GRM-04.1 GRM-04.2	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical. and physical safeguards to protect assets and data from loss.	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		х		
Program Governance and Risk	GRM-05	GRM-05.1	misuse, unauthorized access, disclosure, alteration, and destruction. The Executive and line management shall take formal action to support	Do you review your Information Security Management Program (ISMP) at least once a year?	х			
Management Management			information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?			х	
Governance and Risk	GRM-06	GRM-06.1	Information security policies and procedures shall be established and	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized				
Management Policy			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	by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?			х	
			by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined			х	
		GRM-06.3 GRM-06.4	information security roles and responsibilities for business leadership.	information security roles and responsibilities for business leadership? Do you have agreements to ensure your providers adhere to your information security and privacy policies?		х		
		GRM-06.5	-	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards? Do you disclose which controls, standards, certifications, and/or regulations you comply with?		x		
Governance and Risk Management	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be	is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?		х		
Policy Enforcement		GRM-07.2	made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.					
	GRM-08			Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	х			
Governance and Risk Management Business / Policy	GRM-08		Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	x			
Change Impacts Governance and Risk	GRM-09	GRM-09.1		Do you notify your tenants when you make material changes to your information security and/or privacy policies?	x			
Management Policy Reviews		GRM-09.2	or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its					
			continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance	Do you perform, at minimum, annual reviews to your privacy and security policies?	х			
Governance and Risk	GRM-10	GRM-10.1	obligations. Aligned with the enterprise-wide framework, formal risk assessments shall					
Management Assessments			be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?			x	
			impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall					
			be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?			x	
Governance and Risk	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based					ļ
Management Program	GRM-11	GRM-11.1	naks shall be stabilised to an acceptative revel. Acceptatice revels based on risk criteria shall be estabilised and documented in accordance with reasonable resolution time frames and stakeholder approval.	Do you have a documented, organization-wide program in place to manage risk?		x		
riogram		GRM-11.2		Do you make available documentation of your organization-wide risk management program?		x		
Human Resources	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external					
Asset Returns			business relationships, all organizationally-owned assets shall be returned within an established period.	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	х			
Human Resources	HRS-02	HRS-01.2 HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all	Do you have asset return procedures outlining how assets should be returned within an established period?	х			
Background Screening			employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved	x			
			accessed, the business requirements, and acceptable risk.	third parties subject to background verification?	^			
Human Resources	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?				
Agreements			and must be signed by newly hired or on-boarded workforce personnel	-	x			
Agreements Human Resources	HRS-04	HRS-03.2 HRS-04.1	and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and	Do you inquire that employment agreements are signed by newly hind or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and ascess?	x			
Employment Agreements Human Resources Employment Termination	HRS-04	HRS-04.1	and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting	workforce personnel user access to corporate facilities, resources, and assets? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	x x			
Employment Termination		HRS-04.1 HRS-04.2	and must be signed by newly hired or on-boarded workforce personnel (e.g., fut or part-time employee or contegent staff prior to granting workforce personnel user access to corporate facilities, resources, and Roles and repossibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	workforce personnel user access to corporate facilities, resources, and assets?	x			
	HRS-04 HRS-05	HRS-04.1	and must be signed by newly hired or on-boarded workforce personnel (e.g., lui or part-time employee or consigned staff) prior to granting workforce personnel user access to corporate facilities, resources, and faces and responsities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measure implemented, to manage business risks	workforce personnal ruler access to compare holdlines relocutes, and assets? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets?	x x			
Employment Termination		HRS-04.1 HRS-04.2	and must be signed by newly hined or on-boarded workforce personnel (e.g., hut or part the molybere or contiguest staff) prior to granting workforce personnel user access to corporate ficilities, resources, and takes and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business	workforce personnel user access to compare holdines: neocores, and assets? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk	x x			
Employment Termination		HRS-04.1 HRS-04.2	and must be signed by newly hired or on-boarded workforce personnel (e.g., lui or particum employee or contiguest staff) prior to granting workforce personnel user access to corporate facilities, resources, and Boles and responsities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business statis associated with permitting mobile device access to corporate resources and may require the mementation of higher assurance compensating	workforce personnel user access to composer halfiles; resources, and asset? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data	x x x			
Employment Termination		HRS-04.1 HRS-04.2	and must be signed by newly hired or on-banded workforce personnel (e.g., lui or part time employee or contigues staff) prior to granting workforce personnel user access to corporate facilities, resources, and Bales and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and spocedures shall be established, and supporting business processes and technical measures implemented, to manage business associated with permitting mobile device access to corporate resources associated with permitting mobile device access to corporate resources control and acceptable-use polices and procedures (e.g., mandated access that function).	workforce personnel user access to comporter hollines: neocores, and assets? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your vensitive data and benant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAI)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	x x x			
Employment Termination Human Resources Portable / Mobile Devices	HRS-05	HRS-04.1 HRS-04.2 HRS-05.1	and must be signed by newly hined or on-boarded workforce personnel (e.g., lut or part time employee or contiguest staff) prior to granting workforce personnel user access to corporate facilities, resources, and Bales and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Philosis and technical measures implemented, to manage business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business accosted with premating mobile device access to corporate resorvers and may require the implementation of higher assurance compensation controls and acceptable use policies and procedures (e.g., manafated ascirily toxing, stronger identity, entitlement and access controls, and devices monitoring).	workforce personnel user access to compare holdines: neocores, and assets? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk	x x x			
Employment Termination Human Resources Portable/ Mobile Devices Human Resources Non-Disclosure Agreements	HRS-05 HRS-06	HRS-04.1 HRS-04.2 HRS-05.1 HRS-06.1	and must be signed by newly hined or on-boarded workforce personnel (e.g., lut or part time employee or contiguent staff) prior to granting workforce personnel user access to corporate facilities, resources, and Bales and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Philoics and procedures shall be established, and supporting business processes and technical measures implemented, to manage business sites accounted with greachese using bioteness. To compare the employment certralistic model of the established, and supporting business processes and technical measures implemented, to manage business sites accounted with greachese use policies and procedures (e.g., manafaed security training, stronger identity, entitlement and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting the organization's reflection of data and operation data	workforce personnel user access to compose halfilles; en place to govern change in employment and/or termination? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portable devices (e.g., destops computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and	x x x			
Employment Termination Human Resources Portable / Mobile Devices	HRS-05	HRS-04.1 HRS-04.2 HRS-05.1	and must be signed by newly hired or on-banded workforce personnel (e.g., lut or part time employee or contiguest atf3) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measure implemented, to manage business structure with granting mobile divide scales to corporate resources control and acceptable-use policies and procedures (e.g., maadated device mentioning). the organization's noned, for the protection of data and operationed details shall be identified, documented, and reviewed at planned intervals.	workforce personnel user access to compose halfilles; en place to govern change in employment and/or termination? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portable devices (e.g., destops computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and	x x x			
Employment Terminablos Norable / Mobile Devices Human Resources Non-Dictiosure Agreements Human Resources Rolo: / Responsibilities	HRS-05 HRS-06	HRS-04.1 HRS-04.2 HRS-05.1 HRS-06.1	and must be signed by newly hired or on-banded workforce personnel (e.g., lut or partitue molybere) contigues utility prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and commutated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business rules and may require the implementation of the same standard and control and acceptable-use policies and procedure (e.g., mandated and may require the implementation of the same scattering, manage control and acceptable-use policies and procedure (e.g., mandated and encir monitoring). Regulaments fine one-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and generational desitua- table documented as the relation excess, and third-parry sur- late documented as the relation excess, and work and a bid documented as the relation excess and excess.	workforce personnel user access to compose halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile device (e.g., lipitops, cell personal digit assistants (PAAI), unch are generally higher risk than now portable devices (e.g., desktop computers at the provider explanation's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reserved a planned intervals? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	x x x x			
Employment Termination Human Resources Portable/ Mobile Devices Human Resources Non-Disclosure Agreements	HRS-05 HRS-05 HRS-07	HRS-04.1 HRS-04.2 HRS-05.1 HRS-06.1 HRS-07.1	and must be signed by newly hired or on-banded workforce personnel (e.g., lut or part time employee or contiguest atf3) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business structure with any end of the structure of the structure sources of the structure of the structure of the structure control and acceptable-use policies and procedures (e.g., mandated device mentioning). The organization's none-factorized resident and access controls, and device mentioning. Bale documented by related to information asset and accurity table be documented by related to information asset and accurity bale be documented by related to information asset and accurity. Policies and procedures that the established, and supporting business processes and technical to exercise the structure of defining the organization's none-factorized reviewed at planned intervals. Roles and procedures that the established, and supporting business processes and technical measures implemented, for defining allowances accorditions for permitting using of organizationally owned or according in the proceedures that the established, and supporting business processes and technical measures implemented, for defining allowances according in the permitting using of organizationally owned or according in the permitting using of organizationally owned or according in the permitting using of organizational owned or according on the permitting using of organizationally owned	workforce personnel user access to component halfillers, includes and assets? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., beptop, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervato?	x x x x	×		
Employment Terminablos Norable / Mobile Devices Human Resources Non-Dictiosure Agreements Human Resources Rolo: / Responsibilities	HRS-05 HRS-05 HRS-07	HRS-04.1 HRS-04.2 HRS-05.1 HRS-06.1 HRS-07.1	and must be signed by newly hined or on-banded workforce personnel (e.g., lut or part time employee or contigent staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measure implemented, to manage business structures and technical measure implemented, to manage business structures and technical measure implemented, to manage business processes and technical measure implemented, to manage business structure structures for non-disclosure or confidentially agreements reflecting the organization's needs for the protection of data and operational detahls and be documented by relation of any and access controls, and device monitoring). Requirements for non-disclosure or confidentially agreements reflecting the agreements for non-disclosure or confidentially agreements reflecting that be documented by relation of third-party users shall be documented by relation of third-party users shall be documented by relation of third-party users shall be documented by relation of third-party users and conditions for permitting users of organizational worked or managed outser end-point devices (e.g., issued workstations, laptops, and business and technical measure implemented, for defining allowances processes and technical measures implemented, for defining allowances and conditions for permitting users for agreements works and and and the documented or measures and worksholess components.	winkforce personnel user access to compose halfiles, executors, and asset? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile derice (e.g., upprot, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable device (e.g., desktop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentially agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and releved at planned intervals? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	x x x x			
Employment Terminablos Norable / Mobile Devices Human Resources Non-Dictiosure Agreements Human Resources Rolo: / Responsibilities	HRS-05 HRS-06 HRS-07 HRS-03	HRS-06.1 HRS-06.2 HRS-06.1 HRS-06.1 HRS-07.1 HRS-08.1 HRS-08.1	and must be signed by newly hined or on-banded workforce personnel (e.g., lut or part time employee or contiguest atf3) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business structures and technical measures implemented, to manage business processes and technical measures implemented, to manage business processes and technical measures in proceedures (e.g., manadated user) training, structure description of data and possibilities of device mentioning). Reductation for non-disclosure or confidentiality agreements refering the organization'n needs for the protection of data and possibilities of contraction, and device mentioning. Reductated and procedures they relate to information asset and accurate table documented and reviewed at planned intervals. Policies and procedures they relate to information asset and accurate and according to representing usage of organizationally awared or managed outser end-point devices (e.g., issued workstations), bupport, and according in for proteinities (e.g., issued workstations, bupporting business processes and technical measures implemented, for defining allowances according in for proteinities (e.g., issued workstations, bupport, and according on the proteinities and contractions and systems components, defining allowances and conditions to permitties and according in the proteinities and contractions and systems components, defining allowances and conditions to permitties and and and accurates and additionally, defining allowances and conditions to permit usage of protoces and protections and conditions to permit usage of protoces and conditions to permit usage of approtection and and to accurate to and additionally.	workforce personnel user access to compose halfiles, executors, and asset? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile derice (e.g., lipitops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and relevand at planned intervals? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities uses those of the tenant? Do you provide tenants with a role definition document clarifying your administrative accomponents? Do you define allowance and conditions for BYOD devices and it applications to access corporate resources?	x x x x	x x		
Employment Terminablos Norable / Mobile Devices Human Resources Non-Dictiosure Agreements Human Resources Rolog / Responsibilities	HRS-05 HRS-05 HRS-07	HRS-04.1 HRS-04.2 HRS-05.1 HRS-05.1 HRS-05.1 HRS-07.1 HRS-08.1	and must be signed by newly hined or on-banded workforce personnel (e.g., lut or part time employee or contiguest atfill prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measure implemented, to manage business sincutated with permitting mobile device access to corporate resources control and accessibilities and procedures (e.g., mandated device monitoring). Requirements for non-disclosure or confidentiality agreements infecting and accessibilities of control-disclosure and access controls, and device monitoring). Requirements for non-disclosure or confidentiality agreements infecting and a be documented by related to information asks and access and ball be documented by related to infinite and subjects controls, and device monitoring). Policies and procedures shall be established, and supports business processes and technical measure implemented, for defining allowances and ball be documented by related to infinite approximate infecting accession and technical measures implemented, for defining allowances and conditions for permitting using of organizational-ball work of additional, defining allowances and confidential type and train-gainty uses additional, defining allowances and confidents to permitting additional devices and technical measures implemented, for defining allowances processes and technical measures implemented, for defining allowances and conditions to permitting used or organizational-ball work of additional, defining allowances and confidents to permit usage of processes and technical measures and confidents to permit usage devices and procedures thalling established, and systems components. Additionally, defining allowances and confidents to perent usage devices and balle be establish	workforce personnel user access to compose halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., liptops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable devices (e.g., desitop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities usus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities usus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities usus those of the tenant? Do you be policies and procedures in place to define allowances and confiding tongenones? Do you devices and conditions for BYOD devices and its applications to access corporate resources? Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	HRS-05 HRS-06 HRS-07 HRS-03	HRS-06.1 HRS-06.2 HRS-06.1 HRS-06.1 HRS-07.1 HRS-08.1 HRS-08.1	and must be signed by newly hined or on-boarded workforce personnel (e.g., lut or part time employee or contigent staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business sites accesses and technical measures implemented, to manage business structures and technical measures implemented, to manage business structures and technical measures implemented, to manage business accesses and technical measures implemented, to manage business accesses and technical measures implemented. The manage business accesses to corporate resources and may require the trugiometistication of lighter assurance compensating device mentioning). Requirements for non-discusses controlls, and device mentioning. Relate and received a plannet intervals. Tables and received a plannets method access controls, and device mentioning is then protection of data and operational details that be detertified, documented, and received a plannets reflecting that be detertified, and the established, and supporting business processes and technical measures implementer, for dating glowners processes and technical measures and confictions to permits usage of processes and technical measures and confictions to access to accounter end-point devices (e.g., issue workstations, busings, and managed user end-point devices (e.g., issue workstations, busings, and managed user end-point devices and accidead placing works and accession molitic devices and	workforce personnel user access to compose halfiles: in place to govern change in employment and/or termination? Are documented policies, procedures, and guidelines account for timely revocation of access and return of assets? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., beptop, cell phones, and personal digital assistants (PDA)), which are generally higher risk than non-portable devices (e.g., destop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clurifying your administrative responsibilities versus those of the tenant? Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components? Do you define allowance and conditions of BYDD devices and its applications to access corporate resources? Do you provide efformal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, doud delivery model, legregation of dutes implications, and conflict interest) for all persons whis access to tenant data?	x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	HRS-05 HRS-06 HRS-07 HRS-03	HRS-06.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-09.1	and must be signed by newly hined or on-boarded workforce personnel (e.g., lui de part time employee or contigent staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks accounted with programmentary models and the set of the pro- cess of the set of the security training, stronger identity, entitiement and access controls, and decimation of the set of the provision of data and operational dealsh shall be identified, documented, and supporting business. Regularements for non-disclosure or confidentiality agreements reflectings thal be documented as they relied to information asian descript shall be identified, documented, and reviewed at planned intervals. Relies and responsibilities of contractors, employees, and third-party users shall be documented as they relied to information asian discussion, reporting and acception and measures implemented, for defining disolances and conditions for permitting usage of organizationally owned or managed user end point devices in the vectoristic to permitting usage of personal mobile devices and associated applications with access to organization mobile devices) and if infariture network kind systems components. Acceurity awareness and excercing benefaciation to permitting usage of personal mobile devices and associated applications with access to real particular personal mobile devices and associated applications with access to real contractors, hird party users, and employees of the conjanziational contractors, hird party users, and employees of the conjanziational the contractors.	workforce personnel user access to compose halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile divices (e.g., laptops, cell phones, and personal digital assistants (POAL), which are generally higher risk than non-portable devices (e.g., deptops, cell phones, and personal digital assistants (POAL), which are generally higher risk than non-portable devices (e.g., deptops, cell phones, and personal digital assistants (POAL), which are generally higher risk than non-portable devices (e.g., deptops, cell phones, and personal digital assistants)? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities uses those of the tenant? Do you bave policies and procedures in place to define allowances and conditions for permitting usage of organizationally owned or minanged use end point divices and IT infrastructure return and systems components? Do you devide allowance and conditions for 8YOO devices and It supplications to access corporate resources? Do you devide allowance and conditions for general facilities and conditions for all persons with access to tenant data? Do you devide devices to tenant data?	x x x x x x x x x x x x x x x x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	HRS-05 HRS-06 HRS-07 HRS-03	HRS-06.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-08.2 HRS-09.1 HRS-09.2 HRS-09.3 HRS-09.4	and must be signed by newly hined or on-boarded workforce personnel (e.g., lui or part time employee or contigent staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Philos and approachures shall be established, and supporting business processes and technical measures implemented, to manage business risks accounted with prevalence and the stablished, and supporting business processes and technical measures implemented, to manage business risks accounted with prevalence and the stablished, and supporting business processes and technical measures implemented, to manage business risks accounted with prevalence and the stablished, and supporting business accounted with prevalence and the stablished, and supporting business access the stablished, exe policies and prevention of the and preceding the resonant and the stablished and access controls, and device monitoring. Requirements for non-disclosure or confidentiality agreements reflecting thal be identified, documented, and reviewed at planned intervals. Relies and responsibilities of contractors, employees, and third-party users shall be identified, and supporting business and confidons for permitting usage of organizationally owned of managed our employ devices (e.g., isource and worksitions, tappon, and mobile devices) and if infrastruture network and systems components. Accelorations and acceloration of permitting usage of organizational vectors and accountions for permitting usage of organizational vectors and account previous and associated applications with access to a exectory associated. The stablished and suppont, and mobile devices and associated applications with access to and contractors, hird sparty users, and employees of the organizational data and there exployerita. A mindividue the exects to organizational data shall receive	workforce personnel user access to compose halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portiable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destops computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally owned or managed user end-point devices and IT infrastructure network and systems components? Do you define allowance and conditions for 8YOD devices and It supplications to access corporate resources? Do you provide a format, rote-based, security awareness training program for cloud-related access and data management issues e.g., multi-tenancy, rutionality, doub deviney model, egregation of actes implications, and conflicts of interval; for a persons with secess to tenance dar. Do you provide a format, rote-based, security awareness training program for cloud-related access and data management issues e.g., multi-tenancy, rutionality, doub devices and it supplications to access components? Do you provide a format, rote-based, security awareness training program for cloud-related access and data management issues e.g., multi-tenancy, rutionality, code devices and the information security controls they m	x x x x x x x x x x x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	HRS-05 HRS-06 HRS-07 HRS-03	HRS-06.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-09.1	and must be signed by newly hined or on-boarded workforce personnel (e.g., lui or part time employee or contigent staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Philos and approachures shall be established, and supporting business processes and technical measures implemented, to manage business risks accounted with prevalence and the stablished, and supporting business processes and technical measures implemented, to manage business risks accounted with prevalence and the stablished, and supporting business processes and technical measures implemented, to manage business risks accounted with prevalence and the stablished, and supporting business accounted with prevalence and the stablished, and supporting business access the stablished, exe policies and prevention of the and preceding the resonant and the stablished and access controls, and device monitoring. Requirements for non-disclosure or confidentiality agreements reflecting thal be identified, documented, and reviewed at planned intervals. Relies and responsibilities of contractors, employees, and third-party users shall be identified, and supporting business and confidons for permitting usage of organizationally owned of managed our employ devices (e.g., isource and worksitions, tappon, and mobile devices) and if infrastruture network and systems components. Accelorations and acceloration of permitting usage of organizational vectors and accountions for permitting usage of organizational vectors and account previous and associated applications with access to a exectory associated. The stablished and suppont, and mobile devices and associated applications with access to and contractors, hird sparty users, and employees of the organizational data and there exployerita. A mindividue the exects to organizational data shall receive	workforce personnel user access to compone halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of asset? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., beptop, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervisi? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying rour administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying rours administrative responsibilities versus those of the tenant? Do you devices and conditions for BYOD devices and its applications to access corporate resources? Do you provide a format, role-based, security awareness training rogram for cloud-related access and data management issues teg., multi-enancy, rationality, could elivery model, segregation of duits implications, and conflicts of interest) for all persons with access to tenant data? Do you specifically train your employees regarding their specific role and the information security controls hey must faltil? Do you document edingoveed	x x x x x x x x x x x x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	HRS-05 HRS-06 HRS-07 HRS-03	HRS-06.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-08.2 HRS-09.1 HRS-09.2 HRS-09.3 HRS-09.4	and must be signed by newly hined or on-boarded workforce personnel (e.g., lui or part time employee or contigent staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Philos and approachures shall be established, and supporting business processes and technical measures implemented, to manage business risks accounted with prevalence and the stablished, and supporting business processes and technical measures implemented, to manage business risks accounted with prevalence and the stablished, and supporting business processes and technical measures implemented, to manage business risks accounted with prevalence and the stablished, and supporting business accounted with prevalence and the stablished, and supporting business access the stablished, exe policies and prevention of the and preceding the resonant and the stablished and access controls, and device monitoring. Requirements for non-disclosure or confidentiality agreements reflecting thal be identified, documented, and reviewed at planned intervals. Relies and responsibilities of contractors, employees, and third-party users shall be identified, and supporting business and confidons for permitting usage of organizationally owned of managed our employ devices (e.g., isource and worksitions, tappon, and mobile devices) and if infrastruture network and systems components. Accelorations and acceloration of permitting usage of organizational vectors and accountions for permitting usage of organizational vectors and account previous and associated applications with access to a exectory associated. The stablished and suppont, and mobile devices and associated applications with access to and contractors, hird sparty users, and employees of the organizational data and there exployerita. A mindividue the exects to organizational data shall receive	workforce personnel user access to compose halfiles: en place to goven change in employment and/or termination? Are documented policies, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of asset? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., beptop, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document sharping room for cloud-related access and data management issues (e.g., multi-tenancy, antionality, could delivery model, segregation of dutes implications, and conflicts of interest) for all persons with access to term data? Do you specifically train your employees regarding the specific role and the formation security controls they must fulfil? Do you specifically train your employees regarding the specific role and the formation security controls they must fulfil? Do you specifically train your employees regarding the specific role and the formation security controls they must fulfil? Do you specifically train dower employees regarding the specific role and the formation secur	x x x x x x x x x x x x x x x x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	HR5 05 HR5 06 HR5 07 HR5 08	HRS-04.1 HRS-04.2 HRS-05.1 HRS-06.1 HRS-06.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-09.3 HRS-09.5 HRS-09.6	and must be signed by newly hined or on-banded workforce personnel (e.g., lut or part time employee or contigent staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measure implemented, to manage business sites accesses and technical measure implemented, to manage business processes and technical measure implemented, to manage business accesses to corporate menoses and may require the trajeometistic of higher assure compensation device monitoring). Requirements for non-disclosure or confidentially agreements reflecting that be documented by the protection of data and operational detable shall be documented by the protection of data and operational detable shall be documented by the protection of data and operational detable shall be documented by the protection of data and operational detable shall be documented by the protection of data and operational detable shall be documented by the protection of data and operational detable shall be documented by the protection of data and operational detable shall be documented by the protection of data and operational detable shall be documented by the protection of data and operational detable shall be documented by the protection of data and operational detable shall be documented by the protection data and operational detable data data data endocumented by the protection data and operation and mandated when appropriate. All the stabilitic data data operations and mandet device and procedures and confidions to permit usage of protections, informing an	workforce personnel user access to compose halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of asset? Are policies and procedures established and messures implemented to strictly limit access to your sensitive data and tenant data from portiable and mobile devices (e.g., laptopa, cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clurifying your administrative responsibilities versus those of the tenant? Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally owned or managed user end-point devices and II infrastructure network and systems components? Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, rustionality, doub devices and it sapplications to access corporate resources? Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, rustionality, doub devices and it sapplications to access corporate res	x x x x x x x x x x x x x x x x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	HR5 05 HR5 06 HR5 07 HR5 08	HRS-04.1 HRS-04.2 HRS-05.1 HRS-06.1 HRS-06.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-09.3 HRS-09.5 HRS-09.6	and must be signed by newly hined or on-boarded workforce personnel (e.g., lut or part time employee or contigent staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Paticies and procedures shall be established, and supporting business processes and technical measure implemented, to manage business sing accesses and technical measures implemented, to manage business sing accesses and technical measures implemented, to manage business sing accesses and technical measures implemented, to manage business processes and technical measures implemented, to manage business accesses the molecular of the processor of the access on composite access training, stronger identically agreements reflecting Requirements for non-disclosure or confidentiality agreements reflecting to all additional or access on the access on the addition of the additional densities of the procedure data and operational detains that be identified, documented and technical densities and security. Pacificies and procedures shall be established, and supporting business and conflictions for permitties and exolutions to particular glowances and conflictions for permitties and exolutions to particular glowances and conflictions for permitties and exolutions to particular glowances and contractions, future glowance and exolutions to particular glowances to constructions and exolutions to permitties and exolutions to particular glowances and contractions, future glowance and exolutions to permit allowances to constructions and exolutions to permitting allowances to constructions, future allowances and econditions to permit asgoption constructions, future glowance and econditions to permit asgoptions and and densities and procedures and econditions to permit asgoptions constructions, future and asources onglowance with access to prograni	workforce personnel user access to compose halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and messures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile divices (e.g., laptops, cell phones, and personal digital assistants (POAL), which are generally higher risk than non-portable devices (e.g., deptops, cell phones, and personal digital assistants (POAL), which are generally higher risk than non-portable devices (e.g., deptops, cell phones, and personal digital assistants (POAL), which are generally higher risk than non-portable devices (e.g., deptops, cell phones, and personal digital assistants). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you bave policies and procedures in place to define allowances and conditions for permitting usage of organizationally owned or minaged user end-point divices and IT infrastructure network and systems components? Do you uprovide tenant, twich based, security avereness training grogram for cloud-related access and data management fiscures is buy ou pourders format, two based, security avereness training grogram for cloud-related access and data management faulters are purcharding train your employees regarding their specific relate the information security controls they must fulfit? Do you uprovide tormat, two thated, security avereness training grograms for cloud-related access and data management faulters are purchard data? Do you uprovide toread data traveast popyee regarding	x x x x x x x x x x x x x x x x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	HR5 05 HR5 06 HR5 07 HR5 08	HRS-06.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-06.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.1 HRS-08.2 HRS-08.1 HRS	and must be signed by newly hined or on-boarded workforce personnel (e.g., lut or part time employee or configure staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business sites accesses and technical measures implemented, to manage business sites processes and technical measures implemented, to manage business sites accesses and technical measures implemented, to manage business sites accesses and technical measures implemented, to manage business sites accesses and technical measures in processes to corporate measures and may require the implementation of higher assurance compensatiog device monitoring). Requirements for non-disclosure or confidentiality agreements reflecting to agranatarity in each for the protection dist and operational deals that be identified. Gournement, and resewed at planned intervals. Relea and responsibilities of contrasting englements reflecting business by the relates to information assets and security. Policies and procedures that the established, and supporting business processes to information and the stablished and supporting business processes to information and the stablished of and supporting business processes to information and the stablished and a supporting business processes to information and the stablished and a supporting business processes to information and a supporting business processes to information and a supporting business processes to information and and operations with access to organization accentry avecesses that and procedures that and the stablished of and mendet when appropriate avarees and conditions to permit uses of processions in function relative to the organization. Additionally procedures that and	workforce personnel user access to compose halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of asset? Are policies and procedures established and messures implemented to strictly limit access to your sensitive data and tenant data from portiable and mobile devices (e.g., laptopa, cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clurifying your administrative responsibilities versus those of the tenant? Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally owned or managed user end-point devices and II infrastructure network and systems components? Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, rustionality, doub devices and it sapplications to access corporate resources? Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, rustionality, doub devices and it sapplications to access corporate res	x x x x x x x x x x x x x x x x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	HR5-65 HR5-06 HR5-07 HR5-09 HR5-09	HRS-04.1 HRS-04.2 HRS-05.1 HRS-05.1 HRS-06.1 HRS-07.1 HRS-08.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-09.1	and must be signed by newly hined or on-boarded workforce personnel (e.g., lut or part time employee or configure staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Paticles and procedures shall be established, and supporting business processes and technical measures implemented, to manage business situa- accident with prevalues use pilotes and procedures to corporate resources and may require the mplementation of higher assurance compensation controls and acceptible use pilotes and procedures to corporate resources and may require the mplementation of higher assurance compensation device monitoring. Requirements for non-disclosure or confidentiality agreements reflecting requirements of non-disclosure or confidentiality agreements reflecting to a disclosure or confidentiality agreements reflecting to a disclosure or confidentiality agreements reflecting to add the documented as they relate to information assets and security. Policies and procedures shall be established, and supporting business and confidences on advections or participation with access to access and technical measures implemented, for defining allowances and confidences on advections or participation with access to access and technical measures and engloses, and documented additions for permiting usage of organizational worked or access and technical measures and conditions to permiting business and conditions for permiting usage of againational worked or access and technical measures implemented. (to defining allowances and conditions for permiting usage of againational worked or access and technical measures and conditions to permiting usage of permitiations and access and conditions to permiting usage for a distribution afford and additions of the and accent advectives and ascoread orights worked for all contractions,	workforce personnel user access to compose halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of asset? Are policies and procedures established and messures implemented to strictly limit access to your sensitive data and ternant data from portiable and mobile devices (e.g., laptopa, cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clurifying your administrative responsibilities versus those of the tenant? Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally owned or managed user end-point devices and II infrastructure network and systems components? Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, rustionality, doub delivery model, genegation of datas implication, and conflicts of interest) for all persons whis access the tenant data? Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, rustiona	x x x x x x x x x x x x x x x x x x x			
Emportant Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Resources Acceptable Use Human Resources Instrument Resources Human Resources Instrument Resources Human Resources Instrument Res	HR5-65 HR5-06 HR5-07 HR5-09 HR5-09	HRS-06.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-08.2 HRS-09.2 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.4 HRS-09.1 HRS-09.4 HRS-09.1 HRS-09.2 HRS-09.4 HRS-09.1 HRS	and must be signed by newly hired or on-banded workforce personnel (e.g., lut or partitume employee or configure staff) prior to granting workforce personnel user access to corporate lacilles, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and commutated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business rules and may require the melementation of the start of the start of the start of may require the melementation of the start of the start of the start and commutated in measures implemented to manage business rules and may require the melementation of the start of the start the organisment constraints and access controls, and device monitoring). Regimements for non-disclosure or confidentiality agreement infecting the organisment and access controls and a planned intervals. Table is descripted in contractions, employees, and third pairs users and conditions for pairs with the established, and supporting business processes and technical measures implemented, for defining allowances and conditions for pairs devices the thread access controls, support and acceptable use policits of contractors, employees, and third pairs users processes and technical measures implemented, for defining allowances and conditions for pairs and the established, and supporting business processes and technical measures implemented, for defining allowances and conditions for pairs and the established, and supporting business processes and technical measures implemented, for defining allowances and conditions for pairs and the established and supporting business processes and technical measures in the metal conditions to permit acues of personal nocle devices and associated applications which access to personal nocle devices and associated applications to permit acues of personal function relative to the organizational measures of	windforce personnel user access to compose habilities, reduces, and asset? Are documented policies, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely rencetion of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., tippipor, cell ponces, and personal digit assistants (PDAI), unch are generally higher risk than new portable devices (e.g., deptop, cell ponces, and personal digit assistants (PDAI), unch are generally higher risk than new portable devices (e.g., deptop, cell ponces, and personal digit assistants (PDAI), unch are generally higher risk than new portable devices (e.g., deptop, cell ponces, and personal digit assistants (PDAI), unch are generally higher risk than new portable devices (e.g., deptop, cell ponces, and personal digit assistants (PDAI), unch are generally higher risk than new portable devices (e.g., deptop, cell ponces, and personal digits and operational deaths identified, documented, and resewed at planned intervals? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants, rustically and reserve and is applications for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components? Do you provide a format, note-based, security awareness and conditions for security controls they must fulfil? Do you dowide a format, note-based, security awareness are applied of tesis implications, and conflicts of the interval (MIT)? Do you dowide a format, note-based, security awareness program for cloud-related access and data management issues to accessive and	x x x x x x x x x x x x x x x x x x x			
Employment Termination Human Resources Portable / Mobile Devices Human Resources Agreements Human Resources Acceptable Use Human Resources	185-05 185-07 185-08 185-08 185-09 185-10	HRS-06.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-06.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.1 HRS-08.2 HRS-08.1 HRS	and must be signed by newly hind or on-banded workforce personnel set, hild or partitume employeen consigned staff prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and commutated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business shall and may require the engementation of the star sources compressing controls and acceptable-use policies and procedures (e.g., mandated and may require the engementation of the star sources compressing controls and acceptable-use policies and procedures (e.g., mandated and may require the model for the star sources compressing the organization's means of the star sources compressing the organization's needs for the protections of data and goestational debias hall be identified, documented, and reviewed at planned intervals. Reles and responsibilities of contractors, employees, and third party users processes and technical measures implemented, for defining allowances and conditions for protections of the star supporting business processes and technical measures implemented, for defining allowances and conditions for infrastructure resources data organizationally- measure end-point devices (e.g., succed workstations, support and conditions for protections of the star substring allowances personal mobile devices and socies data displasmes components. A accertity and the star star substring and supporting business processes and technical measures implemented, for defining allowances personal mobile devices and associated applications with access to regunizational measures end-point devices (e.g., succed workstational and and mandated when appropriate. All individuals with access to regunizational measures and technical measures of their roles and responsibilities for • Maintaining a sustem and compliance w	workforce personnel user access to compose halfiles, resources, and asset? Are documented policies, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of asset? Are policies and procedures established and messures implemented to strictly limit access to your sensitive data and ternant data from portiable and mobile devices (e.g., laptopa, cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI), which are generally higher risk than non-portiable devices (e.g., destopa cell phones, and personal digital assistants (PDAI). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clurifying your administrative responsibilities versus those of the tenant? Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally owned or managed user end-point devices and II infrastructure network and systems components? Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, rustionality, doub delivery model, genegation of datas implication, and conflicts of interest) for all persons whis access the tenant data? Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, rustiona	x x x x x x x x x x x x x x x x x x x			
Employment Employment Fernination Human Resources Portable / Mobile Devices Muman Resources Agreements Human Resources Acceptable Use Human Resources Acceptable Use Human Resources Composition Human Resources Acceptable Use Human Resources Composition Human Resources Montagement Human Resources Human Resourc	185-05 185-07 185-08 185-08 185-09 185-10	HRS-04.1 HRS-04.2 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-03.1 HRS-03.2 HRS-03.2 HRS-03.2 HRS-03.2 HRS-03.2 HRS-03.1 HRS-03.2 HRS-03.1 HRS-03.2 HRS-03.1 HRS-03.2 HRS-03.1 HRS	and must be signed by newly hine do on-boarded workforce personnel (e.g., lut or part time employee or contigent staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processe and technical measure implemented, to manage business singuisticates with program factors and the stablished accessed on the procedures in the established, and supporting business processes and technical measure implemented, to manage business singuisticates with program factors of higher assures compensating and may require the traphometation of higher assures controls, and device monitoring). Requirements for non-disclosure or confidentially agreements reflecting the organization's needs for the protection of data and operational deaths able to bentified, documented, and reserved at planned interval. Policies and procedures shall be established, and supports business processes and technical measures implements, for diming advances and conditions for perimiting using of organizational work of and access and technical measures implements, for diming advances processes and technical measures implements, for diming advances processes and technical measures implements, for diming advances according in procedures and the established, and supports business processes and technical measures implements of the organizational work of managed out end-point devices (e.g., issued workstation, subposed or managed out end-point devices (e.g., issued workstation, addition, additions,	workforce personnel user access to compose halfiles: in place to govern change in employment and/or termination? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptors, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable devices (e.g., deptors, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable devices (e.g., deptors, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable devices (e.g., deptors, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable devices (e.g., deptors, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable devices (e.g., deptors, cell phones, and personal digital assistants (PDAI). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, document clurifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clurifying your administrative responsibilities versus those of the tenant? Do you define allowance and conditions for BYOD devices and its applications to access corporate resources? Do you define allowance and conditions for BYOD devices and its applications to access corporate resources? Do you define allowance and conditions of BYOD devices and its applications accurity controls they must fudfil? Do you define allowance and conditions of BYOD devices and the information accurity controls they must fudfil? Do you define all	x x x x x x x x x x x x x x x x x x x			
Employment Employment Fernination Human Resources Portable / Mobile Devices Muman Resources Agreements Human Resources Acceptable Use Human Resources Acceptable Use Human Resources Composition Human Resources Acceptable Use Human Resources Composition Human Resources Montagement Human Resources Human Resourc	185-05 185-07 185-08 185-08 185-09 185-10	HRS-04.1 HRS-04.2 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-03.1 HRS-03.2 HRS-03.2 HRS-03.2 HRS-03.2 HRS-03.2 HRS-03.1 HRS-03.2 HRS-03.1 HRS-03.2 HRS-03.1 HRS-03.2 HRS-03.1 HRS	and must be signed by newly hind or on-banded workforce personnel set, hild or partitume employeen consigned staff prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and commutated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business shall and may require the engementation of the star sources compressing controls and acceptable-use policies and procedures (e.g., mandated and may require the engementation of the star sources compressing controls and acceptable-use policies and procedures (e.g., mandated and may require the model for the star sources compressing the organization's means of the star sources compressing the organization's needs for the protections of data and goestational debias hall be identified, documented, and reviewed at planned intervals. Reles and responsibilities of contractors, employees, and third party users processes and technical measures implemented, for defining allowances and conditions for protections of the star supporting business processes and technical measures implemented, for defining allowances and conditions for infrastructure resources data organizationally- measure end-point devices (e.g., succed workstations, support and conditions for protections of the star substring allowances personal mobile devices and socies data displasmes components. A accertity and the star star substring and supporting business processes and technical measures implemented, for defining allowances personal mobile devices and associated applications with access to regunizational measures end-point devices (e.g., succed workstational and and mandated when appropriate. All individuals with access to regunizational measures and technical measures of their roles and responsibilities for • Maintaining a sustem and compliance w	awddorcy personnel user access to compose halfiles, reduces, and aade? Are documented policie, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable advices (e.g., deptop, cell proves, and personal digital assistant; (PDA)), which are generally higher-risk than non-portable devices (e.g., deptop, cell provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reserved at planned intervals? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants until a rinfastructure network and system: components? Do you provide a formal, role-based, security waveness training program for cloud-related access and data management tosues with access to tenant data? Do you specificity that your employees regarding ther specific role and the information security controls they must fulfil? Do you specificity that your employees regarding ther specific role and the information security controls they must fulfil? Do you specificity that your employees regarding ther specific role and the information security controls they must fulfil? Do you specificity that your employees regonalisties for maintaining aware	x x x x x x x x x x x x x x x x x x x			
Employment Employment Fernination Human Resources Portable / Mobile Device / Mobile Nor-Docksiure Agreenets Agreenets Agreenets Agreenets Agreenets Agreenets Acceptable Use Human Resources Acceptable Use Human Resources Acceptable Use Human Resources Construction Human Resources Acceptable Use Human Resources Human Resources H	185-05 185-07 185-08 185-08 185-09 185-10	HRS-04.1 HRS-04.2 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-03.1 HRS-03.2 HRS-03.2 HRS-03.2 HRS-03.2 HRS-03.2 HRS-03.1 HRS-03.2 HRS-03.1 HRS-03.2 HRS-03.1 HRS-03.2 HRS-03.1 HRS	and must be signed by newly hind or on-banded workforce personnel set, hild or partitume employeen consigned staff prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and commutated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business shall and may require the engementation of the star sources compressing controls and acceptable-use policies and procedures (e.g., mandated and may require the engementation of the star sources compressing controls and acceptable-use policies and procedures (e.g., mandated and may require the model for the star sources compressing the organization's means of the star sources compressing the organization's needs for the protections of data and goestational debias hall be identified, documented, and reviewed at planned intervals. Reles and responsibilities of contractors, employees, and third party users processes and technical measures implemented, for defining allowances and conditions for protections of the star supporting business processes and technical measures implemented, for defining allowances and conditions for infrastructure resources data organizationally- measure end-point devices (e.g., succed workstations, support and conditions for protections of the star substring allowances personal mobile devices and socies data displasmes components. A accertity and the star star substring and supporting business processes and technical measures implemented, for defining allowances personal mobile devices and associated applications with access to regunizational measures end-point devices (e.g., succed workstational and and mandated when appropriate. All individuals with access to regunizational measures and technical measures of their roles and responsibilities for • Maintaining a sustem and compliance w	awddorcy personnel user access to compose halfiles, reduces, and aade? Are documented policie, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable advices (e.g., deptop, cell proves, and personal digital assistant; (PDA)), which are generally higher-risk than non-portable devices (e.g., deptop, cell provider organization's facilities)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reserved at planned intervals? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide terants until a rinfastructure network and system: components? Do you provide a formal, role-based, security waveness training program for cloud-related access and data management tosues with access to tenant data? Do you specificity that your employees regarding ther specific role and the information security controls they must fulfil? Do you specificity that your employees regarding ther specific role and the information security controls they must fulfil? Do you specificity that your employees regarding ther specific role and the information security controls they must fulfil? Do you specificity that your employees regonalisties for maintaining aware	x x x x x x x x x x x x x x x x x x x			
Employment Termination Human Resources Partable / Mebile Devices Mon Ductorium Agreements Human Resources Responsbilities Human Resources Training / Awareness Training / Awareness User Responsbility Human Resources Training / Awareness User Responsbility Human Resources User Responsbility Human Resources User Responsbility	HR5-03 HR5-03 HR5-03 HR5-03 HR5-03 HR5-10 HR5-11 HR5-11	HRS-04.1 HRS-04.2 HRS-05.1 HRS-05.1 HRS-05.1 HRS-08.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.3 HRS-08.3 HRS-08.3 HRS-08.3 HRS-08.3 HRS-08.3 HRS-08.3 HRS-08.1 HRS-08.1 HRS-10.2 HRS-10.3 HRS-10.2 HRS-10.3 HRS-10.2 HRS-10.3 HRS-10.2 HRS-10.3 HRS-10.2 HRS-10.3 HRS-10.2 HRS-10.2 HRS-10.2 HRS-10.3 HRS-10.2 HRS	and must be signed by newly hine di oro-boarded workforce personnel ser, la la orpartitu emplycen o contiguest attiff prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks processes and technical measures implemented, to manage business risks processes and technical measures implemented, to manage business risks processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business processes and technical measures implemented, to manage business risks and acceptable-use policies and procedures (e.g., manadate the organization'n mech for the protection of data and popurational details table be described by exployed and the evolution access and security. Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting using of organizationally owned or managed ourse end-point devices (e.g., suceed workstations, laptop, and allo decumented and traditions to permit usage of remanaged ourse end-point devices (e.g., suceed workstations, laptop, and and acted whon appropriate. All molicitus to any strems components. Additionally, defining allowances and conditions to permit usage orferacional function relative to the organizational order and additionally including and conditions to permit usage orferacional function relative to the organization. A security propriate. All molicitus with access to organization and mandated by compositive and measures and conditions to permit usage orferacional function relative to the organization. A security appropriate anameers tabusities to to organization and mandated proced	windforce personnel user access to compose habilities in place to govern change in employment and/or termination? The de ocumented policies, procedures, and guidelines in place to govern change in employment and/or termination? The beta above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., beptop, cell phones, and personal digital assistants (PAA)), unch are generally higher-risk than now portable devices (e.g., deptop, cell phones, and personal digital assistants (PAA)), unch are generally higher-risk than now portable devices (e.g., deptop, cell phones, and personal digital assistants (PAA)), unch are generally higher-risk than now portable devices (e.g., deptop, cell phones, and personal digital assistants (PAA)), unch are generally higher-risk than now portable devices (e.g., deptop, cell phones, and personal digital assistants (PAA)), unch are generally higher-risk than now portable devices (e.g., deptop, cell phones, and personal digital assistants (PAA)). Unch are generally higher-risk than now portable devices (e.g., deptop, cell phones, and personal digital assistants (PAA)). Are requirements for non-disclosure or confidentiality agreements reflecting the organizational stress (e.g., deptop, cell phones). Do you provide teransts with a role definition document clarifying your administrative responsibilities versus those of the teranst? Do you provide teransts with a role definition document clarifying your administrative responsibilities versus those of the teranst? Do you proved a formal, cound deptop, and the produces and is applications for components? Do you provide teranst, attorative, mode deptop of devices and is applications, access corporate resources? Do you provide a formal, notabased, security model, agergegitation of dates implications, accordite and maintement suscess	x x x x x x x x x x x x x x x x x x x			
Employment Employment Fernination Human Resources Portable / Mobile Device / Mobile Nor-Docksiure Agreenets Agreenets Agreenets Agreenets Agreenets Agreenets Acceptable Use Human Resources Acceptable Use Human Resources Acceptable Use Human Resources Construction Human Resources Acceptable Use Human Resources Human Resources H	HR5-03 HR5-03 HR5-03 HR5-03 HR5-03 HR5-10 HR5-11 HR5-11	HRS-04.1 HRS-04.2 HRS-05.1 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.1 HRS-08.2 HRS-08.1 HRS	and must be signed by newly hind or on-banded workforce personnel set, hild or partitume employeen consigned staff prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and commutated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business (bits processes and technical measures implemented, to manage business (bits and may require the employment termination or drange in employment procedures (shall be established, and supporting business processes and technical measures implemented, to manage business (bits and may require the employment termination or the starting controls and acceptable-use policies and procedures (e.g., mandated and may require the emponetisation of paties and goversion ad exists and the exist of the emponetisation of the and access controls, and device monitoring). Relea and responsibilities of contractors, employees, and third party users had be documented as the vielable to linking advances to accounting the expension of the and access controls, and device monitoring). Release and procedures shall be established, and supporting business processes and technical measures implemented, for defining advancess accountions for procedures shall be established, and supporting business processes and technical measures implemented, for defining advancess accounting the procedures shall be established or all advancess personal mobile devices and associated application with established for all advances measures and accounting meriorment to programs and accounts and user and point devices and associated and responsibilities for • Associations was and approcedures shall be established for all advances and approcedures shall be established and responsibilities for • Associations was and approcedures shall be established process an	windforce personnel user access to compose habilities in place to govern change in employment and/or termination? Are documented policies, procedures, and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile device (e.g., lipitops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable device (e.g., lipitops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable device (e.g., device) confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities usage of organizationally-owned or managed user end-point devices and r1 infrastructure network and systems components? Do you device and conditions for PIOD devices and its applications to access corporate resources? Do you device a formal, role-based, security awareness training grogram for cloud-related access and data management sissues (e.g., multi-tenany, runobased, security awareness training grogram for cloud-related access and data management sissues to you dedine allowance and conditions of training they appeting relations security controls they must fulfil? Do you document data? Do you document data you employee regarding ther securities and condites to interest) for all persons they administration and data stewards poperly educated on thein kingt responsibilities for maini	x x x x x x x x x x x x x x x x x x x			
Employment Employment Fernination Human Resources Portable / Mobile Device / Mobile Nor-Docksiure Agreenets Agreenets Agreenets Agreenets Agreenets Agreenets Acceptable Use Human Resources Acceptable Use Human Resources Acceptable Use Human Resources Construction Human Resources Acceptable Use Human Resources Human Resources H	HR5-03 HR5-03 HR5-03 HR5-03 HR5-03 HR5-10 HR5-11 HR5-11	HRS-04.1 HRS-04.2 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.1 HRS	and must be signed by newly hind or on-banded workforce personnel set, hild or part time employeen contigues attrift prior to granting workforce personnel user access to corporate facilities, resources, and these and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business structures and technical measures implemented, to manage business processes and technical measures in proceedures (e.g., manadated the organisation's model divide access to upport and excess control and acceptable-use policies and procedures (e.g., manadated the organisation's model divide access to apport and excess control and acceptable-use policies and procedures (e.g., manadated the organisation's meaks for the protection of data and goorganisation actess and access to the protection of data and policies and procedures (e.g., toused the organisation's meaks for the protection of data and access controls, and divide monitoring). Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and condition for permiting usage of organizationally owned or managed user end-point divide (e.g., toused workstations, to granization divide shall include and policies and procedures thall be established and systems constructions, life approachese, and conditions to permit usage of the approachesis divide your properties. All individuals with access to organization and mandated when appropriate. All individuals with access to organization and manadated procedures shall be establish	windforce personnel user access to compose habilities, in place to govern change in employment and/or termination? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., lipitops, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable and mobile devices (e.g., lipitops, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable devices (e.g., device) computers at the provider cognitation's fueltiles;?) Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clurifying your administrative responsibilities versus those of the tenant? Do you bee policies and procedures in place to define allowances and confidition for permitting usage of organizationally owned or managed user end-point devices and IT infrastructure network and systems components? Do you device allowance and confiditions for BYOD devices and its applications to access corporate resources? Do you operade a formit, role-based, security awareness training grogram for focud-related access and data management sisues (e.g., multi-teamy, tanobaltis, clud devicey model, segregation of dutes implications, security controls they must fulfil? Do you operade aformit, role-based, security awareness training grogram for clud-related access and data management sisues (e.g., multi-teamy, tanobaltis, for maintaining awarenes and complication for algersons they ob document employee acknowhedgement of training they fave complete? A	x x x x x x x x x x x x x x x x x x x			
Employment Employment Fernination Human Resources Portable / Mobile Device / Mobile Nor-Docksiure Agreenets Agreenets Agreenets Agreenets Agreenets Agreenets Acceptable Use Human Resources Acceptable Use Human Resources Acceptable Use Human Resources Construction Human Resources Acceptable Use Human Resources Human Resources H	HR5-03 HR5-03 HR5-03 HR5-03 HR5-03 HR5-10 HR5-11 HR5-11	HIS-04.1 HIS-04.2 HIS-05.1 HIS-05.1 HIS-05.1 HIS-05.1 HIS-06.1 HIS-06.1 HIS-08.2 HIS	and must be signed by newly hine do on-banded workforce personnel set, hild or partitum employeen contigues attaff prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibles for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business structures that and the established, and supporting business processes and technical measures implemented, to manage business structures and technical measures implemented, to manage business processes and technical measures implemented, to manage business structure training, torger disetty, entitlement and access controls, and device mentioning. Release the estimation of the and ported technical access and access controls and access controls and device mentioning. Release and technical measures implemented, for dening disources and access the prior devices and procedures to exponse thereing. The again access the prior technical measures in the again the again termitoring. Release and procedures shall be established, and supporting business processes and technical measures implemented, for dening disources according in for promodifications and controls components. Additionally, defining allowances and conditions to granitational and and device menoprisite and the citablished, and supporting business processes and technical measures implemented, for dening disources to conditions for permiting usage of organizational shares and according in proceeding environment of the signal actions and manaded are end-point devices (e.g., issue workstations, sloppa, and additionally procedures shall be established for all according processes and econduring environment A sectify againstation and excesses of the organization and manded when apporpriste. All measures of the organization and manded when apporpriste. All	windforce personnel user access to compose habilities, reduces, and asset? Are documented policies, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and messures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile device (e.g., lipitops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable device (e.g., deptops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable device (e.g., deptops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable device (e.g., deptops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable device (e.g., deptops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable device (e.g., deptops, cell phones, and personal digital assistants (PDA)), which are generally higher-risk than non-portable devices (e.g., deptops, cell phones, and personal digital assistants (PDA)). Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational detable identified, documented, and relevaed at planned intervals? Do you provide ternants with a role definition document clarifying your administrative responsibilities wersus those of the tenant? Do you define allowance and conditions for BYOD devices and its applications to access corporate resources? Do you define allowance and conditions for BYOD devices and its applications to access corporate resources? Do you define allowance and conditions for BYOD devices and its applications to access corporate resources? Do you define allowance and conditions for BYOD devices and the applications accurity	x x x x x x x x x x x x x x x x x x x	x		
Employment Employment Fernination Human Resources Portable / Mobile Device / Mobile Nor-Docksiure Agreenets Agreenets Agreenets Agreenets Agreenets Agreenets Acceptable Use Human Resources Acceptable Use Human Resources Acceptable Use Human Resources Construction Human Resources Acceptable Use Human Resources Human Resources H	HR5-03 HR5-03 HR5-03 HR5-03 HR5-03 HR5-10 HR5-11 HR5-11	HRS-04.1 HRS-04.2 HRS-05.1 HRS-05.1 HRS-05.1 HRS-06.1 HRS-08.1 HRS-08.1 HRS-08.1 HRS-08.1 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.2 HRS-08.1 HRS	and must be signed by newly hine do on-banded workforce personnel (e.g., lut or part time employeen contiguent attiff prior to granting workforce personnel user access to corporate facilities, resources, and change in employment for prioring monitoring the signed, documented, and communicated. Pacifics and procedures shall be established, and supporting business processes and technical measures implemented, to manage business fails accessed and technical measures implemented, to manage business fails processes and technical measures implemented, to manage business fails controls due corptable-use policies, and procedures (e.g., manadated executly training, corper directly, entitiement and access controls, and device mentioning). Requirements for non-disclosure or confidentiality agreements reflecting and accessibilities of control-disclosure or confidentiality agreements reflecting and be identified, documented, and reviewed at planned intervals. Pacifics and procedures that be established, and supporting business processes and technical measures implemented, for directly and device mentioning). Pacifics and procedures that be established, and supporting business processes and technical measures implemented, for diring allowances inconditions for promoduces and conditions to generational devices and accession of instatuture measures of the organizational additionally, defining allowances of the organizational additionally, defining allowances and conditions to person and additionally procedures, processes, and policies relating or display organization and additional procedures, processes, and policies relating and measures organizational procedures, shall be established for all additionally processes, and policies relating and regular updates in agrantationally procedures, shall be established in relative additional procedures, shall be established in relative Additionally procedures, shall be established after an agrantationally owneaves and compliance with established policies a	windforce personnel user access to compose habilities, in place to govern change in employment and/or termination? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do the above procedures and guidelines account for timely revocation of access and return of assets? Are policies and procedures established and messures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., lipotos, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable and mobile devices (e.g., lipotos, cell phones, and personal digital assistants (PDAI), which are generally higher-risk than non-portable devices (e.g., devices or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals? Do you provide tenants with a role definition document clurifying your administrative responsibilities versus those of the tenant? Do you bee policies and procedures in place to define allowances and confilition for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components? Do you device allowance and confilitions for BYOD devices and its applications to access corporate resources? Do you operaide aformat, role-based, security awareness training grogram for focular-detaid access and data management sissues (e.g., multi-teamy, tanobaltis, clud devicey model, segregation of dutes implications, security controls they must fulfil? Do you operaide aformat, role-based, security awareness training grogram for cloud-related access and data management sissues (e.g., multi-teamy, tanobaltis, cloud devicey model, segregation of dutes implications, security controls they must fulfil? Do you supperficially train your employee regarding ther specific role and tomination security controls they must fulfil? Are	x x x x x x x x x x x x x x x x x x x	x		
Employment Termination Persination Portable / Mobile Devices Portable / Mobile Devices Portable / Mobile Portable / Mobile Portable / Mobile Agreements Human Resources Responsibility Human Resources Fraining / Awareness Human Resources Human Resources	HR5-03 HR5-03 HR5-03 HR5-03 HR5-03 HR5-10 HR5-11 HR5-11	HIS-04.1 HIS-04.2 HIS-05.1 HIS-05.1 HIS-05.1 HIS-06.1 HIS-06.1 HIS-06.1 HIS-08.2 HIS-08.2 HIS-08.2 HIS-08.2 HIS-08.2 HIS-08.2 HIS-08.1 HIS-08.2 HIS-08.2 HIS-08.1 HIS	and must be signed by newly hind or on-banded workforce personnel set, hild or part time employeen consigned staff prior to granting workforce personnel user access to corporate tacilities, resources, and takes and responsibles for performing employment termination or change in employment procedures is suffice assigned, documented, and commutated. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business rules and may require the melementation of the resources, and device monitoring). Regimements for one-disclosure or content and access controls, and device monitoring. Regimements for non-disclosure or content and access controls, and device monitoring. Regimements for non-disclosure or content and access controls, and device monitoring. Regimements for non-disclosure or content and access controls, and device monitoring. Regimements for non-disclosure or content in the esting the organization's needs for the protection of data and questional debias to access the sufficient of contractors, employees, and third party sures processes and technical measures implemented, for defining advances and continon for genoming surger of agrantizationally owned or managed one end-point device (e.g., sureal-workshitching, advancess advances and particular in essures implemented, for defining advancess advances and technical measures implemented, for defining advancess advances and particular is accessed as a responsibilities for managed one end-point device (e.g., sureal-workshitching, advancess advances, the sure particular is advancess and as and advances and associated applications to permit usge of advancess, and measures and the established and responsibilities for • Advancess, and associated applications to permit usge of advancess, and assoc	awddorcy personnel user access to compose halfiles, reduces, and adde? Are documented policies, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely rencetion of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., biptop, cell phones, and personal digit assistants (PAA)), units are generally higher risk than now portable devices (e.g., deptop, cell phones, and personal digit assistants (PAA)), units are generally higher risk than now portable devices (e.g., deptop, cell phones, and personal digit assistants (PAA)), units are generally higher risk than now portable devices (e.g., deptop, cell phones, and personal digit assistants (PAA)), units are generally higher risk than now portable devices (e.g., deptop, cell phones, and personal digit assistants (PAA)), units are generally higher risk than now portable devices (e.g., deptop, cell phones, and personal digits assistants)? Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational deaths dentified, documented, and reference and conditions for permitting usage of organizationally owned or managed user end-point devices and IT infrastructure network and systems components? Do you provide a format, note-based, security awareness training program) for cloud-related access and data management issues and substructure, networks and the protective regarding their specific role and the information, security controls they must fulfi? Do you specifical training organical cloudered a precensultie for acquiring and maintaining access to accession and data integrity? Are geronomit and and provided with awareness program at least once a year? Are geronomit and and provided with awareness program at least once a year? Are geronomit and dat	x x x x x x x x x x x x x x x x x x x	x		
Employment Termination Human Resources Portable / Meble Dovices Non-Disclosure Non-Disclosure Agreements Human Resources Acceptable Use Human Resources Training / Awareness Human Resources Liser Responsibility Human Resources Iterative Access Management Auda Tooh Access	HR5-03 HR5-03 HR5-03 HR5-03 HR5-03 HR5-10 HR5-10 HR5-11 HR5-11 HR5-11 HR5-11 HR5-12 HR5-12 HR5-12	HIS-04.1 HIS-04.2 HIS-05.1 HIS-05.1 HIS-05.1 HIS-05.1 HIS-06.1 HIS-06.1 HIS-08.2 HIS	and must be signed by newly hine do on-boarded workforce personnel (e.g., lut or part time employeen consigned staff) prior to granting workforce personnel user access to corporate facilities, resources, and tables and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. Policies and procedures shall be established, and supporting business processes and technical measure implemented, to manage business fails accessed with the employment termination of the device monitoring. Requirements for non-disclosure or confidentiality agreements reflecting the device the employment termination access occurred, and device monitoring. Requirements for non-disclosure or confidentiality agreements reflecting the device the employment termination access occurred, and device monitoring. Requirements for non-disclosure or confidentiality agreements reflecting the device termination access and excess controls, and device monitoring. Requirements for non-disclosure or confidentiality agreements reflecting the device termination access and excess controls, and device monitoring. Requirements for non-disclosure or confidentiality agreements reflecting the device the device of contractors, employees, and thrid-party users able documented at the relate like thride activity agreements reflecting threads and societaed applications acids and access controls, and device monitoring and access controls and societaes components. Additionally, defining allowances and confidents to permits used of managed access and societaed applications with access to agreement molitic devices and access controls and systems concretures, threads and access controls and applications and and mandated when appropriate. All individuals with access to organization and mandated when appropriate. Ministructure relations with access to organization agreement comporties averages with the propublication and mandated societaers threin the appropriate	awddorcy personnel user access to compose halfiles, reduces, and aade? Are documented policie, procedures, and guidelines in place to goven change in employment and/or termination? Do the above procedures and guidelines account for timely rencetion of access and return of assets? Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., biptop, cell phones, and personal digital assistants (PKA)), units are generally higher-risk than non-portable devices (e.g., deptop, cell phones, and personal digital assistants (PKA)), units are generally higher-risk than non-portable devices (e.g., deptop, cell phones, and personal digital assistants (PKA)), units are generally higher-risk than non-portable devices (e.g., deptop, cell phones, and personal digital assistants (PKA)), units are generally higher-risk than non-portable devices (e.g., deptop, cell phones, and personal digital assistants (PKA)). Units are generally higher-risk than non-portable devices (e.g., deptop, cell phones, and personal digital assistants (PKA)). Units are generally higher-risk than non-portable devices (e.g., deptop, cell phones, and personal digital assistants (PKA)). Units are generally higher-risk than non-portable devices (e.g., deptop, cell phones, and personal digital assistants (PKA)). The devices of the tenant? Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? Do you provide tenants (PKA) and procedures in place to define allowances and conditions for permitting usage of organizationally owned or managed user end-point devices and IT infrastructure network and systems components? Do you provide tenant, and data management issues (e.g., multi-responsibilities for maintaining ascess to board data management tossues (board-responsibilities for maintaining access to board data management systems? Do you provide tank and provided with	x x x x x x x x x x x x x x x x x x x	x		

Identity & Access	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity				1	r
Management Policies and Procedures			Fonces and proceedings shall be established to such and manage buentity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	x			
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	х			
Identity & Access	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting					
Management Segregation of Duties			Dusiness processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?		x		
Identity & Access	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	х			
Source Code Access		IAM-06.2	use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access	to autonize personner only: Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	х			
Identity & Access Management	IAM-07	IAM-07.1 IAM-07.2	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's	Does your organization conduct third-party unauthorized access risk assessments?		х		
Third Party Access			information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?		x		
			derived from the risk analysis shall be implemented prior to provisioning access.					
Identity & Access Management User Access Restriction /			Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?		x		
Authorization		IAM-08.2		Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities		x		
		IAM-08.3		used for authentication? Do you limit identities' replication only to users explicitly defined as business necessary?	х	^		
Identity & Access Management User Access Authorization			Provisioning user access (e.g., employees, contractors, customes teranst), business partners and/or useplic relationship) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access.	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical applications, infrastructure systems, and network components?	x			
		IAM-09.2	especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems		x		
Identity & Access	IAM-10	IAM-10.1	control. User access shall be authorized and revalidated for entitlement	and network components? Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and		^		
Management User Access Reviews			appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by	administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	х			
		IAM-10.2 IAM-10.3	evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations,	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced? Do you ensure that remediation actions for access violations follow user access policies?	x	х	+	
		IAM-10.4	remediation must follow established user access policies and procedures.	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	~	х		
Identity & Access Management	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual)					
Management User Access Revocation			applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	х			
		IAM-11.2	customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	x			
Identity & Access	IAM-12	IAM-12.1	resoonsibility over implementation of control. Internal corporate or customer (tenant) user account credentials shall be	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	х	-		
Management User ID Credentials		IAM-12.2 IAM-12.3	restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and	Do you use open standards to delegate authentication capabilities to your tenants? Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing	х	x	-	WS SOAP
		IAM-12.4	procedures: eldentity trust verification and service-to-service application (API) and	users? Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		x		
		IAM-12.5	information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and		x		
		IAM-12.6	revocation • Account credential and/or identity store minimization or re-use when feasible	context-based entitlement to data? Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?		x		
		IAM-12.7 IAM-12.8	 Adherence to industry acceptable and/or regulatory compliant 	Do you allow tenants to use third-party identity assurance services? Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout	х			LDAP
		IAM-12.8	authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Uo you support password (e.g., minimum length, age, nistory, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement? Do you allow tenants/customers to define password and account lockout policies for their accounts?	x			
		IAM-12.10 IAM-12.11		Do you support the shifty to force password changes upon first logon? Do you support the shifty to force password changes upon first logon? Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge	x			
				ouestions. manual unlock)?	^			
Identity & Access	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network,					
Identity & Access Management Utility Programs	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?		x		
	IAM-13 IVS-01	IAM-13.1	virtual machine, and application controls shall be restricted. Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, athering to applicable legal, statutory, or repulsatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or life integrity anomalies, and to support forensic investigative capabilities in	Are access to utility programs used to manage virtualized partitions (e.g. shuddown, clone, etc) appropriately restricted and monitores?? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?		x	x	
Management Utility Programs Infrastructure & Virtualization Security	IAM-13	NS-01.1	virtual machine, and application controls shall be restricted. Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability of detect potentially suspicious networks behaviors and/or	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personnel?	x		x	
Management Utility Programs Infrastructure & Virtualization Security	IAM-13 IVS-01	IAM-13.1	virtual machine, and application controls shall be restricted. Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, athering to applicable legal, statutory, or repulsatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or life integrity anomalies, and to support forensic investigative capabilities in	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? is physical and logical user access to audit logs restricted to authorized personnel? can you provide enter that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed? Are audit logo centrally stored and retained?	x	x	x	
Management Utility Programs Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IAM-13 IVS-01 IVS-02	NS-01.1	virtual machine, and application controls shall be restricted. Higher levels of assumance are required for protection, retention, and Higheryche management of audit logs, atherity to applicable legits, statutory, or regulatory compliance obligations and providing unique user access accontability to descriptionity subjections show for bankwise and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all	monitored? Are file integrity (host) and network: intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? is physical and logical user access to audit logs restricted to authorized personnel? Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been enformed? Are audit toge retended on a regular basis for accurity events (e.g., with automated tools)?	x	x x x	x	
Management Ubliky Programs Infrastructure & Virtualization Security Audit Logang / Intrusion Detection Infrastructure & Virtualization Security	IVS-01	NS-01.1 NS-01.2 NS-01.3 NS-01.4 NS-01.5	virtual machine, and application controls shall be restricted. Higher levels of assume are required for portection, retention, and Higher levels of assume and the state of the portection period and the Higher levels of a sub-task, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to descriptionity subjections network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images at use to legged and all trimes. Any changes of their running state leg., domainst, off, or	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and loaical user access to incidents? Is physical and loaical user access to incidents? Are and/to face centrally stored and retained? Are and/to face retained or are access to incidents? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., domant, off or running)? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., domant, off or running)?	x	x x x x x	x	
Management Utility Programs Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	NS-01.1 NS-01.2 NS-01.3 NS-01.4 NS-01.5 NS-02.1	virtual machine, and application controls shall be restricted. Higher levels of assurance are required for protection, releation, and Hisroch management of audi loss, adhering to applicable legal, subaroy, or regulatory compliance obligations and providing unique user access accountability to detect potentially supports methods the hisro sandor file integry anomalies, and to support forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images and the logged and letr risider regression of their running leade of the changes and the subheged mathematication of the maging site regression the leaded and the subheged running). The results of a change or move of an image and the subheged mathematication of the maging site forget most be mediately and the subheged mathematication of the maging site forget most be threaded by the provider site of a submation to the maging site of the submation site of applicable to mathematication of the mating site of the submation site of applicable to mathematication of the maging site of the submation site of applicable to make site of the submation site of applicable to the submation site of the submation site of applicable to the submation site of the submation site of applicable to the submation site of the submati	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is abruical and advance access to audit bas restricted to authorized personnet? Core you provide evidence that due diligence mapping of regulations and standards to your controls/irechitecture/processes has been and/more? Are audit loss crucinally along and entrained? Are audit loss crucinally along and entrained? De you go and alert any change made to virtual machine mages regardless of their running state (e.g., dormant, off or running)? Do she virtual machines management infrastructure include a tamper audit or software integrity function to detect danges to be build (onlignation of the virtual machine?) Are changes made to virtual machine.	X	x x x	x	
Management Ubliky Programs Infrastructure & Virtualization Security Audit Logang / Intrusion Detection Infrastructure & Virtualization Security	IVS-01	NS-01.1 NS-01.2 NS-01.3 NS-01.4 NS-01.5 NS-02.1 NS-02.2	virtual machine, and application controls shall be restricted. Higher levels of assurance are required for protection, retention, and Higher levels of assurance are required for protection, retention, and Higher levels of assurance are required to the applicable types, statutory or regulatory compliance obligations and providing unique sure access constability to detect potentially supports methods the higher statutory file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all innee. Any changes made to virtual machine images must be logged and an aler trader regardless of their running state (e.g., domain, off, or running). The results of change or more of an image and the ubsequent	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personnel? Cause purp provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed? Are audit logs reviewed in a regular basis for security events (a.e., with automated tools)? Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect danges to the addiconfiguration of the virtual machine?	x	x x x x x x	x	
Management Unliky Programs Infrastructure & Virtualization Security Intrusion Detection Infrastructure & Virtualization Security Covid Infrastructure & Virtualization Security Covid Security Covid	NS-01 NS-02 NS-03	NS-011 NS-012 NS-013 NS-014 NS-014 NS-015 NS-022 NS-022 NS-021	virtual machine, and application controls shall be restricted. Higher levels of assumce are required for protection, televition, and Higher levels of assumce are required for protection, televitian of the region and the region of the providing unique user access or regulatory compliance obligations and providing unique user access the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images at the users of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an after trader regardless of their running state (e.g., domain, off, or running). The results of a change or more of a minee and the ubsequent violation of the image's integrity more the immediately availed to synchronize the system cocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit togs restricted to authorized personnel? Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been aefformed? Are and togs controlly along due training? Dees the virtual machine management infrastructure incide a tamper audit or software integrity function to detect danges to be addictoring crained the virtual machine images regardless of their running state (e.g., domant, off or running?) Does the virtual machine, or moving of an image and subsequent validation of the image's integrity, made immediately adable to customent function (e.g., NTP) to ensure all systems have a common time reference? Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	x	x x x x x	×	
Management Usilip Programs Infrastructure & Virtualization Security Adult Logong / Intrastructure & Virtualization Change Detection Infrastructure & Virtualization Security Clock Geol Infrastructure & Virtualization	IV5-01 IV5-02	NS-01.1 NS-01.2 NS-01.3 NS-01.4 NS-02.1 NS-02.2 NS-02.2	virtual machine, and application controls shall be restricted. Higher levels of assume are required for protection, resention, and Higher levels of assume are required for providing unique, statustry, are regulatory compliance obligations and providing unique user access constability to descript providing unique user access the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and times. Any changes made to virtual machine images at all times, the changes made to virtual machine images at all times. Any changes made to virtual machine images at all times, the change of the change of most of a mixing and the ublexpean virtuation of the image's integrity must be immediately available to arychnoise the system closel of all releases. Any evolution to arychnoise the system closel of all releases the solution of the indigity agreed upon external time source shall be used yution to facilitate uraxing and reconstitution of activity timelines. The availability, suital and measure to define the required system to facilitate, and measure to define the required system to facilitate and mustally agreed upon external time source shall be applianded, program, of measure to the the required system to facilitate, and measure to the the required system to facilitate the acting and reconstitution of activity timelines. The availability, suitable to applicate the required system to facilitate the required system to facilitate the acting and reconstitution of activity for the required system to facilitate the required system to facilitate the required system to facilitate the acting and reconstitution of activity for the required system to facilitate the required system to facil	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personnel? Are add tog creating and the alignment may be added to a strandards to your controls/architecture/processes has been performed? Are add tog creating and retained? Are add tog creating and retained? Do you period and any changes made to virtual machine images regardless of their running state (e.g., domant, off or running?) Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the addiconfiguration of the virtual machine, or moving of an image rapidless of their running state (e.g., domant, off or running?) Do you log and add art of virtual machine, or moving of an image rapidless of their virtual machine, mages integrity, made immediately available to customens through electronic methods (e.g., portails or altric)? Do you use a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network, storage, memory, UO, etc.) oversubscription you matinian and under kind circumaticates (changes) what levels of system (e.g., network, storage, memory, UO, etc.) oversubscription you	x	x x x x x x	x	
Management Usilip Programs Infrastructure & Virtualization Security Audit Logging / Intrusion Detection Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Cost Biomannation	NS-01 NS-02 NS-03	NS-011 NS-012 NS-013 NS-014 NS-014 NS-015 NS-022 NS-022 NS-021	virtual machine, and application controls shall be retricted. Higher levels of assumace are required for protection, retention, and Higher levels of assumace are required for protection, retention, and Higher levels of assumace are required for providing unique user access constability to detect potentially support to providing unique user access the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and after rised regretes of their running levels. (If or any constraints) after rised regretes of their running levels (e.g., domand, off, or unning). The results of a change or more of an image and the ubsequent after rised regretes of their running levels. A reliable and mutually agreed upon external time surves shall be used to rundentee theory dust of acle on a constraint dimetable. A reliable and mutually agreed upon external time surves shall be used to rundentee modes of all reliables in the running structures. The availabling, walking, and reconstitution of activity timelines. The availabling, walking and reconstitution of activity timelines. The availabling, walking, and devalue capacity and reconstres thall be performance in accordance with legal, statutory, and requirests	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to includents? is physical and logical user access to audit logs restricted to authorized personnel? Can you provide extent but due diligence mapping of regulations and standards to your controls/architecture/processes has been aerformed? Are audit logs creating stored and realized the site of the standards to their naming state (e.g., domant, off or running)? Do you log and altert any changes made to writual machine images regulations and standards toblo? Do you log and altert any changes made to writual machine images regulated to their running state (e.g., domant, off or running)? Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the bald/ordinguation of the image's integrity, made immediately makine? Are cauged made to virtual machine, and machine? Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) ovecus/uscription you	x	x x x x x x	x	
Management Unling Pergament Unling Pergament Security Audit Logging / Intrusion Detection Intrusion Detection Intrusion Detection Security Change Detection Infrastructure & Virtualization Security Cash Security Change Detection Infrastructure & Virtualization Security Cash Security Cash Detection Infrastructure & Virtualization	N5-03 N5-03 N5-04	NS-01.1 NS-01.2 NS-01.2 NS-01.3 NS-01.4 NS-02.2 NS-02.3 NS-03.1 NS-03.1 NS-03.1 NS-03.1 NS-03.2 NS-04.4	virtual machine, and application controls shall be restricted. Higher levels of assurance are required for protection, steeholder, and Higher levels of assurance are required for providing unique user access interview management of sublishing, shafting to applicable legal, substruty, are regulated contently supports network behaviors and or file integry anomalies, and to support forensic investigative capabilities in the event of a security breach. The provider shaft ensure the integrity of all virtual machines images at all times, Any changes made to white the capabilities in the event of a security breach. The provider shaft ensure the integrity of all virtual machines images at all times, Any changes made to white the capabilities in a lett runker regression of their uning level capabilities to reactioners. Thereas the integrity of all virtual machines images at all times, Any changes made to white the capabilities to reactioners. The results of a change or more of an image and the subseque advirtual of the results are the capabilities to reactioners through technologi and a contrain effective the systeme of the actions and provides of their uning and the capabilities to reactioners through technologi and a clearly timediately available to reactioners through advirtume acquestive than the machine images The availability, submy, and adequate to supervise that the technologi and provides and the subsequence with blgs, attraction, and requires that the manded to all results the delays the requirements shall be made to mitigate the risk of system overlaad.	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personnel? Can you provide enter that due diligence mapping of regulations and standards to your controls/architecture/processes has been aerformed? Are audit log contrady stored and retained? Are audit logs retended in a required train detection (IDS) tools implemented toohs? Does the virtual machine management infrastructure incide a tamper audit or software integrity function to detect danges to the audit control are audit on a store and and and and toohs? Does the virtual machines on rowing of an mage regurdless of their running state (e.g., dormant, off or running?) Does the virtual machines, or rowing of a mage regurdless of their running state (e.g., dormant, off or running?) Does the virtual machines, or rowing of a mage and subsequent validation of the image's integrity, made immediately available to contorness through electronic methods (e.g., portal or alerts)? Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you vide documentation regarding what leves of system (e.g., network?), IO, etc.; oversubscription you maintain and under dicrumstructure (protocol for system (e.g., network?)). Do you service to do mere material constructure in the hypervisor? Do you service to do mere material constructions to the interacture integrity to the time exervice protocol (e.g., NTP) to ensure all system have a common time reference? Do you service to constructure to the memory veersubscription you maintain and under coursers the runnel machine integration what leves the hypervisor? Do you service to do mere material regarding what leves to rystem (e.g., network?). Do you service to a coursers the time advisor to coursers to the hypervisor? Do you service to an early the	x	x x x x x x x	x	
Management Usilip Programs Infrastructure & Vertualization Security Adult Logong / Intrusion Detection Infrastructure & Vertualization Change Detection Change Detection Infrastructure & Vertualization Security Vertualization Security Vertualization Security Vertualization Security Vertualization Security Vertualization Security Vertualization	NS-01 NS-02 NS-03	NS-011 NS-012 NS-013 NS-013 NS-013 NS-021 NS-022 NS-023 NS-031 NS-031 NS-031 NS-042 NS-043	virtual machine, and application controls shall be restricted. Higher levels of assurance are required for protection, steenstore, and Higher levels of assurance are required for providing unique user access traces and the steenstore of the applicable legal statustory, or regulatory compliance obligations and providing unique user access the event of a security breach. The event of a security breach. The event of a security breach the integrity of all virtual machines images at all and the security breach. The event of a security breach the event of a security breach the event of a security breach. The event of a security breach the event of a security breach the event of a security breach the event of a security breach. The evolved shall ensure the integrity of all virtual machines images at all and the security breach. The evolved shall ensure the integrity of all virtual machines images at all and the security breach. The evolved shall ensure the integrity of all virtual machines images at all and the security breach. The evolved shall ensure the integrity of all virtual machines images at all and the security breach. The evolved shall ensure the integrity of all relevant information processing systems to facilitate tracing and recomstitution of activity timelines. The evolution of the security and the source shall be used to syndromize the system (backs of all relevant information processing and recomstitution of activity timelines. The evolution of the source black is a source shall be used to syndromize an account the system system shall ensure that the equived system for an example of the source black is a source shall be used to syndromize an account the system system shall ensure that the equived system for an example of the source black is a source shall be used to a releval at the source shall be used to a releval at the source shall be used to a releval at the source shall be source shall be a releval at the source shall be source shall be a releval at the source shall be source shall be	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physicial and logical user access to audit logi restricted to authorized personnel? Carbo you provide evidence that due elligence mapping of regulations and standards to your controls/architecture/processes has been aerformed? Are addit logic reviewed on a regular basis for recurity events (e.g., with automated tools)? Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the data data data of tools of the virtual machine magers may change and to be virtual machine imager regulations of software integrity function to detect changes to the addition of the image's integrity, made immediately available to customers through destructions change of a system (e.g., enternat; of or running state (e.g., domant, off or running state long). Do you use a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and unders circuitar enclose the integration to the integration with a lancabilities present in the hyperviso? Do you provide documentation regarding what levels of system (e.g., network, data datacplated pacity resets for all systems used to asynther running state integrity made integrity mode documentation integriting what levels of system (e.g., network, datacplated pacity resets for all systems used to asynthere into the hyperviso? Do you provide documentation regarding what levels of system (e.g., network, datacplated pacity resets for all systems used to asynthere into and in order to continuously meet regulatory, constactual, and busines requirements for all the system runnar.	x x	x x x x x x x	x	
Management Unling Pergament Unling Pergament Security Audit Logging / Intrusion Detection Intrusion Detection Intrusion Detection Security Change Detection Infrastructure & Virtualization Security Cash Security Change Detection Infrastructure & Virtualization Security Cash Security Cash Detection Infrastructure & Virtualization	N5-03 N5-03 N5-04	NS-01.1 NS-01.2 NS-01.2 NS-01.3 NS-01.4 NS-02.2 NS-02.3 NS-03.1 NS-03.1 NS-03.1 NS-03.1 NS-03.2 NS-04.4	virtual machine, and application controls shall be restricted. Higher levels of assurance are regulated for protection, retention, and Higher levels of assurance are regulated for providing unique user access accountability to detect potentially support to applicable tegat, statutory, or regulatory compliance obligations and providing unique user access the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images at all times. Any changes made to virtual machine images at all times, Any changes integrity and the equivalence of the simulation alter trainer organizes of their running levels. (If, or running). The results of a change or move of an image and the subsequent diater to inter organizes of their running levels. (If, or running). The results of a change or move of an image and the subsequent productions of the images in the equivalence of the simulation of productions the support networks of a change or move of an image and the subsequent productions the support networks of all extrast equivalences of productions the support networks of all extrast equivalences of the simulation of the support systems to facilitate tracing and reconstitution of activity timelines. The availability, quality, and adequate capacity and resources hall be planned, regrared, and measured to deliver the required system performance in according to the ford option evolution. The results of to make to might en text of system evolution.	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and balance access to audit logs restricted to authorized personnel? Are audit and investigation access to audit logs restricted to authorized personnel? Are audit and environment of the state and the structure processes has been any provide exceed on a regulate balance mapping of regulations and anadards to your control/urchitecture/processes has been any provide exceed on a regulate balance in structure processes has been approved exceed on a regulate balance in structure person (and the structure) and the structure of	x	x x x x x x x x x x x x x	x	
Management Usilip Programs Infrastructure & Virtualization Security Adult Loging () Infrastructure & Virtualization Change Detection Infrastructure & Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security	N5-63 N5-62 N5-63 N5-63	N5-011 N5-012 N5-013 N5-013 N5-013 N5-013 N5-022 N5-023 N5-023 N5-023 N5-021 N5-021 N5-021	virtual machine, and application controls shall be restricted. Higher levels of assume are required for protection, retention, and Higher levels of assume are required for protection, retention, and Higher levels of assume are required for providing unique user access constability to descript the providing unique user access accontability to descript the strength of all virtual machine images at all the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and times, and to usoport forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and times. Any changes made to virtual machine images must be logged and to change, The results of a change or more of a mixing and the usor-gene virtuation of the image's integrity must be immediately available to relationer through and measure to determine the required systems of the folder of the image's integrity must be immediately available to advictionic the system codes of all releases of the required systems to folder the required systems of the folder of the measure to determine the required systems of the indicate the virtualization technologies used and advictionic the system overbad. The availability, suitable capacity and reconstruction all adviction are more accordance with legal, statutory, and regulatory compliance. biggitate the risk of system overbad. Implements shall be must the the scurity vibrariability assument to folder to restrict and monitor staffic between turbined and configured to restrict and monitor traffic between turbined and configured to restrict and monitor traffic between turbined and and to minging the risk of system overbad.	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root ause analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personnel? Can you provide workene that due elignene mapping of regulations and standards to your controls/architecture/processes has been aerformed? Are audit log contrally stored and retained? Are audit log contrally stored and retained? Are audit log contrally stored and retained? Are audit log controlly stored and retained? Are changes made to virtual machine mages regardless of their running state (e.g., domant, off or running)? Do you log and after their virtual machine images regardless of their running state (e.g., domant, off or running)? Do you use a synchronised time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you use a synchronised time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you synchronised time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you work do countershiltion requiring what levels of hystem (e.g., network, VIO, etc.) oversubscription public eligible to countershiltion requiring workshilting to the memory. Do you work do the memory veersubscription capabilities present in the hypervisio? Do you sereft stute of the memory veersubscription capabilities	x	x x x x x x x x x x x x	x	
Management Usilip Programs Infrastructure & Virtualization Security Autraliant Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Cock Security Cock Security Cock Security Cock Security Capacity / Resource Biofrastructure & Virtualization Security Capacity / Resource Biomony	N5-63 N5-62 N5-63 N5-63	N5-011 N5-012 N5-013 N5-013 N5-013 N5-013 N5-022 N5-023 N5-023 N5-023 N5-021 N5-021 N5-021	virtual machine, and application controls shall be retricted. Figher levels of assume are required for protection, retention, and Figher levels of assume are required for providing unique user access control to add togs, athretic to applicable teggs, statutory, or regulatory compliance obligations and providing unique user access control to a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images at all times. Any changes made to virtual machine images at all times, Any changes made to virtual machine images at all times. Any changes made to virtual machine images at all times. Any changes made to virtual machine images at all times. Any changes made to virtual machine images must be legged and a letr roiser ographs therging must be leg. adomnot. Aff or running. The results of a change or more of an image and the subsequent optimizer to facilitate tracing and reconstitution of activity timelines. The availability, quality, and adequate capacity and resources shall be planned, prepared, and measure to deliver the required system performance in according of thus counting endust. The availability, quality, and adequate capacity and resources thal be planned, prepared, and measure to deliver the requirements shall be induce to might end of a plane endust. The availability, quality, and adequate capacity and resources thal be planed, prepared, and measure to deliver the requirements shall be induce to might end of a plane needbal. The environments that the security vulnerability assessment toxis or services accommodate the virtualization and the univerball. The environments that dividual instances shall be delivered instances	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root acuse analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personnel? Can you provide expresses that due filemen mapping of regulations and standards to your controls/architecture/processes has been performed? Are audit log centrally stored and retained? Do you log and add and the structure thouse a tamper audit or software integrity function to detect changes to the addition for structure though expression? Do you be and add and the structure thouse a tamper audit or software integrity function to detect changes to the addition for structure though expression? Do you be and add and the structure thouse integrity function of the image's integrity, made immediately available to customers through descritorin methods (e.g., portals or alerts)? Do you be any shorthy integriting what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you Do you sport do townershorthy computing the levels of system (e.g., network, add anticipated capacity needs for all systems used to provide storementation used in used in order to constituuely meet regulatory, contractual, and business requirements for all systems contractures and the integrity and anticipated capacity needs for all systems anarrand. Is system performance monoteed and and lowed in o	x	x x x x x x x x x x x x x x x	x	
Management Usilip Programs Infrastructure & Virtualization Security Adult Loging () Infrastructure & Virtualization Change Detection Infrastructure & Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security	N5-63 N5-62 N5-63 N5-63	N5-011 N5-012 N5-013 N5-013 N5-013 N5-013 N5-022 N5-023 N5-023 N5-023 N5-021 N5-021 N5-021	virtual machine, and application controls shall be retricted. Higher levels of assume are required for protection, retention, and Higher levels of assume are required for providing unique user access (Higher levels of assume are required for providing unique user access controllity to devel potentially support forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be legged and a lett rusient egregative length of the length of the development of the security threach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be legged and a lett rusient egregative length of the length of the development of the security operation. The availability, quality, and adequate capacity and resources shall be planned, programe, and reasons of their running enquirements shall be randoms endipsion for the running enduity. The availability, quality, and adequate capacity and resources shall be planned, programe, and reasons of the integrity virtual resources shall be planned, programe, and reasons of their running enquirements shall be randoms. Projections of future capacity requirements shall be randoms revisions and reconstructions of capacity. The work environments and virtual instances shall be existent for the required share shall be profinance in accounted the virtual lations technologies used (e.g., The environment share complex shall be reviewed at least annuality, and projective ba downer methy lations and be used for all share annuality. The over environments and virtual lations techn	monitorest? Are file integrity (host) and network: intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physicial and togical war access to audit logs restricted to authorized personnel? Can you provide evidence that due dilgence mapping of regulations and standards to your controls/architecture/processes has been arritering? Are file integrity (host) and network? Are provide evidence that due dilgence mapping of regulations and standards to your controls/architecture/processes has been arritering? Are provide evidence that due dilgence mapping of regulations and standards to your controls/architecture/processes has been arritering? Are provide and attents of arstenide? Do you log and alter any change made to virtual machine image regulates of their running state (e.g., domant, off or running)? Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the beddictoring arritering in their start use include a tamper audit or software integrity function to detect changes to the beddictoring arritering include is a start of a start off and their start use and their start off the image's integrity, made immediately publicle to continuents include integritor arbitrary in advectoring of an image and subsequent validation of the image's integrity, made immediately public to continuents include integritor arbitrary in advectoring of a manage and subsequent validation of the image's integrity, made immediately public to continuents in the hypervisor? Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network, storage, memory, UO, etc.) oversubscription causes and the integrity restructure of the integrity in the integrity integrity, integrity, neade integrity restructor? Do you urgital to not the transity on the into conti	x x	x x x x x x x x x x x x x x x x x x	x	
Management Usilip Programs Infrastructure & Virtualization Security Addit Logong/ Infrastructure & Virtualization Security Change Detection Change Detection Change Detection Change Detection Change Detection Change Detection Change Detection Security Change Detection Change Detection Security Change Detection Security Change Detection Security Change Detection Security Change Detection Security Change Detection Security Change Detection Security Change Detection Security Change Detection Security Change Security Change Security Infrastructure & Security Network Security Infrastructure & Security Network Security	N5-63 N5-62 N5-63 N5-63	N5-011 N5-012 N5-013 N5-013 N5-013 N5-013 N5-022 N5-023 N5-023 N5-023 N5-021 N5-021 N5-021	virtual machine, and application controls shall be restricted. Higher levels of assume are required for protection, resention, and Higher levels of assume are required for providing unique user access direction management of audit logs, abinery to applicable legit, statutory, or regulatory compliance obligations and providing unique user access accontability to descript the support forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and aber 1 raiset rights of their running legit, add on the logged and aber 1 raiset rights of their running legit, add on the logged and aber 1 raiset rights of their running legit, add on the logged and aber 1 raiset rights of their running legit, add on the logged and aber 1 raiset rights of their running legit, add on the logged and aber 1 raiset rights of their running legit, add on the logged and aber 1 raiset rights of their running legit, add on the running legit visitistion of the image's integrity must be immediately available to running and musually agreed upon external time sources shall be seed profermance in accordance with legal, statutory, and regulatory complance, obligating, for disrupt and legit, add their running and the running performance in accordance with legal, statutory, and regulatory complance obligation aware). The availability, tunial deputies capacity are resources shall be and to mighter the risk of system overbad. Insplementers shall ensure the the security vulnerability basessment tools or services accomparisons shall be knowed and unived and supported by a documented particulation technologies used (e.g., trustation aware). Each operating system shall be hardened to provide only another theory and the mighter the risk of system overbad. Each operating system shall be hardened to provide only mecessary ports.	monitorest? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by foot cause analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personned? Can you provide evidence that due diligence mapping of regulations and tanadards to your controls/architecture/processes has are audit logs restricted on a regular bank for scury events (e.g., with automated tooh)? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the additorofing attained the duritum dimking. Do you use any and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the additorofing attaine to strugget makes to virtual machine, or noving of an image and subsequent validation of the image's integrity, made immediately additorofing attaine torugh encounce and uses at the structure and uses a structure include a tamper audit or software integrity function to detect changes to the additorofing attaine torugh encounce and uses at the structure and uses at the structure and use at the structure and use at the structure and uses at the structure and the structure and uses at the structure and uses at the structure and use and uses and use and use and use at the structure and uses at the structure and use at the structure and use at the structure and users at the structure and uses	x x	x x x x x x x x x x x x x x x x x x	x	
Management Usilip Programs Infrastructure & Virtualization Security Addit Logong/ Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Change Detection Change Detection Change Detection Virtualization Security Change Detection Security Change Detection Security Comparison Security Change Detection Security Change Detection Security Change Detection Security Change Detection Security Security Change Detection Security Security Change Detection Security Security Security Change Detection Security Security Security Change Detection Security Security Security Change Detection Security Securit	N5-63 N5-62 N5-63 N5-63	N5-011 N5-012 N5-013 N5-013 N5-013 N5-013 N5-022 N5-023 N5-023 N5-023 N5-021 N5-021 N5-021	virtual machine, and application controls shall be restricted. Higher levels of assume are required for protection, retention, and Higher levels of assume are required for protection, retention, and Higher levels of assume are required for providing unique user access constability observed proteining support forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and a leter raiser capacitors) of the running level level. Control of the level of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine level, so domain, of, or running. The results of a change or move of an image and the subspection a leter raiser capacitors) there more level in the running structure shall be used to running. The results of a change or move of an image and the subspection a lett raiser capacitor of level running level. Control or admitsh experiments that a change or move of an image and the subspection running. The results of a change or move of an image and the subspection running. The results of a change or move of an image and the subspection running. The results of a change or move of an image and the subspection running. The results of a change or move of an image and the subspection running. The results of a change or move of an image and the subspection running. The results of a change or move of an image and the subspection running. The results of a change or move of an image and the subspection running. The running of the running structure shall be used to running in the runner based or the running structure shall be running and mountably agreed upon external time sources hall be running and mountably agreed upon external time sources hall be running and mountably agreed upon external time sources hall be running and mountably agreed upon external time sources hall be running and runn	monitorest? Are file integrity (host) and network: intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physicial and togical war access to audit logs restricted to authorized personnel? Can you provide evidence that due dilgence mapping of regulations and standards to your controls/architecture/processes has been arritering? Are file integrity (host) and network? Are provide evidence that due dilgence mapping of regulations and standards to your controls/architecture/processes has been arritering? Are provide evidence that due dilgence mapping of regulations and standards to your controls/architecture/processes has been arritering? Are provide and attents of arstenide? Do you log and alter any change made to virtual machine image regulates of their running state (e.g., domant, off or running)? Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the beddictoring arritering in their start use include a tamper audit or software integrity function to detect changes to the beddictoring arritering include is a start of a start off and their start use and their start off the image's integrity, made immediately publicle to continuents include integritor arbitrary in advectoring of an image and subsequent validation of the image's integrity, made immediately public to continuents include integritor arbitrary in advectoring of a manage and subsequent validation of the image's integrity, made immediately public to continuents in the hypervisor? Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network, storage, memory, UO, etc.) oversubscription causes and the integrity restructure of the integrity in the integrity integrity, integrity, neade integrity restructor? Do you urgital to not the transity on the into conti	x x x	x x x x x x x x x x x x x x x x x x	x	
Management Usilip Programs Infrastructure & Virtualization Security Addit Logong/ Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Cook Security Cook Security Netherland Security Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization Security Infrastructure & Virtualization	N5-63 N5-62 N5-63 N5-63	N5-011 N5-012 N5-013 N5-013 N5-013 N5-013 N5-022 N5-023 N5-023 N5-023 N5-021 N5-021 N5-021	virtual machine, and application controls shall be restricted. Higher levels of assume are required for protection, retention, and Higher levels of assume are required for protection, retention, and Higher levels of assume are required for providing unique user access constability to detect potentially support to providing unique user access the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and a level takes and the support to the security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and a level takes and the support to the security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine levels, dommar, dir, or uningit. The results of a change or move of an image and the ubstepend a level takes and the support of the security levels. A reliable and mutually agreed upon external time sources shall be used proferomice the system closel of all retermines the required tayling registrem to facilitate tracing and reconstitution of activity timelines. The availability suality, and advance tapkely and reconstructs that be made to mitigate the risk of system overload. Implementers shall ensure that the security vulnerability assessment tools or arrorizes accommodate the virtualization technologies using effort on the system overload. Implementers shall ensure that the security vulnerability sustements shall be made to mitigate the risk of system overload. Eich operating pytom thall be backmed to provide only necessary ports, protocols, ports, and compensating controls.	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit tags restricted to authorized personnel? Can you provide ence that due filingence mapping of regulations and standards to your controls/architecture/processes has been aerformed? Are addit logic reteared in a required tasks for security events (e.g., with automated tooh)? Does the virtual machine management infrastructure incide a tamper audit or software integrity function to detect changes to the disalidon of the image's integrity, made immediately audited contactions with automated to intra integrity function to detect changes to the disalidon file automated to evirtual machines or moving of an image regardless of their running state (e.g., dormant, off or running)? Does the virtual machines, or rowing of an image and subsequent validation of the image's integrity, made immediately audited to evirtual machines or rowing of an image and subsequent validation of the image's integrity, made immediately audited to evirtual machines or rowing of an image and subsequent validation of the image's integrity, made immediately audited to evirtual machines or rowing of an subsequent validation of the image's integrity, made immediately audited to evirtual machine imagering what levels of tystem (e.g., network, I/O, etc.) oversubscription you maintain and undre directurination: reported of (e.g., NTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of tystem (e.g., network, I/O, etc.) oversubscription rapadilities provide exacting the state integrity audited exacting exacting the termate? Do you provide documentation regarding what levels of tystem (e.g., network, I/O, etc.) oversubscription rapadilities provide exacting the termate? Do you provide documentation required to the termate? Do you provide documentation required to the	x	x x x x x x x x x x x x x x x x x x	x	
Management Usilip Programs infrastructure & Virtualization Security Addit Loging / Intrusion Detection Infrastructure & Virtualization Security Clampe Detection Infrastructure & Virtualization Security Capacity / Resource Journalization Security Virtualization Security Virtualization Security Network Security Network Security Network Security Network Security Network Security Network Security Network Security Infrastructure & Virtualization Security Network Security Network Security Infrastructure & Virtualization Security Network Security Infrastructure & Virtualization Security Network Security Infrastructure & Virtualization Security Network Security Infrastructure & Virtualization Security Network Security Infrastructure & Virtualization	NS-63 NS-62 NS-63 NS-64 NS-65 NS-65 NS-65	N5-011 N5-013 N5-013 N5-014 N5-014 N5-013 N5-022 N5-023 N5-011 N5-023 N5-011 N5-024 N5-021 N5-021 N5-021 N5-021 N5-021 N5-021	virtual machine, and application controls shall be retricted. Higher levels of assume are required for protection, retention, and Higher levels of assume are required for protection, retention, and Higher levels of assume are required for providing unique user access controllity to detect potentially support to remain investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and a let traiser regards to their summission to the security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and a let traiser regards of their running let e G_a, dormat, Of, or running. The results of a change or move of an image and the subsequent and and mustary strength must be let G_a, dormat, Of, or running. The results of a change or move of an image and the subsequent and and mustary strength must be information processing systems to facilitate tracing and recourses half be used to planned. Insprande, and measure to defiver the required system programme objection does do if relevant, and required system programme objection and virtual instanctiones thalf be ande to mitigate the risk of system overload. Implementers shall be hardmend to provide only necessary ports, protoch, ports, and compensating controls. Each operating system shall be hardmend to provide only necessary ports, protoch, and services to method sole and ensure, protoch, and services to method sole and ensure the sequented providement for a discust and overlaps. The absence operation is all be provided to a stread services the method sets shall be provided to a stread sets or changes to a stread sets annually, and provide to a stread sets or changes to a stread set and annually, and provide to a stread sets or changes to a stread set annually, and provide to a stread sets or changes to a stread set annually, and provid	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit togs restricted to authorized personnel? Can our provide evidence that due alignence mapping of regulations and standards to your controls/architecture/processes has been aerformed? Are addit logic reviewed to a regular basis for security events (e.g., with automated tools)? Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the disability of evidence of the virtual machine images regardless of their running state (e.g., dormant, off or running)? Does the virtual machines, or rowing of an image regardless of their running state (e.g., dormant, off or running)? Does the virtual machines, or rowing of an image and subsequent vulidition of the image's integrity, made immediately available to contoments through electronic methods (e.g., portal or alerts)? Do you use anyority-inted time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription russing to autoalisticate present in the hyperviso? Do security viewer and the circumstance/changes in the account common time reference? Do you provide documentation regarding what levels of system (e.g., network, usorage, memory, I/O, etc.) oversubscription russing and they in auto-russing of system (e.g., network, viewer methods for all systems usot Does your yetwork encortered and then in order to continuously meet regulatory, contractual, and business requirements for all the voider uncircles to auto-russing whereas to the tenant? Do our curve systemes monitored and then in order to continuously meet regulatory, contractual, and business requirements for all the uncernor. System peformance monitored and then		x x x x x x x x x x x x x x x x x x	x	
Management Usilip Programs Infrastructure & Virtualization Security Addit Loging/ Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Change Detection Change Detection Infrastructure & Virtualization Security Change Detection Security Change Change Security Change Change Security Change Change Security Change Change Security Change Change Security Change Change Security Change Change Security Change Change Security Change Change Security	NS-63 NS-62 NS-63 NS-64 NS-65 NS-65 NS-65	N5-011 N5-013 N5-013 N5-014 N5-014 N5-013 N5-022 N5-023 N5-011 N5-023 N5-011 N5-024 N5-021 N5-021 N5-021 N5-021 N5-021 N5-021	virtual machine, and application controls shall be restricted. Higher levels of assurance are required for protection, retention, and Higher levels of assurance are required for providing unique user access required to application of shall be, advirtual to applicable legal, statutory, or regulatory compliance obligations and providing unique user access the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and a letr revised regulatory therefore the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and a letr revised regulatory therefore the level of a line and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the ubbegoed mathematication of the imaging virtual machine images and the images of the imaging virtual machine images and the ubbegoed mathematication of the image of the imaging virtual virt	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit tags restricted to authorized personnel? Can you provide ence that due filingence mapping of regulations and standards to your controls/architecture/processes has been aerformed? Are addit logic reteared in a required tasks for security events (e.g., with automated tooh)? Does the virtual machine management infrastructure incide a tamper audit or software integrity function to detect changes to the disalidon of the image's integrity, made immediately audited contactions with automated to intra integrity function to detect changes to the disalidon file automated to evirtual machines or moving of an image regardless of their running state (e.g., dormant, off or running)? Does the virtual machines, or rowing of an image and subsequent validation of the image's integrity, made immediately audited to evirtual machines or rowing of an image and subsequent validation of the image's integrity, made immediately audited to evirtual machines or rowing of an image and subsequent validation of the image's integrity, made immediately audited to evirtual machines or rowing of an subsequent validation of the image's integrity, made immediately audited to evirtual machine imagering what levels of tystem (e.g., network, I/O, etc.) oversubscription you maintain and undre directurination: reported of (e.g., NTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of tystem (e.g., network, I/O, etc.) oversubscription rapadilities provide exacting the state integrity audited exacting exacting the termate? Do you provide documentation regarding what levels of tystem (e.g., network, I/O, etc.) oversubscription rapadilities provide exacting the termate? Do you provide documentation required to the termate? Do you provide documentation required to the	x	x x x x x x x x x x x x x x x x x x	x	
Management Usilip Programs infrastructure & Virtualization Security Adult Loging / Infrastructure & Virtualization Champe Detection Infrastructure & Virtualization Security Champe Detection Infrastructure & Virtualization Security Copyoly / Resource Paraming Infrastructure & Virtualization Security Network Security Infrastructure & Virtualization Security Description Infrastructure & Virtualization Security Description Infrastructure & Virtualization Security Description Infrastructure & Virtualization Security Description Production / Non- Production Environments	NS-63 NS-62 NS-63 NS-64 NS-65 NS-65 NS-65	N5-011 N5-012 N5-013 N5-014 N5-013 N5-023 N5-023 N5-023 N5-023 N5-023 N5-024 N5-024 N5-023 N5-024 N5-023 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025	virtual machine, and application controls shall be retricted.	monitorest? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personnel? Can you provide evidence that due elligence mapping of regulations and standards to your controls/architecture/processes has been aerformed? Are audit logic reviewed in a regular basis for accurate years (i.e.g., with automated tooh)? Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the balance integrity function to detect changes to the addition of the image's integrity, made immediate a startige and toops (i.e.g., dormant, off or running)? Does the virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through destructure include a tamper audit or software integrity function to detect changes to the balancian and under the virtual machine, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through destructure include (i.e.g., network, storage, memory, I/O, etc.) oversubscription your matian and under their curvatures conformation? Do you provide documentation regarding what levels of system (i.e.g., network, storage, memory, I/O, etc.) oversubscription your balancian and under in order to continuously meet regulatory, contractual, and business requirements for all the sorties used to arootide customers with guidance on how to create a layered security architecture equivalence using zive highly update antheories to the tennist? Do your regularly update antheories the allowed access/connectivity (i.e.g., frewall rules) between security domains/zones? Do your regularly update antheories the allowed access/connectivity (i.e.g., frewall rules) between security domains/zones? For your lass offering, do yo	x x x	x x x x x x x x x x x x x x x x x x x	x	
Management Usilip Programs Infrastructure & Vertualization Security Adult Loging / Infrastructure & Vertualization Security Chunge Detection Infrastructure & Vertualization Security Chunge Detection Infrastructure & Vertualization Security Chunge Detection Infrastructure & Vertualization Security Vertualization Security Vertualization Security Network Security Vertualization Security Network Security Network Security Infrastructure & Vertualization Security Network Security Infrastructure & Vertualization Security Network Security Infrastructure & Vertualization Security Network Security Infrastructure & Vertualization Security Infrastructure & Vertualization Security CS Infrastructure & Vertualization Security CS Infrastructure & Vertualization Security Pachecons	NS-03 NS-03 NS-03 NS-04 NS-04 NS-04 NS-04	N5-011 N5-012 N5-013 N5-014 N5-013 N5-023 N5-023 N5-023 N5-023 N5-023 N5-024 N5-024 N5-023 N5-024 N5-023 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025 N5-025	virtual machine, and application controls shall be retricted.	monitored? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cave analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personnel? Car you provide diverse that due difference mapping of regulations and tandards to your controls/architecture/processes has care addition prevents of a result hears for scale type and results? Are addition forevalue on a result hear for except your thick as tandards to your controls/architecture/processes has care addition forevalue on a result hear for except your thick as tandards to your controls/architecture/processes has care addition forevalue on a result hear for except your thick as tandards to your controls/architecture/processes has calculated to a result hear thear thick or except your thick as tandards to your controls/architecture/processes has calculated to a result hear thear thick or except your thick as tandards to your controls/architecture/processes has calculated to a result hear thear thick or except your thick as tandards to your controls/architecture/processes has calculated to a result hear thear thick or except your thick as a tandards to provide the image's integrity, made immediately addition for the image of the image matching of a lange and unders and under what circums hear to protocol (e.g., NTP) to ensure all systems have a common time reference? Do your use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do your use synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do your use your the memory version/circles cacculate previsor? Do your use your the terms to the terms of the intervisor? Do your use your the memory version/circles cacculate count curve, protected, and anticipated cacculate and yourses requirements for all the vortem under tool covide evices to the themats? Do except your base the terms	x	x x x x x x x x x x x x x x x x x x x	x	
Management Usilip Programs infrastructure & Virtualization Security Adult Loging / Intrusion Detection infrastructure & Virtualization Security Claunge Detection Claunge Detection Claunge Detection Claunge Detection Claunge Detection Security Claunge Detection Security Claunge Detection Security Virtualization Security Claunge Detection Security Virtualization Security Network Security Virtualization Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Infrastructure & Virtualization Security Claunge Detection Detection Claunge Detection Security Claunge Detection Network Security Claunge Detection Network Security Claunge Detection Network Security Production Environments Infrastructure & Virtualization	NS-03 NS-03 NS-03 NS-04 NS-04 NS-04 NS-04	NS 011 NS 013 NS 014 NS 014 NS 014 NS 014 NS 022 NS 023 NS 041 NS 041 NS 041 NS 041 NS 041 NS 042 NS 044 NS 041 NS 041 NS 042 NS 044 NS 041 NS 042 NS 041 NS	virtual machine, and application controls shall be restricted.	monitorest? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physical and logical user access to audit logs restricted to authorized personnel? Can you provide evidence that due diligence mapping of regulations and tandards to your controls/architecture/processes has are audit logs restricted to arc efficience mapping of regulations and tandards to your controls/architecture/processes has are audit logs restricted on a regulate basis for scuriny events (i.e.g., with automated tools)? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Do you log and alert any changes made to virtual machine images regardless of their running tate (e.g., dormant, off or running)? Do you log and alert any changes made to virtual machine images are subsequent validation of the image's integrity, made immediately add/configurations brough decourse brough a decourse brough a calcular setting are subsequent validation of the image's integrity, made immediately add/configurations brough decourse brough a decourse setting a systems have a common time reference? Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you system's capacity requirements bake into account current, projected, and anticipated capacity needs for all systems asset[] rainvide service the temant? Do you system's capacity requirements bake into account current, projected, and anticipated capacity needs for all systems asset[] rainvide service the temant? Do you regularly review for appropriateness the allowed access/connectivity domatin/cons? Do you regularly review for appropriateness the allowed access/connectivity equivalence using array of their appropriateness the allowed access/connectivity envirolages between security domatin/cons? Do you regularly review for appropriatene	x x 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 Usilip Programs infrastructure & Virtualization Security Adult Loging / Intrusion Detection infrastructure & Virtualization Security Claunge Detection Claunge Detection Claunge Detection Claunge Detection Claunge Detection Security Claunge Detection Security Claunge Detection Security Virtualization Security Claunge Detection Security Virtualization Security Network Security Virtualization Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Infrastructure & Virtualization Security Claunge Detection Detection Claunge Detection Security Claunge Detection Network Security Claunge Detection Network Security Claunge Detection Network Security Production Environments Infrastructure & Virtualization	NS-03 NS-03 NS-03 NS-04 NS-04 NS-04 NS-04	NS 011 NS 013 NS 014 NS 014 NS 014 NS 014 NS 022 NS 023 NS 041 NS 041 NS 041 NS 041 NS 041 NS 042 NS 044 NS 041 NS 041 NS 042 NS 044 NS 041 NS 042 NS 041 NS	vitual machine, and application controls shall be restricted.	monitorest? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Is physicial and logical user access to angle logs restricted to authorized personned? Can you provide evidence that due ellipseme mapping of regulations and tandards to your controls/architecture/processes has are and toge revealed on a regular bank for scarsby events (e.g., with automated tools)? Do you log and altert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Does the virtual machine management infrastructure induce a tamper audit or software integrity function to detect changes to the dial/configuration to the virtual machine, or noving of an image and subsequent validation of the image's integrity, made immediately makine to contemes through accounts emotion a cause the software autors and the exercises. Do you use a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you use synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you use synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you use synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you system's capacity requirements take into account current, projected, and anticipated capacity needs for all system is avaid additionable capacity needs to continuously meet regulatory, contractual, and busines requirements for all the virtual machine the remark? Do you system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used is corrispondent to covide arrives to the marks? Do you system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems avava?? For your task offering, do you provide cus	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 Usilip Programs infrastructure & Virtualization Security Adult Loging / Intrusion Detection infrastructure & Virtualization Security Claunge Detection Claunge Detection Claunge Detection Claunge Detection Claunge Detection Security Claunge Detection Security Claunge Detection Security Virtualization Security Claunge Detection Security Virtualization Security Network Security Virtualization Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Infrastructure & Virtualization Security Claunge Detection Detection Claunge Detection Security Claunge Detection Network Security Claunge Detection Network Security Claunge Detection Network Security Production Environments Infrastructure & Virtualization	NS-03 NS-03 NS-03 NS-04 NS-04 NS-04 NS-04	N5-011 N5-013 N5-014 N5-014 N5-013 N5-022 N5-023 N5-011 N5-021	virtual machine, and application controls shall be restricted. Figher levels of assume are required for protection, resention, and Figher levels of assume are required for providing unique user access figher levels of assume are required for providing unique user access constability obserts obserts the providing unique user access the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all fines. Any changes made to virtual machine images must be logged and the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all fines. Any changes made to virtual machine images must be logged and the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all fines. Any changes made to virtual machine images must be logged and the rest of the access of the moring the exploration. If or advert The registry of the integrity of all virtual machine images must be logged and the rest of the access of the moring the exploration. The washed to the moring the exploration end to the security violate to proferomice the system the level of access of the required system and is on things the tracing and reconstitution of activity timelines. The availability, sushall we capacity and reconstructes shall be parformance in accordance with legal, statutory, and regulatory compliance obligations. The fight the misser that the security violenability assument tobac moring motion the controls of all evelowed at least annualy, and supported by a documented justification for use for all allowed services, protocols, and services to method approximation status and supported by a documented justification for use for allowed services, protocols, and services to methor components, shall be dearged, developed, deployed, and contagioner shall be dearged, developed, deployed, and contagioner shall be dearged to restrict and monitor and received at least annualy, and supported by a documented justification fo	monitorest? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidence? Is physicial and logical user access to audit togs restricted to authorized personnel? Can you provide evidence that due allignece mapping of regulations and standards to your controls/architecture/processes has been enformed? Are addition controls are signaled to virtual machine images regardless of their running state (e.g., dormant, off or running?) Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the detection of their running state (e.g., dormant, off or running?) Does the virtual machines or moving and mage and subsequent validation of the image's integrity, made immediately available to contement from all extensions and uses equal validation of the image's integrity, made immediately available to contement from all extensions of system (e.g., network, storage, memory, UO, etc.) oversubscription you maintain and under their cummatices' controls (e.g., mitry) to ensure all systems have a common time reference? Do you use a synechronized time-service protocol (e.g., WTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network, storage, memory, UO, etc.) oversubscription you maintain and under their cummatices (controls)? Develow prove systems can be into accell correction projected, and anticipated capacity needs for all systems used to accride the memory versubscription capabilities proteinest in the hyperviso? Develow prove shore that cummatices (contentions) the instructure in the hypervisor? Develow tapetic tables that the other services commodate the virtualization technologies being used (e.g., virtualization and the system starts)? Develow tables to accorde services to the sensitize to accell tabused access/control starts to methodicated capacity dow	x x x x 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 Usilip Programs infrastructure & Virtualization Security Adult Loging / Intrusion Detection infrastructure & Virtualization Security Claunge Detection Claunge Detection Claunge Detection Claunge Detection Claunge Detection Security Claunge Detection Security Claunge Detection Security Virtualization Security Claunge Detection Security Virtualization Security Network Security Virtualization Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Claunge Detection Security Network Security Infrastructure & Virtualization Security Claunge Detection Detection Claunge Detection Security Claunge Detection Network Security Claunge Detection Network Security Claunge Detection Network Security Production Environments Infrastructure & Virtualization	NS-03 NS-03 NS-03 NS-04 NS-04 NS-04 NS-04	N5-01.1 N5-01.2 N5-01.2 N5-01.3 N5-01.3 N5-02.2 N5-03.3 N5-04.1 N5-04.1 N5-05.1 N5-06.1 N5-06.2 N5-06.3 N5-06.4 N5-06.4 N5-06.4	virtual machine, and application controls shall be retricted. Higher levels of assume are required for protection, retention, and Higher levels of assume are required for protection, retention, and Higher levels of assume are required for providing unique user access accontability to detect potentially support to ensist the solution and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all time. Any changes made to virtual machine images must be logged and after risker togeto the for running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after risker togetos) of their running levels (e.g., dommar, off, and after togetos) after togetos) after develses (e.g., dommar, off, and after togetos) after togetos) after develses (e.g., dommar, off, and after togetos) after togetos) after develses (e.g., dommar, off, and after togetos) after togetos) after develses (e.g., dommar, off, and after togetos) after deve	monitorest? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidence? Is physicial and logical user access to audit togs restricted to authorized personnel? Can you provide evidence that due allignece mapping of regulations and standards to your controls/architecture/processes has been aefformed? Are addition controls are single to virtual machine images regardless of their running state (e.g., dormant, off or running?) Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the detection of their running state (e.g., dormant, off or running?) Does the virtual machines or moving and mage and subsequent validation of the image's integrity, made immediately available to contense introduce (e.g., with automated tools)? Does you gain a synchronized time-service protocol (e.g., WTP) to ensure all systems have a common time reference? Do you use a synchronized time-service protocol (e.g., WTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network, storage, memory, UO, etc.) oversubscription you maintain and under their circumstrates/constraints? Do you avain a synchronized time-service protocol (e.g., WTP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network, storage, memory, UO, etc.) oversubscription you maintain and under their circumstratescription with the integrity of the memory oversubscription to memory and anticipated capacity needs for all systems used to accorde services to the tensors? Do you provide documentation regarding what levels of note the continuously meet regulatory, contractual, and business requirements for a the system sure to accorde services to the tensors? De you regulatry investion to asservices to the restructs a hyperode accurity avchi	x x x x x x x x x 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 Usilip Programs infrastructure & Virtualization Security Audit Loging / Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Cock Security Cock Security Virtualization Security Network Security Network Security Network Security Network Security Network Security Hinfrastructure & Virtualization Security Network Security Network Security Security Network Security Network Security	NS-63 NS-62 NS-63 NS-64 NS-66 NS-66 NS-66	NS-01.1 NS-01.2 NS-01.2 NS-01.3 NS-01.3 NS-01.3 NS-01.3 NS-01.3 NS-01.3 NS-02.2 NS-03.3 NS-04.1 NS-04.1 NS-04.1 NS-05.1 NS-06.1 NS-06.3 NS-06.4 NS-06.1 NS-06.2 NS-06.2 NS-06.3 NS-06.4 NS-06.1 NS-06.2 NS-06.3 NS-06.4 NS-06.3 NS-06.4 NS-06.1 NS-06.2 NS-06.3 NS-06.3 NS-06.4 NS-06.3 NS-06.4 NS-06.3 NS-06.4 NS-06.4 NS-06.5	virtual machine, and application controls shall be restricted.	monitorest? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by rote cause analysis, and response to incidents? Is physicial and logical user access to audit togs restricted to authorized personnel? Can you provide ordence that due allignece mapping of regulations and standards to your controls/architecture/processes has been serformed? As audit logic undere add on strained? Are changes made to virtual machine mages regardless of their running state (e.g., domant, off or running?) Do you use a synchronized time-service protocol (e.g., VPI) to ensure all systems have a common time reference? Do your use a synchronized time-service protocol (e.g., VPI) to ensure all systems have a common time reference? Do your ower asynchronized time-service protocol (e.g., VPI) to ensure all systems have a common time reference? Do your ower asynchronized time-service protocol (e.g., VPI) to ensure all systems have a common time reference? Do your ower asynchronized time-service protocol (e.g., VPI) to ensure all systems have a common time reference? Do your ower asynchronized time service to continuously meet regulatory, contractual, and business requirements for a system runned to diverse to obte services a context subscription requires the means? Do security whereability assessment tools of service accommodate the virtualization technologies being used (e.g., virtualization the system used to arrowide and under in order to continuously meet regulatory, contractual, and business need using a system performance montower obte or service accommodate the virtual machine analysis. Do your runnel whereability assessment tools of service accommodate the virtualization technologies being used (e.g., vir	x x x x x x x x 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 Usilip Programs Infrastructure & Virtualization Security Andit Logging / Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Cock Security Cock Security Cock Security Cock Security Cock Security Cock Security Cock Security Cock Security Cock Security Cock Security Infrastructure & Virtualization Security Infrastructure & Virtualization Security Research Cock Security Research Virtualization Security Research Virtualization Security Research Cock Security Research Virtualization Security Research Virtualization Security Research Security Research Security Security Infrastructure & Virtualization Security	NS-63 NS-62 NS-63 NS-64 NS-66 NS-66 NS-66	NS 01.1 NS 01.1 NS 01.1 NS 01.1 NS 01.1 NS 02.2 NS 02.1 NS 03.1 NS 04.1 NS 05.1 NS 06.1 NS 06.2 NS 06.3 NS 06.4 NS 06.2 NS 06.3 NS 06.2 NS 06.2 NS 06.2 NS 06.2 NS 06.2 NS 06.3 NS 06.2 NS 06.3 NS 06.2 NS 06.2 NS 06.2 NS 06.3 NS 06.4 NS 06.2 NS 06.3 NS 06.4 NS 06.2 NS 06.3 NS 06.4 NS 06.5 NS 06.5 <td< td=""><td>virtual machine, and application controls shall be restricted.</td><td>monitories? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by foot cave analysis, and response to incidents? Is physical and logical sum access to autit logs restricted to autiforzied personnel? Car you provide volence that due diligence mapping of regulations and tandards to your controls/architecture/processes has access to autit logs restricted to autiforzied personnel? Car you provide volence that due diligence mapping of regulations and tandards to your controls/architecture/processes has access to autit logs restricted to autiforzied personnel? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Do you us a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Po you us synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you us synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Po you you spreatry to apackly requirements take into account current, projected, and anticipated capacity need: for all systems used to arroid services the memory version scalabilites is continues and machine that circumstence/scaracitosis Do scarafty taus the temath? Are approximate monitored and tunnel in order to continuously meet regulatory, contractual, and business requirements for all the systems using the systems' to apackly requirements take in baccutor arest to continuously meet regulatory, contractual, and business requirements for a file restructive displace in one to to coste a solyce access control dist discumented with business justification? Are</td><td>x x x x x x x x x x x x x</td><td>x x x x x x x x x x x x x x x x x x x</td><td>x</td><td></td></td<>	virtual machine, and application controls shall be restricted.	monitories? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by foot cave analysis, and response to incidents? Is physical and logical sum access to autit logs restricted to autiforzied personnel? Car you provide volence that due diligence mapping of regulations and tandards to your controls/architecture/processes has access to autit logs restricted to autiforzied personnel? Car you provide volence that due diligence mapping of regulations and tandards to your controls/architecture/processes has access to autit logs restricted to autiforzied personnel? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? Do you us a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Po you us synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Do you us synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? Po you you spreatry to apackly requirements take into account current, projected, and anticipated capacity need: for all systems used to arroid services the memory version scalabilites is continues and machine that circumstence/scaracitosis Do scarafty taus the temath? Are approximate monitored and tunnel in order to continuously meet regulatory, contractual, and business requirements for all the systems using the systems' to apackly requirements take in baccutor arest to continuously meet regulatory, contractual, and business requirements for a file restructive displace in one to to coste a solyce access control dist discumented with business justification? Are	x x x x x x x x x 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 Using Programs infrastructure & Virtualization Security Addit Loging / infrastructure & Virtualization Security Chung & Detection Infrastructure & Virtualization Security Chung & Detection Infrastructure & Virtualization Security Chung & Detection Infrastructure & Virtualization Security Chung & Detection Infrastructure & Virtualization Security Capacity / Encource Additional Security Costante Security Security Network Security Virtualization Security Costante Security Costante Security Security Infrastructure & Virtualization Security Security Security Security Segmentation Security Segmentation Security Segmentation Security Segmentation Security Virtualization Security Segmentation Security Virtualization Security Segmentation Security Virtualization Security Segmentation Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization Security Virtualization	NS-03 NS-03 NS-03 NS-04 NS-04 NS-05 NS-07 NS-07 NS-08 NS-09 NS-09 NS-09	N5 01.1 N5 01.1 N5 01.1 N5 01.3 N5 01.3 N5 01.3 N5 02.2 N5 02.2 N5 02.3 N5 02.1 N5 02.1 N5 02.1 N5 04.1 N5 04.1 N5 04.1 N5 05.1 N5 04.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3	virtual machine, and application controls shall be restricted. Higher levels of assume are required for protection, resention, and Higher levels of assume are required for providing unique user access accontability observed potential subjection shows the shows and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and their raiser capacity of the running levels (e.g., dommar, off, and after raiser capacity of the running levels (e.g., dommar, off, and after raiser capacity of the running levels (e.g., dommar, off, and to after raiser capacity of the running levels (e.g., dommar, off, and to after raiser capacity of the running levels (e.g., dommar, off, and to after raiser capacity of the running levels (e.g., dommar, off, and to after raiser capacity of the running levels (e.g., dommar, off, and to after raiser capacity of the running levels (e.g., dommar, off, and to after raiser capacity of the running levels (e.g., dommar, off, and to additions through and metal time source shall be used to support the transpire of the running of the running of the running systems to facilitate tracing and reconstitution of activity timelines. The availability, turing adquarte capacity and reconstructs shall be performance in accordance with legal, statutory, and requisitory complance obligations the virtual attaction technologies used (e.g., trataction aware). Each operating system shall be hardened to provide and interactions, there explores the system shall be hardened to provide and interactions, there and to miggete the virtualization technologies used (e.g., trataction aware). Each operating system shall be hardened to provide and interactions, there apporting the site of a statution activity is statuted and any explores protocol, and envices to meeter ormaloge (anyices any pote, proto	monitorest? Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by roto cause analysis, and response to incidence? Is physicial and logical user access to audit logs restricted to authorized personnel? Can you provide where that due difference mapping of regulations and standards to your controls/architecture/processes has been archivered? Are built logical user access to audit logs restricted to authorized personnel? Can you provide diverse that due difference mapping of regulations and standards to your controls/architecture/processes has been archivered? Are built logicar treatment and restince? Are changes made to virtual machine images regulates of their running state (e.g., dormant, off or running?) Does the virtual machines, or noving off an image and subsequent validation of the image's integrity, made immediately patible to ocitament include hections or avails? Do you use a synchronized time-service protocol (e.g., VFP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network?). Do you use a synchronized time-service protocol (e.g., VFP) to ensure all systems have a common time reference? Do you provide documentation regarding what levels of system (e.g., network?). Do you de synchronized the transmotory were ubuic/relian catabilitie present in the hypervisor? Do youride social to the transmotory over duality in the occur to continuously meet regulatory, contractual, and business requirements for athe virtual machine the transmotory. Do you regulative text the transmotory over duality of services accommodate the virtualization technologies being used (e.g., virtualization the virtual work of the manke?) Do evenify virtual reviced arXives to the ternsks? Do evenify virtual reviced arXives to the ternsks? Do you regulative review for appropriateness the allowed access/connectivity (e.g., frewall rules) between security domain	x x x x x x x x x 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 Utility Pograms infrastructure & Virtualization Security Audit Loging infrastructure & Virtualization Audit Loging infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Change Detection Infrastructure & Virtualization Security Network Security Network Security Network Security Distanture Security Network Security Populacion Environments Infrastructure & Virtualization Security Network Security Distanture Security Network Security Distanture Security Network Security Infrastructure & Virtualization Security Distanture Security Distanture Security Security Distanture Security Security Distanture Security Distanture Security Segmentation Security Virtualization Security Distanture Sec	NS-03 NS-03 NS-03 NS-04 NS-04 NS-05 NS-07 NS-07 NS-08 NS-09 NS-09 NS-09	N5 01.1 N5 01.1 N5 01.1 N5 01.3 N5 01.3 N5 01.3 N5 02.2 N5 02.2 N5 02.3 N5 02.1 N5 02.1 N5 02.1 N5 04.1 N5 04.1 N5 04.1 N5 05.1 N5 04.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3 N5 05.3	virtual machine, and application controls shall be restricted.	monitories? Are file integrity (host) and network intrusion detection (DS) tools implemented to help facilitate timely detection, investigation by root cave analysis, and response to incidents? Is physicial and logical user access to autothis? Are additing prevention of the second seco	x x x x x x x x x x x x	x x x x x x x x x x x x x x x x x x x	x	

Markaterial		1					n		
March Part Part Part Part Part Part Part Part	Infrastructure & Virtualization	IVS-12	IVS-12.1						
No. 1990 No.	Security Wireless Security								
No. No. <td></td> <td></td> <td></td> <td>unauthorized traffic</td> <td>Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?</td> <td></td> <td></td> <td>x</td> <td></td>				unauthorized traffic	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			x	
No. No. <td></td> <td></td> <td></td> <td>transmission, replacing vendor default settings (e.g., encryption keys,</td> <td>permeter and to reading analyticities and the starter</td> <td></td> <td></td> <td></td> <td></td>				transmission, replacing vendor default settings (e.g., encryption keys,	permeter and to reading analyticities and the starter				
No. No. <td></td> <td></td> <td></td> <td>User access to wireless network devices restricted to authorized</td> <td></td> <td></td> <td></td> <td></td> <td></td>				User access to wireless network devices restricted to authorized					
No. No. <td></td> <td></td> <td>IVS-12.2</td> <td>The capability to detect the presence of unauthorized (rogue) wireless</td> <td></td> <td></td> <td></td> <td></td> <td></td>			IVS-12.2	The capability to detect the presence of unauthorized (rogue) wireless					
Answer And And And And And Second Seco				network devices for a timery disconnect from the network				х	
Market bis Market								х	
Control <		IV5-13	IVS-13.1	environments and data flows that may have legal compliance impacts.				x	
No. No. <td>Security Network Architecture</td> <td></td> <td>IVS-13.2</td> <td>depth techniques (e.g., deep packet analysis, traffic throttling, and black-</td> <td></td> <td></td> <td></td> <td></td> <td></td>	Security Network Architecture		IVS-13.2	depth techniques (e.g., deep packet analysis, traffic throttling, and black-					
No. No. </td <td></td> <td></td> <td></td> <td>associated with anomalous ingress or egress traffic patterns (e.g., MAC</td> <td>Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-</td> <td></td> <td></td> <td></td> <td></td>				associated with anomalous ingress or egress traffic patterns (e.g., MAC	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-				
No.					holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns			х	
Number Number </td <td></td> <td></td> <td></td> <td></td> <td>1</td> <td></td> <td></td> <td></td> <td></td>					1				
N N </td <td>Interoperability &</td> <td>IPY-01</td> <td>IPY-01.1</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Interoperability &	IPY-01	IPY-01.1						
<table-container> Main Mark Mark Mark Mark Mark Mark Mark Mark</table-container>	Portability APIs				Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	х			
<table-container> Main Mark Mark Mark Mark Mark Mark Mark Mark</table-container>									
Image Image <t< td=""><td>Portability</td><td>161-02</td><td>17102.1</td><td>and provided to them upon request in an industry-standard format (e.g.,</td><td>Is unstructured customer data available on request in an industry-standard format (e.e., doc., vk. or, ndf)?</td><td>x</td><td></td><td></td><td></td></t<>	Portability	161-02	17102.1	and provided to them upon request in an industry-standard format (e.g.,	Is unstructured customer data available on request in an industry-standard format (e.e., doc., vk. or, ndf)?	x			
Mark And And </td <td>Dota Request</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>pdf,xls,csv</td>	Dota Request								pdf,xls,csv
Or of the second sec	Interoperability & Portability	IPY-03	IPY-03.1			x			
<table-container> Production of the standard proper base provide proper base provide pro</table-container>	Policy & Legal		197-03-2		service and third-party applications?				
Note Note N				usage, and integrity persistence.	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		x		
Note Note N			IPV-02.2	-					
Name of All states No. Probability of the state state state state states No. Probability of the state state state states No. Probability of the state state state states No. Probability of the state state state state state states No. Probability of the state sta								х	
Next Problem	Interoperability &	IPY-04	IPY-04.1			x			
Number of the section of th	Portability Standardized		IPY-04.2	manage the service, and shall make available a document to consumers	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol		x		
PADD	Interoperability &	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure			x	
	Portability Virtualization		IPY-05.2	and shall have documented custom changes made to any hypervisor in	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to				
Name			IPY-05.3		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for				
No. No. No. No. No. No. No. Results No.	Mobile Security	MOS-01	MOS-01.1						
Maximum of the second secon	Anti-Maiware			included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?		х		
No. No. No. No. No. No. No. No. No. <td>Mobile Security Application Stores</td> <td>MOS-02</td> <td>MOS-02.1</td> <td></td> <td>Do you document and make available lists of approved application stores for mobile devices accessing or storing company data</td> <td></td> <td>×</td> <td></td> <td></td>	Mobile Security Application Stores	MOS-02	MOS-02.1		Do you document and make available lists of approved application stores for mobile devices accessing or storing company data		×		
Sector Sector<					and/or company systems?		^		
No. 1 No. 1 <th< td=""><td>Approved</td><td>MOS-03</td><td>MOS-03.1</td><td>of non-approved applications or approved applications not obtained</td><td></td><td></td><td></td><td></td><td></td></th<>	Approved	MOS-03	MOS-03.1	of non-approved applications or approved applications not obtained					
Image: start in the start	Applications			through a pre-identified application store.			x		
Band Band Band Band Park Park Park Park Park Park Park Park									
web yes	Mobile Security	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the					
owner of the second					Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?		х		
owner of the second	Mark Tar Caracteria	1405.05	1005.05.4						
	Awareness and	MUS-US	MUS-05.1	documented definition for mobile devices and the acceptable usage and	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted		×		
Schwarz	i raining				usage and requirements for mobile devices?		^		
Image:	Mobile Security Cloud Based Services	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company		Y.		
constant image is a second problem in the problem is a second problem in the problem is a second problem in the problem is a second problem is a s				data.			~		
Image: state Image: state <th< td=""><td></td><td>MOS-07</td><td>MOS-07.1</td><td>test for mobile device, operating system, and application compatibility</td><td></td><td></td><td>Y.</td><td></td><td></td></th<>		MOS-07	MOS-07.1	test for mobile device, operating system, and application compatibility			Y.		
				issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?		~		
		MOS-08	MOS-08.1						
Non-standing Non-standing standard				-	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?		x		
Less Less <thless< th=""> Less Less</thless<>	Mobile Security Device Inventory	MOS-09	MOS-09.1						
Note bandpart Linkable for a large on the entropy Production should apply on the					Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating	x			
Inclusion here integration here integration <td></td> <td></td> <td></td> <td>included for each device in the inventory.</td> <td>system and patch levels, lost or decommissioned, device assignee)?</td> <td></td> <td></td> <td></td> <td></td>				included for each device in the inventory.	system and patch levels, lost or decommissioned, device assignee)?				
Inclusion here integration here integration here integration 	Mobile Security	MOS-10	M05-10.1	A centralized mobile device management solution shall be deployed to all					
No.51 <th< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td>x</td><td></td><td></td></th<>							x		
formulaImage and the state of a data batched a baseline at lange data batched at lange dat lang	Mobile format	MOCIO	MOSAL	The mobile desire online shall service the use of a service when the	2 2 Bank anna				
Notes where shows and shows and and an and and an and and an and and and		MOS-11	W05-11.1	entire device or for data identified as sensitive on all mobile devices and				x	
$ \begin{array}{c c c c c c } & \begin{tabular}{ c c c } & \begin{tabular}{ c c c c c } & \begin{tabular}{ c c c c c } & \begin{tabular}{ c c c c c c } & \begin{tabular}{ c c c c c c } & \begin{tabular}{ c c c c c } & \begin{tabular}{ c c c c c c } & \begin{tabular}{ c c c c c c } & \begin{tabular}{ c c c c c } & \begin{tabular}{ c c c c c c } & \begin{tabular}{ c c c c c c c c c c c c c c c c c c c$	Mobile Security	MOS-12	M05-12.1						
$ \frac{1}{10000000000000000000000000000000000$	Jailbreaking and			security controls on mobile devices (e.g., jailbreaking or rooting) and is			v		
Note: <th< td=""><td></td><td></td><td></td><td>through a centralized device management system (e.g., mobile device</td><td>rooting}?</td><td></td><td><u>^</u></td><td></td><td></td></th<>				through a centralized device management system (e.g., mobile device	rooting}?		<u>^</u>		
Mathematic Secure (spring) MOS-14 (mode)			MOS-12.2				x		
Note Security log with a leasy table the spectations or holes of one you PRO point during the sequentiation of philor, regurements for light for, edicover, and legit holes?XXNote Security log with a leasy table the device sequence compary during the company owned devices are configured requires that be edificated three table security log with a leasy table the expectations or holes of non-company during the company owned devices?XXXNote Security log with a leasy table the expectations or holes of non-company during the company owned devices?XXXXNote Security log with a leasy table the expectation or holes of non-company during the company owned devices?XXXXNote Security log with a leasy table the expectation or holes of non-company during devices and company owned devices?XXXXNote Security log with the company owned devices are company during devices and company owned devices?XXXXXNote Security log with the company owned devices and company owned devices?XXXXXNote Security log with the security of the company owned devices and company owned devices?XXXXXNote Security log with the security and heaving of log powned pacies for other prior balance management		MOS-13	MOS-13.1		Emerinaria di Bulli el Sculto Lutturis i				
Note: 1Mode: 1Does the DYOD policy (darly state the expectations over the loss of non-company data in case a wipe of the device is required?NXNNobiol: 2 score 1NOS: 4.1NOS: 4.1 <td>yu</td> <td></td> <td></td> <td>BYOD policy shall clearly state the expectations over the loss of non-</td> <td>Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?</td> <td></td> <td>×</td> <td></td> <td></td>	yu			BYOD policy shall clearly state the expectations over the loss of non-	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?		×		
Model Security Relative Sorem MOS-14 MOS-14 MOS-14 MOS-14 MOS-14 MOS-14 MOS-14 MOS-14 MOS-14 Relative Sorem Do you require and enforce via technical controls an automatic lockout screen of the TOD and company sound devices? X Image: Company Sound Sorem Model Security provide y during MOS-15 MOS-161 MOS-162 MOS-162 Op you require and enforce via technical controls an automatic lockout screen of the TOD and company sound devices? X Image: Company Sound Soun			MOS-13.2		Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?		x		
No. 1 No. 1 <t< td=""><td>Mobile Security Lockout Screen</td><td>MOS-14</td><td>MOS-14.1</td><td>BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be approved through</td><td></td><td></td><td>l</td><td></td><td></td></t<>	Mobile Security Lockout Screen	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be approved through			l		
Operating Sates Same applications with the managed through the company's change management processor? X X X And Nobile Security Sates MOS512 Pained Sates MOS512 Pained Pained				technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	х			
Imagement processe: magement pro	Mobile Security Operating Systems	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change	Do you manase all changes to mobile desire operation systems, patch levels, and an Evaluations visually compare it its and	-			
Reserves Model as a proceed through technical controls (as all company divises or						х			
$\frac{1}{MOS^{12}} = \frac{1}{MOS^{12}} + \frac{1}$	Mobile Security	MOS-16			Do you have password policies for enterprise issued mobile devices and/or BYDD mobile devices?		x		
MOS-16.3 MOS-16.3 Do your password policies prohibit the changing of authentication requirements (i.e. password/pNi length) via a mobile device? N X N	rdsswords		MOS-16.2	approved for BYOD usage, and shall prohibit the changing of	Are your password policies enforced through technical controls (i.e. MDM)?		x		
NoBi-12 biology NOS-12 the mobile devices play half requires H900 user to profile multiples the use of anti-makers software (where supported);			MOS-16.3	passwurd/Pin lengths and authentication requirements.	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?		x		
MoS-120 Model security future MoS-230 MoS-232 In use of anit-malware software (where supported). MoS-232 De you have a policy that reguine SirDO users to get/filed corporate data? N N N N MoS-120 Model security motor MoS-232 MoS-232 All model devices prime the true through the company PEOD parsing reguine and prime wide or corporate data wide for all company-accepted BYOD devices to an entropy-mark coepted BYOD devices? N N N MoS-180 MoS	Mobile Security	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups					
Noise Noise <t< td=""><td>- Unicy</td><td></td><td></td><td>the use of anti-malware software (where supported).</td><td>Do you have a policy that requires BYOD users to perform backups of specified corporate data?</td><td></td><td>x</td><td></td><td></td></t<>	- Unicy			the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?		x		
$\frac{1}{10000000000000000000000000000000000$					Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?				
Remote Water Parts		MOS-18	MOS-17.3 MOS-18.1	All mobile devices permitted for use through the company BYOD program			x		
Mole State Mode State <td></td> <td></td> <td></td> <td>or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by</td> <td>Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?</td> <td></td> <td>х</td> <td></td> <td></td>				or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?		х		
Security Patchen Security Patchen Company Information shall allow for remote software version/gath results are adaptivised if patches installed upon general releases by the device manufacture related patches installed upon general releases by the device manufacture updates remotely. C critical patches C critical patches <thc critical<br="">patches C critical patches</thc>	Mobile format	MOC 10		the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?		x		
Image: Instruction of the processing of the device manufacture of the performance of the perform				company information shall allow for remote software version/patch		х			
Model security MOS-202 The BYOD policy shall carriy the systems and servers allowed for use or access on the BYOD-enabled device? X				related patches installed upon general release by the device manufacturer	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?		x		
Liters access on a BYOD-enabled device. Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?				updates remotely.	, and a second s				
Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device? X		MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.					
MOX.202 Doer your BYOD policy specify the user roles that are allowed access via a BYOD enabled device? X					Lives your BYOD policy clarity the systems and servers allowed for use or access on the BYOD-enabled device?		x		
			MOS-20.2	1	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?		х		

Security Incident Management, E- Discovery, & Cloud Forensics Contact / Authority Maintenance	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other (egg) jurisdictional authorities shall be maintained and regulary updated (e.g. change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance laws that any compliance and the statistical terms of the compliance investigation requiring rapid engagement with law enforcement.	Do you maintain faisions and points of contact with local authorities in accordance with contracts and appropriate regulations?		x		
Security Incident Management, E- Discovery, & Cloud Forensics Incident	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?		x		
Incident Management		SEF-02.2 SEF-02.3		Do you integrate customized tenant requirements into your security incident response plans? Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?			x	
Security Incident Management, E-	SEF-03	SEF-02.4 SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or	Have you tested your security incident response plans in the last year? Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	х		X	
Discovery, & Cloud Forensics Incident Reporting		SEF-03.2	mormeo or meir responsionity and, ir required, snail consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	х			
Security Incident	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?		x		
Discovery, & Cloud Forensics		SEF-04.2	the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?		x		
Incident Response Legal Preparation		SEF-04.3	by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	х			
Security Incident	SEF-05	SEF-04.4 SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types,	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas? Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	х		x	
Management, E- Discovery, & Cloud Forensics Incident Resnanse		SEF-05.2	volumes, and costs of information security incidents.	Will you share statistical information for security incident data with your tenants upon request?		x		
Supply Chain Management, Transparency, and Accountability		STA-01.1 STA-01.2	Providers shall inspect, account for, and work with their cloud supply- chain partners to correct data quality errors and associated risks.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?		x		
Transparency, and Accountability Data Quality and Integrity		STA-01.2	Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	x			
Supply Chain Management, Transparency, and Accountability Incident Reporting	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?		x		
Incident Reporting Supply Chain	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual)	Do you collect capacity and use data for all relevant components of your cloud service offering?		x		
Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services		STA-03.2	application and system-system interface (AP) designs and configurations, and infrastructure network and system components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you provide tenants with capacity planning and use reports?		x		
Supply Chain Management, Transparency, and Accountability			The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	х			
Supply Chain Management,	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	х			
Accountability Third Party		STA-05.2 STA-05.3	 Provisions and/or terms: Scope of business relationship and services offered (e.g., customer 	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation? Does legal counsel review all third-party agreements?	x			
Agreements		STA-05.4 STA-05.5	(tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of	Do third-party agreements include provision for the security and protection of information and assets? Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	x			
		STA-05.6 STA-05.7	provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services,	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations? Can you provide the physical location/geography of storage of a tenant's data upon request?	x x			
		STA-05.8 STA-05.9	and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant)	Can you provide the physical location/geography of storage of a tenant's data in advance? Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		x		
		STA-05.10	primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?		х		
		STA-05.11 STA-05.12	and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies? Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		x x		
Supply Chain Management, Transparency, and Accountability Supply Chain			Providers shall review the risk management and governance processes for their partners so that practices are consistent and adigned to account risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	x			
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics			Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAb) between providers and customers (lenanis) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result nactions to address service-level conflicts or	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (lenants)?	x			
		STA-07.2	inconsistencies resulting from disparate supplier relationships.	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	х			
		STA-07.3 STA-07.4		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships? Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	х	x		
		STA-07.5 STA-07.6		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?		x		
		STA-07.6 STA-07.7 STA-07.8		Do you provide customers with ongoing wisbility and reporting of your SLA performance? Do your data management policies and procedures address tenant and service level conflicts of interests? Do you review all service level agreements at feast annually?		X		
Supply Chain Management	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review	Do you assure reasonable information security across your information supply chain by performing an annual review?	х	^		
Transparency, and Accountability Third Party Assessment		STA-08.2	shall include all partners/third party providers upon which their information supply chain depends on.	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	x			
Supply Chain Management.	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?		х		
Transparency, and		STA-09.2	definitions, and delivery level agreements included in third-party	requirements are met? Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?		х		
Threat and Vulnerability Management	TVM-01	TVM-01.1 TVM-01.2	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	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	х			
Antivirus / Malicious Software			devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you ensure that security thread detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	x			
Threat and Vulnerability Management	TVM-02	TVM-02.1 TVM-02.2	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	х	x		
Vulnerability / Patch Management		TVM-02.3 TVM-02.4	vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? Will you make the results of vulnerability scans available to tenants at their request? Do you have a capability to patch vulnerabilities across all of your computing device, applications, and systems?	Y	X		
		TVM-02.6	implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be	bo you have a capability to parch youre abilities across an or your computing devices, applications, and systems?	^			
			developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer	Do you inform customent (lenant) of policies and procedures and identified weaknesses if customer (lenant) data is used as part the service and/or customer (lenant) has some shared responsibility over implementation of control?		x		
Threat and Vulnerability	TVM-03	TVM-03.1	(tenant) has some shared responsibility over implementation of control. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			x	
Management Mobile Code		TVM-03.2	of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local					
			system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network	Is all unauthorized mobile code prevented from executing?			x	
			and systems components.	ц		1	1	
link to the Cloud Secur	rity Alliance "Consens	us Assessments Ini	rved. You may download, store, display on your computer, view, print, and tiative Questionnaire CAIQ Version 3.1" at (a) the Computer August and the store of t					
			: (a) the Consensus Assessments Initiative Questionnaire v3.1 may be used b) the Consensus Assessments Initiative Questionnaire v3.1 may not be					

Into the focus Security Alliance "Consensus Assessments Initiative Questionnaire CAQ Version 3.1" et http://www.colustervollailance.org.subject to het following: (b) the Consensus Assessments Initiative Questionnaire v.3.1 may be used safely for your personal, informational, non-cammeraia use; (b) the Consensus Assessments Initiative Questionnaire v.3.1 may not be safely for your personal, informational, non-cammeraia use; (b) the Consensus Assessments Initiative Questionnaire v.3.1 may not be middle of altered in a www.c); (b) the Consensus Assessments Initiative Questionnaire v.3.1 may not be restinative; and (c) the trademark, copyright or other notices may not be removed. You may quote particular built and that the period of the consensus Assessments Initiative Questionnaire v.3.1 as permitted by the fair built provides that you and the Assessments Initiative descrimtly Alliance Councer Consensus Assessments Initiative Classification 2.1, D(b); (Fyou are interested in obtaining alterner to bits material robustness and the operative forces, place as costa chief devolutionary Hallmann and alterner to bits material robustness and the operative forces, place as costa chief devolutionary Hallmann and alterner to bits material robustness and the assessments Initiative Consensus Assessments I