## CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

		UA	1443.1					
Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Conser	sus Assess	ment Answers	Notes
Application &	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed,	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software	Yes	No	Not Applicable	
Interface Security Application Security		AIS-01.2	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.	Development Lifecycle (SDLC)?  Do you use an automated source code analysis tool to detect security defects in code prior to production?	x			
		AIS-01.3 AIS-01.4		Do you use manual source-code analysis to detect security defects in code prior to production?	x			
		AIS-01.5		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?  [SaaS only] Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	х	x		
Application & Interface Security	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer	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			
Customer Access	AIS-03	AIS-02.2 AIS-03.1	access shall be addressed.	Are all requirements and trust levels for customers' access defined and documented?	x			
Application & Interface Security Data Integrity	~503	AIS-03.2	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 misuse.	Does your data management policies and procedures require audits to verify data input and output integrity routines?  Are data input and output integrity routines (i.e. MDS/SHA checksums) implemented for application interfaces and databases to prevent	x			
Application & Interface Security	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple	manual or systematic processing errors or corruption of data?  Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard,				
Data Security / Integrity			system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data security Architecture designed using an industry standard (e.g., CUSA, MULTISAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?		×		
Audit Assurance & Compliance	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon	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?	x			
Audit Planning  Audit Assurance &	AAC-02	AAC-01.2 AAC-02.1	Independent reviews and accessments shall be performed at least annually to	Does your audit program take into account effectiveness of implementation of security operations?  Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	х	×		
Compliance Independent Audits		AAC-02-2 AAC-02-3	ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	х			
		AAC 02 A		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?  Do you conduct internal audits at least annually?	x			
		AAC-02.5		Do you conduct independent audits at least annually?	x	×		
		AAC-02.6 AAC-02.7		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		
Audit Assurance & Compliance	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust				
Information System Regulatory Mapping			standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	×			
Business Continuity Management &	BCR-01	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 business continuity plans are consistent in addressing priorities for testing,	Does your organization have a plan or framework for business continuity management or disaster recovery management?  Do you have more than one provider for each service you depend on?	x x			
Business Continuity Planning		BCR 01.3	maintenance, and information security requirements. Requirements for business continuity plans include the following:	Do you provide a disaster recovery capability?	x			
		BCR-01.4 BCR-01.5	Defined purpose and scope, aligned with relevant dependencies     Accessible to and understood by those who will use them     Owned by a named person(s) who is responsible for their review, update, and	Do you monitor service continuity with upstream providers in the event of provider failure?  Do you provide access to operational redundancy reports, including the services you rely on?	х	x		
		BCR-01.6 BCR-01.7	approval  • Defined lines of communication roles and responsibilities	Do you provide a tenant-triggered fail over option?			x	
Business Continuity Management &	BCR-02	BCR-02:1	Detailed recovery procedures, manual work-around, and reference	Do you share your business continuity and redundancy plans with your tenants?			x	
Operational Resilience Business Continuity			business community aims security injurient response plants and to subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	×			
Testing			supply chain business process dependencies.	•				
Business Continuity Management &	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?			×	
Operational Resilience Power/ Business Continuity	BCR-04	BCR-03.2 BCR-04.1	connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from information system documentation (e.g., administrator and use guides, and architecture diagrams) shall be made available to authorized personnel to	Has your organization implemented environmental controls, fall-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?			×	
Management & Operational Resilience				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			
Documentation			Configuring, installing, and operating the information system     Effectively using the system's security features		•			
Business Continuity Management &	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar					
Environmental Risks			induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated,	Is physical damage anticipated and are countermeasures included in the design of physical protections?	x			
Purinage Continuity	BCR-06	BCR-06.1	designed, and have countermeasures applied.  To reduce the risks from environmental threats, hazards, and opportunities for					
Management & Operational Resilience			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, tornadoes,		x		
Equipment Location			equipment located at a reasonable distance.	earthquakes, hurricanes, etc.]?		^		
Business Continuity Management &	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 support personnel.	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?			x	
Operational Resilience Business Continuity Management &	BCR-08	BCR-08:1	continuity and availability of operations and 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?			x	
Operational Resilience Equipment Power			отнавляни прита дводгарители учресть подпива пирасс ваявания.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	×			
Foilures								
Business Continuity Management &	BCR-09	BCR-09-1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following:	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc)?	х			
Business Continuity	BCR-10	BCR-10.1	Interporate the tonowing:  - Identify critical products and consider  Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	х			
Operational Resilience Policy			and technical measures impremented, for appropriate II governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce,					
			and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBITS). 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?	×			
			responsibilities supported by regular workbette training.					
Business Continuity Management &	BCR-11	BCR-11.1 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 policies and procedures,	Do you have technical capabilities to enforce tenant data retention policies?  Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or	x			
Retention Policy		BCR-11.3	retention person or any critical asset as per estatesished policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	regulatory compliance requirements?  Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business	x	x		
		BCR-11.4	continuity planning and tested accordingly for effectiveness.	requirements?  If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	x			
		BCR-11.5 BCR-11.6		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?  Does your cloud solution include software/provider independent restore and recovery capabilities?	x	x		
		BCR-11.7	No. of the last of	Lobes your cross solutions include someway provider independent resorter and recovery capabilities?  Do you test your backup or redundancy mechanisms at least annually?	x			
Configuration Management	11101	cconn	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure					
New Development / Acquisition			acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	x			
Change Control & Configuration Management	CCC-02	CCC-02.1 CCC-02.2	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?  Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	х		×	
Change Control &	CCC-03	CCC-03.1	organization (e.g., TIL service management processes).  Organizations shall follow a defined quality change control and testing process (e.g., TIL Service Management) with established baselines, testing, and release	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	x		*	
Management Quality Testing		CCC-03.2 CCC-03.3	e.g., TIL service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Is documentation describing known issues with certain products/services available?		x		
		CCC-03.4		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?  Do you have controls in place to ensure that standards of quality are being met for all software development?	x			
		CCC-03.5 CCC-03.6		Do you have controls in place to detect source code security defects for any outsourced software development activities?			×	
Change Control &	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented to restrict the installation of	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	х			
Management Unauthorized			and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?		x		
Software installations			infrastructure network and systems components.					
Change Control & Configuration	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to:	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?			×	
Management Production Changes		CCC-05-2 CCC-05-3	Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations.     Infrastructure network and systems components.	Do you have policies and procedures established for managing risks with respect to change management in production environments?  Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with		x		
Data Security &	DS-01	DSI-01.1	Technical measures shall be implemented to provide assurance that all changes  Data and objects containing data shall be assigned a classification by the data	existing SLAs?  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	х			
Information Lifecycle Management Classification		DSI-01.2	owner based on data type, value, sensitivity, and criticality to the organization.	systems from booting/instantiating/transporting data in the wrong country)?  Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			x x	
Data Security & Information Lifecycle	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services applications and infrastructure network and systems?	x			
Management Data Inventory / Flows Data Security &	DSI-03	DSI-02.2 DSI-03.1	data flows for data that is resident (permanently or temporarily) within the service's secena-hically distributed (physical and virtual) asselfications and Data related to electronic commerce (e-commerce) that traverse public networks shall be appropriately classified and protected from fraudulent	Can you ensure that data does not migrate beyond a defined geographical residency?  Do you provide standardized (e.g. ISQ/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect	х			
Data Security & Data Security & Information Lifecycle Management E-commerce Transactions		DSI-03.2	activity, unauthorized disclosure, or modification in such a manner to prevent	their data if it is required to move through public networks (e.g., the Internet)?  Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public			x	
Transactions Data Security &	DSI-04	DSI-04.1	contract dispute and compromise of data.  Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label	networks (e.g., Internet-based replication of data from one environment to another)?  Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?		x	x	
Data Security & Information Lifecycle Management Handling / Lobeling /		DSI-04.2	security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		x		
Handling / Lobeling / Security Policy 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?		x		
Information Lifecycle Management Nonproduction Data			environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is 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?			x	
Out of			scrubbing of sensitive data elements.					
Data Security & Information Lifecycle Management	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?				
Ownership / Stewardship				The transformation regarding data seewardship defines, asagind, documented, and communicated?	х			
			•					

Data Security & Information Lifecycle		DSI-07.1 DSI-07.2	Policies and procedures shall be established with supporting business processer and technical measures implemented for the secure disposal and complete	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?  Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant.	x			
Management Secure Disposol Datacenter Security	DCS-01	DCS-01.1	removal of data from all storage media, ensuring data is not recoverable by any computer forensic means. Assets must be classified in terms of business criticality, service-level	data once a customer has exited your environment or has vacated a resource?	x			
Asset Management		DCS-01.1 DCS-01.2	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?  Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned			x x	
Datacenter Security	DCS-02	DCS-02.1	their upper execution set of the maintained and undated computer, and assigned.  Physical security perimeters (e.g., fences, walls, barriers, guards, gates,	ownership?			^	
Controlled Access Points			electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitived at and information systems?			×	
Datacenter Security	DCS-03	DCS-03.1	information systems.  Automated equipment identification shall be used as a method of connection	Do you have a capability to use system geographic location as an authentication factor?			v	
Datacenter Security Equipment Identification		DCS-03.2	authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	is automated equipment identification used as a method to validate connection authentication integrity based on known equipment			x	
Datacenter Security Offsite Authorization	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of 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?			×	
Ogsite Authorization  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			l		
			information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with your asset management policies and procedures?			x	
Datacenter Security	DCS-06	DCS-06.1	or securely stored until it can be destroyed.  Policies and procedures shall be established, and supporting business processes	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working				
Policy		DCS-06.2	rollices, and procedures shall be established, and supporting outsies processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	environment in offices, rooms, facilities, and secure areas?			x	
				Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, 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 personnel are allowed access.	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor 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 facilities to prevent	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?			×	
Datacenter Security	DCS-09	DCS-09.1	unauthorized data corruption, compromise, and loss.  Physical access to information assets and functions by users and support					
User Access Encryption & Key	BKM-01	EKM-01.1	personnel shall be restricted.  Kews must have identifiable owners (binding kews to identities) and there shall	Do you restrict physical access to information assets and functions by users and support personnel?			×	
Management Entitlement			be key management policies.	Do you have key management policies binding keys to identifiable owners?		×		
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?		×		
Key Generation		EKM-02.2 EKM-02.3	cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for	Do you have a capability to manage encryption keys on behalf of tenants?		х		
		EKM-02.3 EKM-02.4	secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the	Do you maintain key management procedures?  Do you have documented ownership for each stage of the lifecycle of encryption keys?		x x		
		EKM-02.5	used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer flemant data is used as part of the service, and for the customer	Do you have documented ownership for each stage of the lifecycle of encryption keys?  Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	x	^		
Encryption & Key Management	EKM-03	EKM-03.1 EKM-03.2	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for	Do you encrypt tenant data at rest (on disk/storage) within your environment?		x		
Encryption		Dim03.2	protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?			х	
Encryption & Key	EXM-04	EKM-03.3 EKM-04.1	networks, and electronic messaging) as per applicable legal, statutory, and Platform and data appropriate encryption (e.g., AES-256) in open/validated	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?  Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	v	x		
Management Storage and Access		EXM-04.2	formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?		x		
		EKM-04.3 EKM-04.4	consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you store encryption keys in the cloud?	x			
Governance and Risk	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired,	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 systems,		x		
Management Boseline Requirements		GRM-01.2	organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable	routers, DNS servers, etc.]?  Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security			х	
Governance and Risk	GRM-02	GRM-02.1	legal, statutory, and regulatory compliance obligations. Deviations from standard baceline configurations must be authorised eleberate schools. Risk assessments associated with data governance requirements shall be	to you need the capacitity to continuously monitor and report the compilance of your immustraction against your information accounty baselines?  Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention			х	
Management Risk Assessments		GRM-02.1	not assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:  - Awareness of where sensitive data is stored and transmitted across	Code your organizations has assessments asset into account watermess or data researcy, agail and sautoby requirements for retember periods and data protection and disselfication.  Do you conduct risk assessments associated with data povernance requirements at least once a year?		x		
Governance and Risk	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of		^			
Monagement Oversight			security policies, procedures, and standards that are relevant to their area or responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	×			
Governance and Risk	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed,	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		x		
Management Monagement	GRM-05	GRM-04.2 GRM-05.1	documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, proportion and line on a person of that I have formally action to report information.	Do you review your information Security Management Program (ISMP) at least once a year?	x			
Management Monogement	GRM-US	GRM-US.1	Executive and line management shall take formal action to support 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		Į.		
/involvement			AND THE	commitment, and ensure the action has been assigned?	x			
Governance and Risk	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by				
Management Policy			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 role or	accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	x		<u></u>	
		GRM-05.2	organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and		×		
		GRM-06.3	security management program inclusive of defined information security roles and responsibilities for business leadership.	responsibilities for business leadership?				
		GRM-06.4		Do you have agreements to ensure your providers adhere to your information security and privacy policies?  Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?		x x		
		GRM-06.5		Do you disclose which controls, standards, certifications, and/or regulations you comply with?		- х		
Governance and Risk Management	GRM-07	GRM-07.1 GRM-07.2	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware	is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?  Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	x			
Governance and Risk	GRM-08	GRM-08.1	of what action might be taken in the event of a violation, and disciplinary Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.		x			
Business/Policy			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?	×			
Governance and Risk	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or	Do you notify your tenants when you make material changes to your information security and/or privacy policies?			×	
Management Policy Reviews		GRM-09.2	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	Do you perform, at minimum, annual reviews to your privacy and security policies?	х			
Governance and Risk Management	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of	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			
Assessments Government and Birk	GRM-11	GRM-10.2 GRM-11.1	all identified risks using qualitative and quantitative methods. The likelihood	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	x			
Management Program		GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established 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?  Do you make available documentation of your organization-wide risk management program?		x x		
Human Resources Asset Returns	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	x			
		HRS-01.2	within an established period.	returning organizationally-owned assets?  Do you have asset return procedures outlining how assets should be returned within an established period?	x			
Human Resources Bockground Screening	HRS-02		Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third	×	٦		
			background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	parties subject to background verification?	*		<u></u>	
Human Resources Employment	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?				
Agreements			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		×			
		HRS-03.2	user access to corporate facilities, resources, and assets.	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	x			
Human Resources Employment	HRS 04	HRS-04.1 HRS-04.2	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	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			
Human Resources	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes	purchase and government account on timery revocation of access and record of access?	x			
Portable / Möbile Devices			and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from				
			emplementation on ingine assurance compensating controls and acceptations of policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non- portable devices (e.g., desktop computers at the provider organization's facilities)?		x		
Human Resources Non-Disclosure	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be lidentified idocumented and reviewed at planned intervals:	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?	х			
Agreements Human Resources	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall					
Roles / Responsibilities			be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	×	Į.		
Human Resources Acceptoble Use	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions	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?	х			
		HRS-08-2	for permitting usage of organizationally-owned or managed user end-point devices (e.e., issued workstations, laptops, and mobile devices) and IT	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?		x		
Numan Resources Training / Awareness	HRS 09		A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi- tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant		×		
		HRS-09.2	appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function	data?  Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	x			
		HRS-09.3	processors, processes, and poincies relating to their processorial function relative to the organization.	Do you document employee acknowledgment of training they have completed?		×		
		HRS-09.4		is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	x			
		HRS-09.5 HRS-09.6		Are personnel trained and provided with awareness programs at least once a year?  Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	x			
Human Resources	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for:  • Maintaining awareness and compliance with established policies and	Are paraministrators and not assistances properly educated on their regain responsibilities with regain to security and pata integrity?  Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable resultatory requirements?	x			
eser responsibility		HRS-10.2	<ul> <li>Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.</li> </ul>	standards, and applicable regulatory requirements?  Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	x			
Human Rozov	uoc ++	HRS-10.3	outspanners  - Maintaining a safe and secure working environment  - Policies and procedures shall be established to require that unattended	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	x			
Workspace		HRS-11.2	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?  Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	x			
identity & Access	IAM01	IAM-01.1	inactivity.  Access to, and use of, audit tools that interact with the organization's	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners,				
Management Audit Tools Access		IAM-01.2	information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	natwork uniffers, APIs, etc.]?  Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	x			
Identity & Access	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	x			
User Access Policy		IAM-02.2	appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally	Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	x			
		IAM-02.3	owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures,	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	х			
		IAM-02.4	processes, and measures must incorporate the following:  • Procedures, supporting roles, and responsibilities for provisioning and de-	Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?			x	
		IAM-02.5 IAM-02.6	provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?  Do your policies and procedures in corporate security controls for establishing higher levels of assurance for critical business case	х			
		IAM-02.7	changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)	considerations, supported by multifactor authentication?	x			
Identity & Arcess	IAM-03	IAM-03.1	Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote User access to diagnostic and configuration ports shall be restricted to	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		x		
			authorized individuals and applications.	Is user access to disponsic and configuration ports restricted to authorized individuals and applications?	x	l		
Management Diagnostic /					^			
Management Diagnostic / Configuration Parts Access						I		

Identity & Access Management								
		IAM-04.1 IAM-04.2	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?  Do you manage and store the user identity of all personnel who have network access, including their level of access?	×			
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 user					
Segregation of Duties			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?		×		
Identity & Access	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to	×			
Management Source Code Access		IAM-06.2	source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least orivilege based on iob function as one established user access colicies and	authorized personnel only?  Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to			×	
Identity & Access	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business	authorized personnel only?  Does your organization conduct third-party unauthorized access risk assessments?			×	
Management Third Porty Access		IAM-07.2	processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	x		-	
Identity & Access Management	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?			x	
User Access Restriction /Authorization		IAM-08.2	on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?			x	
		IAM-08.3		Do you limit identities' replication only to users explicitly defined as business necessary?			x	
Identity & Access Management User Access		IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally- owned or managed (physical and virtual) applications, infrastructure systems,	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure	x			
Authorization		IAM-09.2	and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per	systems, and network components?  Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business				
		IAM-10.1	established policies and procedures. Upon request, provider shall inform  User access shall be authorized and revalidated for entitlement	partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?		x		
Management		IAM-10.1	user access shall be authorized and revaluated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role		×		
DAI ALCEIJ ALVENI		IAM-10.2	demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow	or function?  Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?		x		
		IAM-10.3	established user access policies and procedures.	Do you ensure that remediation actions for access violations follow user access policies?	x			
		IAM-10.4		Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?		x		
Identity & Access Management		IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per	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?	x			
Revocation		IAM-11.2	established policies and procedures and based on user's change in status (e.g.,	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 Management	IAM-12	IAM-12.1 IAM-12.2	internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?			х	
User ID Credentials		IAM-12.3	access management and in accordance with established policies and procedures:	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 users?	x			1
		IAM-12.4	Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)     Account condens in lifecture was promoted from instructivities through	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	Account credential lifecycle management from instantiation through revocation     Account credential and/or identity store minimization or re-use when	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	x			
		IAM-12.6 IAM-12.7	Account credential and/or identity store minimization or re-use when feasible     Adherence to industry acceptable and/or regulatory compliant	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	<ul> <li>Annerence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi- factor, expireable, non-shared authentication secrets)</li> </ul>	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 duration)	x			
		IAM-12.9	1	policy enforcement?  Do you allow tenants/customers to define password and account lockout policies for their accounts?	x		×	
		IAM-12.10	1	Do you support the ability to force password changes upon first logon?	x		_ ^	
		IAM-12.11	4	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?			x	
Identity & Access Management	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.					
Utility Programs Access			4	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?			x	
Infrastructure & Virtualization Security	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory	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	
Audit Logging / Intrusion Detection		IVS-01.2	compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity	Is physical and logical user access to audit logs restricted to authorized personnel?	x			
		IVS-01.3	anomalies, and to support forensic investigative capabilities in the event of a security breach.	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?			x	
		IVS-01.4	4	Are audit logs centrally stored and retained?	x	1		
Infrastructure &	IVS-02	IVS-01.5	The provider shall ensure the integrity of all virtual machine images at all times.	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?  Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormans, off or running)?		×	x	
Virtualization Security Change Detection		IVS-02.2	Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?			x	
		IVS-02.3	change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available			×	
Infrastructure &	IVS-03	IVS-03.1	methods (e.g., portals or alerts).  A reliable and mutually agreed upon external time source shall be used to purchase in the outer state of the property of t	to customers through electronic methods (e.g., portals or alerts)?				
Clock Synchronization			synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	x			
Infrastructure & Virtualization Security	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?			x	
Copocity / Resource Planning		IVS-04.2	accordance with legal, statutory, and regulatory compliance obligations.  Projections of future capacity requirements shall be made to mitigate the risk.	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			x	
		IVS-04.3	of system overload.	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	x			
		IVS-04.4		is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	x			
infrastructure & Virtualization Security	IVS-05	IVS-05.1	implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization					
Monagement - Vulnerability			aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	x			
Monagement								
infrastructure &	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections.	For your laaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			x	
Network Security		IVS-06.2	These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and	Do you regularly update network architecture diagrams that include data flows between security domains/zones?			x	
		IVS-06.3	compensating controls.	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?			x	
		IVS 06.4	Each operating system shall be hardened to provide only necessary ports.	Are all firewall access control lists documented with business justification?			x	
Virtualization Security	105-07	105-07-1	protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls				
Base Controls			part of their baseline operating build standard or template.	(e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	x			
Infrastructure &	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	x			
Virtualization Security Production / Non-		IVS-08.2	unauthorized access or changes to information assets. Separation of the	For your laaS offering, do you provide tenants with guidance on how to create suitable production and test environments?				
Fournaments Infrastructure &							x	
Virtualization Security Segmentation	IVS-09	IVS-08.3 IVS-09.1	authentication sources, and clear segregation of duties for personnel accessing these environments as part of their inh duties Multi-tenant organizationally-owned or managed (physical and virtual)	Do you logically and physically segregate production and non-production environments?  Are outern and network environments contacted by a financial or without financial to ensure business and outerness convicts requirements?	x		x	
	IVS-09	IVS-08.3 IVS-09.1 IVS-09.2	authentication sources, and clear segregation of duties for personnel accessing these monitonements is next of their inch duties. Multi-tenant organizationally womed or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured south that provider and	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?  Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual.			x	
	rvs.o9	IVS-08.3 IVS-09.1 IVS-09.2 IVS-09.3	authentication sources, and clear segregation of duties for personnel accessing the commissionments as over of their inch duties. Multi-teams to generationally-even for managed (physical and virtual) applications, and infrastructure system and network components, phill be designed, developed, deployed, and configured such that provider and outcome featuring user access is appropriately segmented from other tenant users, based on the following conditions.	Are system and network environments protected by a firewall or virtual firewall to ensure budness and customer accurity requirements? Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and controlled.  The system and network environments protected by a firewall or virtual firewall to ensure compliance with legal regulatory and controlled to the controlled or firewall to ensure compliance with legal regulatory and controlled to the controlled to receive any environments for the receiver requirements for the results requirement for the receiver requirements for the results requirement and the receiver requirements for the results requirements and the results are requirements for the results are requirements and the results are requirements for the results are requirements and the results are requirements.	x x		x	
	IVS-09	IVS09.1 IVS09.2 IVS09.3 IVS09.4	authentication natures, and clear aggregation of festive for personnel accessing these amenimental can see and trible facilities. Must 1-managed (physical and virtual) publications, and inflatantizatures system and retwork components, shall be diseigned, divelloped, disployed, and configured such that provider and castome (plannal) pure access is appropriately aggressed for hother provider and castome (plannal) pure access is appropriately aggressed for hother transmit — Established policies and procedures — Established policies and procedures.	As system and network environments protected by a frewall or virtual frewall to maure business and customer according requirements?  As system and reduced, environments protected by a flewall or virtual frewall to ensure orongenous with legal regulatory and controcated.  Proceedings of the control or protected by a flewall or virtual frewall to ensure orongenous the legal regulatory and controcated protections. The proceedings of the proceedings	x x x		x	
	IVS 09	IVS-08.3 IVS-09.1 IVS-09.2 IVS-09.3 IVS-09.4	arbentication source, and claim arguegation of dutation for personnal accounts between excessorate and arbeit arbeit and arbeit and program and revised application and virtual applications, and orbitativity assignment and reference components, that the applications, and orbitativity are support and year or the arbeit and arbeit and southern the plant type access is applicated by application and that provide and southern the plant type access is applicated by application and the program of a "Established policies" and procedures.  **Institution of business critical assess and/of sensitivity used data and assessment and arbeit or business critical assess and/of sensitivity used data and assessment Compilations with long further type and pulsary compilations collecting Compilations with long further type and pulsary compilations collecting consistency and controlled are supported to the controlled and are consistent as the controlled assessment and are consistent as the controlled assessment and are controlled assessment and are controlled assessment and are supported as a controlled assessment as a controlled assessment and and a controlled assessment as a controlled assessment as a controlled as a controlled assessment as a controlled assessment as a controlled as a controlled assessment as a controlled assessment as a controlled as a controlled assessment as a controlled assessment as a controlled as a controlled assessment as a controlled as a controlled assessment as a controlled as a controlled as a controlled controlled as a controlled as a controlled a	As system and network environments protected by a firewalf or virtual frewalf to ensure business and customer accurity requirements?  As system and reduceds, environments protected by a firewalf or virtual frewalf to ensure orospiscos with legal, requirements?  As system and reduceds, environments protected by a firewalf or virtual frewalf to ensure protected and reduced as the purpose of the protection of the purpose of t	x x x		x	
infrastructure & Virtualization Security	IVS-09	IVS-08-3 IVS-09-1 IVS-09-2 IVS-09-3 IVS-09-4 IVS-09-5 IVS-10-1 IVS-10-2	where the control was experienced and the supportion of districts for promotional accuracy and associations and an experienced and the control of the contr	An appear and interest environments protected by a forward or writing forward to environmental contents and contents and contents and contents and experiments of the system and extent or the state completion for the state completion of the state o	x x x		×	
infrastructure & Virtualization Security VM Security - Data Protection infrastructure &	IVS-10	IVS-09-1 IVS-09-2 IVS-09-3 IVS-09-4 IVS-09-5 IVS-10-1 IVS-10-2	whether common sources, and clear supportion of decide for previous decidents previous and common sources and common sources and common sources applications, and inflatation clear segment and remarks components, shall be designed, developed, and configured and components, shall be designed, developed, and configured and the provider and contains the beautify use accessed application of segments for most the standard common sources are proprietably agreement for most or treated a fastilization policies and optionative a "landardinary policies and optionative and mandards compress and policy and policies and and mandards compress and policy and policies and and mandards compress and control policy and collisional policy and mandards compress and control policy and common and policies and a policy and a policy and a policy and a policy and a policy and a policy policy and a policy policy and a policy and a policy and and a policy and and and and and and and and	As system and network environments protected by a firewalf or virtual frewalf to ensure business and customer accurity requirements?  As system and reduceds, environments protected by a firewalf or virtual frewalf to ensure orospiscos with legal, requirements?  As system and reduceds, environments protected by a firewalf or virtual frewalf to ensure protected and reduced as the purpose of the protection of the purpose of t	x x x		x x x	
Virtualization Security VM Security - Data Protection	(VS-10	IVS 08.3 IVS 09.1 IVS 09.2 IVS 09.3 IVS 09.4 IVS 09.5 IVS 10.1 IVS 10.2	Antheritication sources, and clear supportion of dicties for promoted accessing measurements and antheritication of the control of the contr	An option and interests environmental protected by a forward or retail forward to environ because and customer security requirements of any option and network environmental protected by a forward or retail forward to environ because and customer security requirements of any option and any option of the protection of	x x x		x x	
Virtualization Security VM Security - Data Protection	NS10	IVS-09-1 IVS-09-2 IVS-09-3 IVS-09-4 IVS-09-5 IVS-10-1 IVS-10-2	whether common sources, and clear supportion of decide for previous decidents previous and common sources and common sources and common sources applications, and inflatation clear segment and remarks components, shall be designed, developed, and configured and components, shall be designed, developed, and configured and the provider and contains the beautify use accessed application of segments for most the standard common sources are proprietably agreement for most or treated a fastilization policies and optionative a "landardinary policies and optionative and mandards compress and policy and policies and and mandards compress and policy and policies and and mandards compress and control policy and collisional policy and mandards compress and control policy and common and policies and a policy and a policy and a policy and a policy and a policy and a policy policy and a policy policy and a policy and a policy and and a policy and and and and and and and and	An appear and interest environments protected by a forward or writing forward to environmental contents and contents and contents and contents and experiments of the system and extent or the state completion for the state completion of the state o	x x x		×	
Virtualization Security VM Security - Data Protection Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening		NS-09-1 NS-09-2 NS-09-3 NS-09-4 NS-09-5 NS-10-1 NS-10-2	arbenticiono source, and clara segregation of decide for previous description of the company of	An option and interest environments protected by a forward or writing forward to environmental customer acceler requirements of a system and interest environments protected. As yet less of with an experiment of the environments protected and appropriate boolston and supermentally experiments of the experiment of experiments of the exp	x x x		x x	
Virtualization Security VM Security - Data Protection	N509	IVS-09-1 IVS-09-2 IVS-09-3 IVS-09-4 IVS-09-5 IVS-10-1 IVS-10-2	arbentication burses, and claur supportion of direct for previous accessing the contraction of the contract	An option and interest environments protected by a forward or writing forward to environmental customer acceler requirements of a system and interest environments protected. As yet less of with an experiment of the environments protected and appropriate boolston and supermentally experiments of the experiment of experiments of the exp	x x x		x x	
Virtualization Security VMA Security - Data Pratection Infrastructure & Virtualization Security VMMA Security Hypervisor Hardening		NS-09-1 NS-09-2 NS-09-3 NS-09-4 NS-09-5 NS-10-1 NS-10-2	arbentication burses, and class asymptoms of active for previous accessing the activation of the control of th	segotion and intensity environments protected by a forward or writing forward to environmental contraction environments protected by a forward or writing forward to environmental or environmental contractions and contractions are sufficiently as a forward or writing forward to environmental contractions and contractions are sufficiently and sufficiently and sufficiently are sufficiently and procedures established and mechanisms configured and implications such sufficiently are sufficiently and procedures established and mechanisms configured and improve such sufficiently are sufficiently and procedures established and mechanisms configured and improve such sufficiently are sufficiently and procedures established and mechanisms configured and improve such sufficiently are sufficiently and procedures are sufficiently and procedures are sufficiently and procedures are sufficiently and sufficiently and procedures are sufficiently and sufficiently are sufficiently and sufficient and sufficiently are sufficiently and sufficient and sufficiently are s	x x x x		x x	
Virtualization Security VMA Security - Data Pratection Infrastructure & Virtualization Security VMMA Security Hypervisor Hardening		NS-09-1 NS-09-2 NS-09-3 NS-09-4 NS-09-5 NS-10-1 NS-10-2	arbenticiono source, and clara segregation of districts for previous all accessing designations and an arbenticida districts and arbenticida districts.	segment and it describe environments prosted by a forward or wind freeable to environments and customer security requirement?  As system and referred with environments presided by a forward or wind freeable to environment and customer security requirement?  As system and referred with environments prosted by a feward or wind freeable to environment and environment and extraction and support and contribution of the page properties solidated and expensation of the internation and extraction and expensation and expensation or the expensation of the expensation	x x x x x		x x	
Virtualization Security VMA Security - Data Pratection Infrastructure & Virtualization Security VMMA Security Hypervisor Hardening		NS-09-1 NS-09-2 NS-09-3 NS-09-4 NS-09-5 NS-10-1 NS-10-2	arbenticiono source, and clara segregation of desides for previous description of the control of	sergetime and interests environments protected by a forward or virtual forward to enumer becomes and customer security requirements?  As system and notework environments protected by a forward or virtual forward to enumer becomes and customer security requirements?  As well as which in the territory or the environments or the appropriate booletion and apprendiction of bissenial access to inflationations or great the protection of the environments or the protection of the environment or the environment	x x x x x	x	x x	
Virtualization Security VMA Security - Data Pratection Infrastructure & Virtualization Security VMMA Security Hypervisor Hardening		NS-09-1 NS-09-2 NS-09-3 NS-09-4 NS-09-5 NS-10-1 NS-10-2 NS-11-1	arbenticiono sources, and claur approprient of divise for previous al accessing destination of the control and accessing and accessing and accessing applications, and inflamentarian years and natives for components, public applications, and inflamentarian years and natives for components, public designing, developed, and configured with the product and survey, based on the following considerations: and accessing a production of the configured and accessing a production of the matter and accessing a production of the configured and accessing a production of an accessing a production of the configured and accessing a production of the matter and accessing a production and big in head of animal accession of the production of the accession and big in head of animal accession developed and accession and accession and big in the accession of the accession production and accession and accession and the production of a cell and accession production accession accession and accession and accession and accession of the accession production accession accession and accession accession accession accession and production accession accessi	An explain and intensive minimization producted by a forward or with all forward to entral forward to entral continuous and cultivors with commonwhile producted by a New for with all forwards to entral complainments?  A region and intensive minimization producted by a New for with all forwards to entral complainments?  A region and the second production of the appropriate includes and algorithments?  Do you have the addity to legislarly regioned or entropic customer date such that date may be produced for a single intensive data?  Any potent and the addity to legislarly regioned or entropic customer date such that date may be produced for a single intensive data?  Any potent and intensive demonstrations to the second or virtual forwards to entral production and includes of an additional control or second and entraneous demonstrations and include the second and entraneous demonstrations and entran	x x x x x	x	x x x	
Virtualization Security Miscourity - County Miscourity Miscouri	NS 12	NS-091 NS-092 NS-093 NS-095 NS-101 NS-102 NS-101 NS-102 NS-101 NS-102 NS-103 NS	arbenticiono sources, and clarar segregation of desire for previous al accessing formation of the control and accessing and accessing seglications, and influentations gettern and retrained components, shall be designed, developed, and configence and consequents that the produce and seglications, and influentations gettern and retrained formations are seglicated and accessing a segment of the produce and seglications are segmentations and accessing a segment of the control accessing segments are segmentations and segments are segments and segments and an undest amonger internal control and high lovest of assurance of the segments and segments are segments and segments and accessing a segment of the segments are complianted with large segments and segments are segments. Segments are accessing a segment of the segments are segments as segments are segments as a segment of the segments are segments as segments are segments as segments are and to send our segments are segments as and to send our segments are and the segments are and to segment as and to segments are and to send our and to segments are and to segment as a segment of the segments are and to segment and a segment of the segments are and to segment as a segment and a and segments are and to segment as and to segments and and and and and and and and	An option and network environments protected by a forward or virtual forward to environmental contents and co	x x x x x	x	x x	
Virtualization Security Miscourity - Advances  Miscourity		NS-09-1 NS-09-2 NS-09-3 NS-09-4 NS-09-5 NS-10-1 NS-10-2 NS-11-1	Ambertication sources, and clear appropriate of solid sets by previous of accessing Management and Control and Co	Any other and relevant environments prostocide by a forward or writted forward to environmental control environments and environments	x x x x x	x	x x x	
Virtualization Security  Mi Security - VM Se	NS 12	NS-091 NS-092 NS-093 NS-095 NS-101 NS-102 NS-101 NS-102 NS-101 NS-102 NS-103 NS	arbenticiono sources, and clara segregation of desire for previous accessing alternativamente anno arbentición desire. A segregation de service de la contractiva del la contractiva de la contractiva del la contractiva de la contractiva del la contractiva d	An experiment of extension environments protected by a forward or writing forward to environmental contension and customer security resourcements of any system and colored environments protected by a forward or writing forward to environmental contension and customer security resourcements of the appropriate biolistics and segmentation of the appropriate biolistics and section of the appropr	x x x x x x x x	x	x x x	
Withuillastion Security With Security - John of Miscourity - John of Miscourity - Withuillastion Security Withuillastion Security - MMM Security - Impervious Security Withuillastion Security Antonio Aschillecture  Materiaps reputation of Withuillastion Security Antonio Miscourity Security S	NS-12 NS-13 IPY01 IPY02	N5091 N5092 N5094 N5095 N5101 N5101 N5101 N5102 N5111 N5112 N5123 N5123 N5112 PV011	arbenticiono sources, and claur approprient of divise for previous al accessing automatica de la companio del la companio de la companio del la companio della companio del la companio del l	sergetime and interest invariance appropriate by a forward or virtual forward to enumer becomes and customer security requirement?  As system and colored with constructions of the security o	x x x x x	x	x x x	
Virtualization Security Miscarley, Obtor	(V5-12 (V5-13	N5001 N5003 N5004 N5005 N5102 N5102 N5111 N5121 N5121 N5122 PV011 PV011	arbenticiono louces, and clara segregation of discles for previous al accessing transmissiones and accessing and accessing and accessing seglication, and influentaciones plants and natural components, public seglication, and influentaciones plants and natural components, public seglication, and influentaciones and accessing accessing accessing a seglication of the following considerations and accessing accessing a service and accessing a seglication of the seglication of the seglication of the following consideration and high level of classication and in made to engage and productions. See a seglication of the seglication of the seglication of the seglication of the seglication of the seglication of the seglication of the seglication of the seglication of the seglication consideration of the seglication of the seglication of the seglication seglication of the seglication of the seglication of the seglication seglication of the seglication of the seglication of the seglication of the seglication seglication of the seglication of the seglication of the seglication of the seglication seglication of the seglication of the seglication of the seglication of the seglication seglication of the seglication of the seglicat	An experiment of extension environments protected by a forward or writing forward to environmental contension and customer security resourcements of any system and colored environments protected by a forward or writing forward to environmental contension and customer security resourcements of the appropriate biolistics and segmentation of the appropriate biolistics and section of the appropr	x x x x x x x x	x	x x x	
Withuillastion Security With Security - John of Miscourity - John of Miscourity - Withuillastion Security Withuillastion Security - MMM Security - Impervious Security Withuillastion Security Antonio Aschillecture  Materiaps reputation of Withuillastion Security Antonio Miscourity Security S	NS-12 NS-13 IPY01 IPY02	N51031 N51033 N51034 N51031 N51031 N51031 N5112 N51131 N51131 N51131 N51131 PV011 PV011	arbenticiono sources, and clarar segregation of acides for previous of accessing designation control and accessing acides accessing acides accessing acides	An experiment of interest environmental protected by a forward or virtual forward to environmental control control and control and a speciment of the environmental protected by a forward or virtual forward to environmental protected and control and a speciment of the environmental protected by a forward or virtual forward to environmental control control and environmental and environmental and environmental and environmental and environmental and environme	x x x x x x x x x x x x x x x x x x x	x	x x x	
Websition Neorly Michiganity John Missioners B. Missioners	PY01 PY02 PY03	N5101 N5003 N5003 N5003 N5101 N5101 N511 N5111 N	arbenticiono sources, and clara segregation of actives for presented accessing activation and accessing activation of the composition of accessing applications, and inflamentation accessing activation and accessing applications, and inflamentations accessing acce	An experiment of section of minimum control producted by a forward or writing forward to environmental control environmental control of section of production and control environmental control of section of production and control environmental control of the appropriate biolistics and segmentation of the environmental control of the e	x x x x x x x x x x x x x x x x x x x	×	x x x x x	
Antoniomos security displacement of the control of	NS-12 NS-13 IPY01 IPY02	W5001   W5003   W5004   W5004   W5005   W5102   W5102   W5102   W5102   W5102   W5102   W5103   W5103   W5005   W500	arbenticiono sources, and claur segregation of actives for presented accessing accessing a segregation of accessing a segregation of accessing segregation, and influentacions yet man and research components, shall be application, and influentacions yet man and research components, shall be adapted, developed, and configured accessing accessing a segregation of a segregation of the following considerations of the segregation of the segregation of the segregation of the production of a segregation of the segregation of the production of segregation of segregation of the segregation of the production of segregation segregation segregation segregation of segregation segregation segregation segregation of seg	An explant and colored minimum expression producted by a forward or virtual forward to enumer benines and customer security resourcement?  As system and colored for an excessary measurement for the appropriate boridon and supermental or the security of t	x x x x x x x x x x x x x x x x x x x	×	x x x x x	
Antonional Security Andread Security Se	PY01 PY02 PY03	97011 97012 97013 95101 95101 95101 95101 95101 97011 97011 97011 97011 97013	arbenticiono sources, and clarar segregation of actives for presented accessing formation of the control and accessing accession accessing accession access	the system and released new intermental producted by a forward or virtual forward to search content and customer security requirements of the system and released new intermental producted by a forward or virtual forward to service complete and customer security requirements of the system and released to the successful producted by the system and released to the successful producted by the system and released to the successful producted by the system and released to the successful producted by the system and released to the successful producted by the system and released to the system and released to the successful producted by the system and released to the successful producted by the system and released to the system and released to the system and released to the successful producted by the system and released to the protection for the system and released to the protection and released to the released t	x x x x x x x x x x x x x x x x x x x	x	x x x x x	
Antonious Security Medical Conference in Con	PY01 PY02 PY03	W1012   W101	arbenticiono sources, and clarar segregation of desires for presented accessing desirementation and annual arbenticida desirementation and accessing seglications, and influentations general and research components, shall be disaggined, developed, and configered and that provides and seglications, and influentations general and accessing a segmentation of the seglication of the development of the segmentation of the segmentation of the segmentation of the development of the segmentation of the segmentation of the segmentation of the segmentation of the segmentation of the segmentation of segmentation of the segmentation of the segmentation of the segmentation of segmentation of the segmentation of the segmentation of the segmentation of segmentation	sergicine and released environments protected by a feward or writing feward to environments and customer south resourcements and systems and released environments protected by a feward or writing feward to environments and customer souther resourcements and explanations and systems and released environments and explanations and explanations and segmentation of the supposition of the supposition and segmentation of the supposition of the supposition and segmentation of the supposition of supposition of the supposition of the supposition of the supposition of supposition of the supposition of the supposition of supposition of the supposition of s	x x x x x x x x x x x x x x x x x x x	x	x x x x x x x x	
Antonional Security Andreas  Antonional Security Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional     Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional    Antonional     Antonional     Antonional     Antonional     Antonional     Antonional     Antonional     Antonional     Antonional     Antonional     Antonional     Antonional      Antonional     Antonional     Antonional     Antonional     Antonional     Antonional     Antonional      Antonional      Antonional      Antonional      Antonional      Antonional      Antonional      Antonional      Antonional       Antonional      Anto	PY01 PY02 PY03	97011 97012 97013 95101 95101 95101 95101 95101 97011 97011 97011 97011 97013	arbenticiono nueves, and clara segregation of actives for previous al accessing applications, and inflastructures petime and natives of an extra segregation of actives and previous and previous applications, and inflastructures petime and natives for components, public applications, and inflastructures petime and natives for components, public applications, and inflastructures petime and natives for components, public designations, and an extra segregation of providents and segregations and in material segregations and intelligent and an elementary and an extra segregation of providents and high health and an elementary designations and active petime and control sea of high health and segregations of the previous and active petime and active and an elementary designation of the active petime and active and health and active and previous and active petime and active and active and active and previous and active petime and active and active and active and active and previous and active and active and active and active and active and previous active and active and active and active and active and previous active and active and active and active and previous active and active and active and active and previous active active and active and active and previous active active providents and previous active active and active	segment and retends environments protected by a forward or virtual forward to environmental control environmental control environments and customer security requirements?  A regular and color environments protected by a forward or virtual forward to environmental control environments and customer and customer and control environments and customer and 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 x x x x x x x x x x x x x x x	
Antonianous Security Andreadous Security Securit	PY01 PY01 PY02 PY03 PY04	1000   1000	arbenticiono locarea, and clarar segregation of actives for presental accessing accession and accessing accession and accession accessi	An experiment of interest invariancement speciation by a forward or virtual forward to consist outcomes accult requirement of the special production	x x x x x x x x x x x x x x x x x x x	x	x x x x x x x x	
And Annual Security of London London Security of London	9701 9701 9703 9703 9705	W1001   W1002   W1003   W100	arbenticiono sources, and claur segregation of actives for previous all accessing segregations of a segregation of actives for previous and accessing segregation, and influentations gettern and research components, shall be disaggined, developed, and configured active segregation of actives and segregation developed actives and active segregation of active segregation of segregation developed actives and segregation of active segregation of segregation of the following considerations of the segregation of the produce and segregation of the segregation of the produced segregation of segregation of the segregation of the produced segregation of segregations of segregation of the segregation of the produced segregation segregation of segregation of the segregation of the produced segregation segregation of segregation of the produced segregation of segregation of segregation of segregation of the produced segregation segregation of segregation of the produced segregation of segregation of segregation of segregation of the produced segregation segregation of segregation of the produced segregation of segregation of segregation of the produced segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation of segregation segregation segregation and segregation segregation of segregation segregation segregation segregation segregation segregation segregation segregation segregation segregatio	largetime and interests environmental protected by a forward or virtual forward to environmental control control and organization of the specimen and control control control and a specimen and control control control and a specimen and control control control and a specimen and control	x x x x x x x x x x x x x x x x x x x	x	x x x x x x x x x x x x x x x x x x x	
Antonional searchy Antonional se	PY01 PY02 PY03 PY03 PY05 PY05 M0501	1000   1000	arbenticiono sources, and clarar segregation of acides for previous of accessing descriptions of acides o	Any other and relevant environments protected by a forward or writing forward to environments and customer security resourcement?  Any open and collected the environments protected by a forward or writing forward to environments and customer security resourcements?  Any open and environments are environments and environments environments. The environments are environments are environments are environments are environments are environments are environments. A proportion are environments are environments are environments are environments are environments are environments are environments. A proportion are environments are environments are environments are environments. A proportion are environments are environments are environments are environments. A proportion are environments are environments are environments are environments. A proportion are environments are environments are environments are environments. A proportion are environments are environments are environments. A proportion are environments are environments are environments are environments. A proportion are environments are environments are environments are environments are envi	x x x x x x x x x x x x x x x x x x x	x	x x x x x x x x	
Antonional search  Antonional se	9701 9701 9703 9703 9705	W1001   W1002   W1003   W100	arbenticiono nueves, and clara segregation of actives for previous al accessing activation and accessing activation of the composition of accessing applications, and influentacions yet and activate of accessing applications, and influentacions yet and activate compositions, public applications, and influentacions yet accessing accessing accessing applications, and accessing accession accessing accessing accessing accessing accessing accessing accession accessing accessing accessing accessing accessing accessing accessing accessing accession accession accessing accessing accession accession accession accession acces	Interest the experimental and interest invariance interest producted by a forward or written forward to consist and customer acutify requirement?  As spotlam and colored interest interest consistent and the experimental consistent and customer acutify requiremental consistent and specimental consistent and colored interest	x x x x x x x x x x x x x x x x x x x	x	x x x x x x x x x x x x x x x x x x x	
Antonious Security  Million Control Control  Million Cont	PY01 PY02 PY03 PY03 PY05 PY05 M0501	W1001   W1002   W1003   W100	arbenticiono sources, and claur appropries of divise for previous accessing applications, and influentations yet and an arbenticion and arbenticion arbenticion arbenticion arbenticion arbenticion arbenticion arbenticion arbenticion arbenticion arbenticiona arbentici	Any other and released environments protected by a forward or writing forward to environments and customer security resourcements?  Any open and college environments protected by a forward or writing forward to environments and customer security resourcements?  Any open and college environments protected by a forward or writing forward to environments and customer security and college environments.  On you have the saddly to begoin a sequence or enough customer and state with the data may be produced for a department only, without environments and college environments protected by a forward or writing or an analysis of the saddly to be possible sequence or enough customer and state with the data may be produced for a department or writing and college environments protected by a forward or virtual forward to a security protection and installation of amounts and a security and a security protected by a forward or virtual forward to a security produced or writing and a security or security	x x x x x x x x x x x x x x x x x x x	x	x x x x x x x x x	
And the second of the second o	PY01 PY01 PY02 PY03 PY03 PY04 PY05 M0501 M0502 M0504	W5001 W5003 W5003 W5003 W5101	arbenticiono sources, and claur segregation of actives for presented accessing accessions and accessing accessions and accessions accessions and accessions applications, and influentacions gettern and natives for components, shall be disaggined, developed, and configured active products of accession applications, and influentacions gettern accessions acce	Any other and relevant worknowness, prostocial by a forward or writing forward to enumer beneficial and control or support of the special power of the forward or writing forwards to enumer beneficial and support of the special power of the p	x x x x x x x x x x x x x x x x x x x	x	x x x x x x x x x x x x x x x x x x x	
Ministration & secret (Ministration & Secret (Ministration & Ministration & Minis	PY01 PY02 PY03 PY03 PY04 PY04 PY05 AXX-01 AXX-01 AXX-03	W5001 W5003 W5003 W5003 W5101	arbenticiono sources, and clarar segregation of actives for previous al accessing descriptions of the control	sergicine and released environmental protected by a forward or virtual forward to environmental contrave souther recurrences?  As system and released environmental protected by a forward or virtual forward to environmental contrave environmental protection or a system and released environmental protection or a system and released environmental protection or a system and released to environmental protection of the appropriate independent of the appropriate or environmental protection and suppressed or environmental protection of the appropriate or environmental protection of the appropriate or environmental protection or a system and the appropriate or environmental protection or a system and the appropriate or environmental protection or a system and the appropriate or environmental protection or a system and the approving an environmental protection or an	x x x x x x x x x x x x x x x x x x x	x	x x x x x x x x x	
Antonious Security  Apparent  Appare	PY01 PY01 PY02 PY03 PY03 PY04 PY05 M0501 M0502 M0504	W5001 W5003 W5003 W5003 W5101	arbenticiono sources, and claur approprient of direct for previous al exempt applications, and inflastructures pleane and referent components, public applications, and inflastructures pleane and referent components, public applications, and inflastructures pleane and referent components, public designates, developed, and configured next the produce and surface and productions.  In the surface and applications of the surface and productions and surface and productions.  In the surface and productions of the surface and productions of the surface and productions of the surface and productions of the surface and productions of the surface and the surface and surface and surface and productions of the surface and surface and surface and publications are surface and surface and surface and publications are surface and surface and publications are surface and surface and surface and publications are surface and surface and publications are surface and publications and procedures and surface and publications are surface and publications and procedures shall be established, and supporting business processes were and publications and procedures shall be established, and supporting business processes were and publications and procedures shall be established, and supporting business processes were and publications and procedures shall be established, and supporting business processes were and publications and procedures shall be established, and supporting business processes were and publications and procedures shall be established, and supporting business processes were and publications and procedures shall be established, and supporting business shall be publications; and shall be a subject of the support of publications and procedures shall be established, and shall be a support of shall be a support of publications and procedures shall be established by the articles of shall be a support of	Any other and released environments protected by a forward or writing forward to environments and customer security resourcements?  Any open and college environments protected by a forward or writing forward to environments and customer security resourcements?  Any open and college environments protected by a forward or writing forward to environments and customer security and college environments.  On you have the saddly to begoin a sequence or enough customer and state with the data may be produced for a department only, without environments and college environments protected by a forward or writing or an analysis of the saddly to be possible sequence or enough customer and state with the data may be produced for a department or writing and college environments protected by a forward or virtual forward to a security protection and installation of amounts and a security and a security protected by a forward or virtual forward to a security produced or writing and a security or security	x x x x x x x x x x x x x x x x x x x	x	x x x x x x x x x	

Mobile Security								
Cloud Based Services	MUS-06	MUS-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 data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			×	
Mobile Security	MOS-07	MOS-07.1	The company shall have a documented application validation process to test	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			×	
Compatibility Mobile Security	MOS-08	MOS-08.1	for mobile device, operating system, and application compatibility issues.  The BYOD policy shall define the device and eligibility requirements to allow for					
Device Eligibility			BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			x	
Mobile Security  Device Inventory	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices. (i.e.					
			operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			×	
			each device in the inventory.					
Mobile Security	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or			x	
Device Management Mobile Security	MOS-11	M0S-11.1	mobile devices permitted to store, transmit, or process customer data.  The mobile device policy shall require the use of encryption either for the entire	process company data?				
Encryption	MOS-11	MUS-11.1	device or for data identified as sensitive on all mobile devices and shall be	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			x	
Mobile Security	MOS-12	M0S-12.1	enforced through technology controls.  The mobile device policy shall prohibit the circumvention of built-in security.	*				
Jailbreaking and	100-12	MOS-12.2	controls on mobile devices (e.g., jailbreaking or rooting) and is enforced	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jaiibreaking or rooting)?  Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the			×	
Rooting			through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	circumvention of built-in security controls?			x	
Mobile Security Legal	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			x	
Mobile Security	MOS-14	MOS-13.2 MOS-14.1	clearly state the expectations over the loss of non-company data in the case BYOD and/or company owned devices are configured to require an automatic	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	
Lockout Screen	N/US-14	MUS-14.1	lockout screen, and the requirement shall be enforced through technical	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			x	
Mobile Security	MOS-15	MOS-15.1	controls.  Changes to mobile device operating systems, patch levels, and/or applications					
Operating Systems	MUS-15	MUS-15.1	shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management			x	
Mobile Security	M05-16	M05-16.1	Password noticies applicable to mobile devices shall be documented and	processer				
Passwords	MU5-16	MUS-16.1 MOS-16.2	enforced through technical controls on all company desices or desices	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			x	
		MOS-16.3	approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Are your password policies enforced through technical controls (i.e. MDM)?  Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			x	
Mobile Security Policy	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			x	
Policy		MOS-17.2	data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			×	
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			×	
Mobile Security	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			×	
Remote Wipe		MOS-18.2	company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			×	
Mobile Security Security Patches	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			×	
,		MOS-19.2	All mobile devices shall have the latest available security-related patches	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			 X	
Mobile Security	MOS-20	MOS-20.1	installed upon general release by the device manufacturer or carrier and The BYOD policy shall clarify the systems and servers allowed for use or access	Does your 8YOD policy clarify the systems and servers allowed for use or access on the 8YOD-enabled device?			×	
Users		MOS-20.2	on a BYDD-enabled device.	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			x	
Security Incident Management F	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and					
Management, E- Discovery, & Cloud			regularly updated (e.g., change in impacted-scope and/or a change in any	Down exists a listener and points of contract with local authorities is				
Forensics Contact/Authority			compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	×			
Mointenance			engagement with law enforcement.					
Security Incident	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes	Do you have a documented security incident response plan?		x		
Discovery, & Cloud		SEF-02.2	and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service	Do you integrate customized tenant requirements into your security incident response plans?		x		
Security Incident Management, E- Discovery, & Cloud Forensics Incident Management		SEF-02.3	management policies and procedures.	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		х		
		SEF-02.4		Have you tested your security incident response plans in the last year?	_	х		
Security Incident Management, E-	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security	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?	×			
Security Incident Management, E- Discovery, & Cloud Forensics		SEF-03.2	report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a	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?		×		
Security Incident	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and				
Management, E- Discovery, & Cloud		SEE OA 2	presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification,	controls?		×		
Forensics		SEF-04.2 SEF-04.3	customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?  Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant.		х		
Legal Preparation		2,104.3	breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	те ром сиримне от имуритетид индивион ногох (неизм от инш и ноги и хрестьс point in time) for a specific tenant without freezing other tenant data?	x			
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	х			
Security Incident Management, E-	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	х			
Discovery, & Cloud	STA-01	SEF-05.2 STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain	Will you share statistical information for security incident data with your tenants upon request?	х			
Management,	35A-01	STA-01.1 STA-01.2	partners to correct data quality errors and associated risks. Providers shall	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?  Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and		×		
Transparency, and Accountability			design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege	Do you design and imprement 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?	×			
Supply Chain Management,	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.,			1		
Transparency, and			portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., oortals)?		×		
Incident Reporting			1					
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?	х			
Transparency, and		STA-03.2	application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed,	Do you provide tenants with capacity planning and use reports?		x		
Supply Chain Management	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.					
Transparency, and			and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and	x			
Provider Internal			1	metrics?	*			
Assessments			<u>                                     </u>			<u></u>	<u> </u>	<u></u>
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		1	
Transparency, and		STA-05.2	provisions and/or terms:	transmitted?  Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	x		1	
Third Party		STA-05.3	<ul> <li>Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and</li> </ul>	Does legal counsel review all third-party agreements?	x		1	
regreements		STA-05.4		Does regal counsel review all third-party agreements?  Do third-party agreements include provision for the security and protection of information and assets?	x	1	1	
		STA-05.5	subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance	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	considerations)	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?			x	
		STA-05.7	<ul> <li>Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references</li> </ul>	Can you provide the physical location/geography of storage of a tenant's data upon request?	х			
		STA-05.8	to detailed supporting and relevant business processes and technical measures	Can you provide the physical location/geography of storage of a tenant's data in advance?	×			
		STA-05.9	implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business real significant	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?			x	
		STA-05.10	business relationships  Notification and/or pre-authorization of any changes controlled by the	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	provider with customer (tenant) impacts  Timely notification of a security incident (or confirmed breach) to all	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?			×	
Supply Chain	STAOS	STA-05-12	customers (tenants) and other business relationships impacted (i.e., up-and Providers shall review the risk management and governance processes of their	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		х		
Management,			partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.					
Accountability			anneances norm ocner members or unac partners 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?		×		
Supply Chain Governance Reviews			1					
	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete,		1		
Supply Chain	31A-07		of service agreements (e.g., SLAs) between providers and customers (tenants)	accurate, and indexent agreements (e.g., S.k.a) between providers and customers (tenants)?  Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain	×			
Supply Chain Management, Transparency and	SIAO7	CT			x	1	1	1
Supply Chain Management, Transparency, and Accountability	SIAU	STA-07.2	across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established	(upstream/downstream)?				
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	SIAU	STA-07.2 STA-07.3	serous for televal as supply chain (uppartunity own-stamily recovers shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	(upstream/downstream)?  Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?			x	
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	314-07	STA-07.2 STA-07.3 STA-07.4	agreements. The reviews should result in actions to address service-level	bipstream(downstrain)?  Can you manage service bend conflicts or inconsistencies resulting from disparate supplier relationships?  Do you provide the senants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	×		x	
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	314-07	STA-07.3 STA-07.4 STA-07.5	agreements. The reviews should result in actions to address service-level	Jupateum (Momentzum)?  Canyou manage service-level conflicts or inconsistencies resulting from disparate supplier relationships2  Copyou provide teamstat with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?  Do you make standards based information security metrics (SSA, CAMM, etc.) available to your temants?		x	x	
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	314-07	STA-07.3 STA-07.4 STA-07.5 STA-07.6	agreements. The reviews should result in actions to address service-level	Lipstrame (Reconstration)  Lipstrame (Reconstration)  Despite a provision of the control of the	x	x	х	
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	314-07	STA-07.3 STA-07.4 STA-07.5	agreements. The reviews should result in actions to address service-level	Suptrace (Nonentrace)  Do you provide transits with origining visibility and reporting dryour operational Service Level Agreement (ELA) performance?  Do you provide transits with origining visibility and reporting of your operational Service Level Agreement (ELA) performance?  Do you need standards should information security weekinck (SEA, AAAM), etc.) available to you to transit?  Do you provide customers with origining visibilities and reporting of your VEA performance?  Do you data management profices and provideness address treated and service level conflicts of interests?	x x x	x	x	
Supply Chain Manage ment, Transparency, and Accountability Supply Chain Metrics  Supply Chain	STAGE	STA-07.3 STA-07.4 STA-07.5 STA-07.6	agreements. The reviews should result in actions to address service level conflicts to inconstruction resulting from disparate supplier relationships, the conflict of the construction of the conflict of t	Ligate and (Constitution)  Despise analysis and colored conflicts or in consideraticles resulting from disparate supplier relationships?  Despise provide insents with copying valuability and reporting of your operational fervice Liver Agreement (EA)-performance?  Despise provides insents with copying valuability and reporting of your SEA performance?  Despise provides continents with origining valuability and reporting of your SEA performance?  Despise provides continents with origining valuability and reporting of your SEA performance?  Despise provides continents with origining valuability and reporting of your SEA performance?  Despise provides continents with origining valuability and reporting of your SEA performance?  Despise provides continents with origining valuability and reporting of your SEA performance?  Despise provides and provides and reporting of your SEA performance?  Despise provides and provides and reporting of your SEA performance?	x x x	x	x	
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics Supply Chain Management,	STA-08	STA-07.3 STA-07.4 STA-07.5 STA-07.6	agreements. The reviews should result is actions to address service-level coefficies or inconsistencies resulting from disparate supplier relationships. The properties of the service o	Logistes and Reconstration	x x x x	x	x	
Supply Chain Manage ment, Transparency, and Accountability Supply Chain Metrics Supply Chain Manage ment, Transparency, and Supply Chain	STA 08	STA-07.3 STA-07.4 STA-07.5 STA-07.6 STA-07.7 STA-07.8 STA-08.1	agreement. The reviews though result is action to address service level conflict or incontributions or resulting from disparate supplier relationships, and the conflict of recentributions or resulting from disparate supplier relationships, and the conflict of the confli	Loyacean (Alexander Leave)  Carpor amangar and recisional collection of inconsident Clear resulting 1 from disquared supplier in all consisting 2  Source provide insents with cognitive of collection of inconsident Service Leave Agreement (E.A.) performance?  Source which settled the collection form that country collection (C.A.) CAMAR (e.A.) countries for port transfer?  Source which settled the collection form that countries (C.A.) CAMAR (e.A.) countries for port transfer?  Source which settled the collection form that countries (C.A.) CAMAR (e.A.) countries for port of the management of portion and providence and settled countries of the collection of the collection form of the collection of the collection of the collection form of the collection of the collection form of the collection of t	x x x	x	x	
Supply Chain Managament, Transparency, and Accountability Supply Chain Managament, Transparency, and Managament, Transparency, and Managament, Managam	STAGE STAGE	STA-07.3 STA-07.4 STA-07.5 STA-07.6 STA-07.7 STA-07.8 STA-08.1	Agreement. The revolves though result is actions to address control revolved conditions of the conditi	Ligate and Informational Composition of the Composi	x x x x x	x	x	
Supply Chain Management, Manag	\$1A-08 \$1A-08	STA-07.3 STA-07.4 STA-07.5 STA-07.6 STA-07.7 STA-07.8 STA-08.1	agreement. The reviews though result is action to address service level conflict or incontributions or resulting from disparate supplier relationships, and the conflict of recentributions or resulting from disparate supplier relationships, and the conflict of the confli	Logic team (Indicent team)  Copy on among are more cleared collect or inconsistent cise resulting from disparate supplier relationships?  Copy on among are more cleared collect or inconsistent cise resulting from disparate supplier relationships?  Copy on a set a standard work of agreement (SLA) (SAM) (Med. 1947)  Stopp on under standard seal of financial or search (SLA) (SAM) (Med. 1947)  Stopp on under standard seal of financial or search search (SLA) (SAM) (Med. 1947)  Stopp on other standards unpolitic and procedures desired. (SLA) (SAM) (Med. 1947)  Stopp on other standards unpolitic and procedures desired seatonships of the standards to team at an excellent seatonships of the standards to team at a seaton seatonships or seato	x x x x x	x	x	
Supply Chain Management, Transparency, and Accountability Supply Chain Menagement, Transparency, and Management, Transparency, and Supply Chain Management, Transparency, and Treat and World Chain Management, Transparency, and Treat and	STAG8 STAG9	STA-07-3 STA-07-4 STA-07-5 STA-07-5 STA-07-7 STA-07-8 STA-08-1 STA-08-2 STA-09-1 STA-09-2 TVM-01-1	agreement. The reviews should result in actions to address service level conflicts or inconstancing resulting from disparate supprior relationships.  Provider in All Insurer resourcing from disparate supprior relationships, and the provider in the service supply characteristic services. The review shall include supply characteristic services are supply characteristic services. The review shall include all partners which any providers shall demonstrate compliance with information supply characteristic services are supply characteristic services and information supply characteristic services are supply characteristic services and information supply characteristic services are supply characteristic services and information supply characteristic services are supply characteristic services and information supply characteristic services are supply characteristic services and supply characteristic services are supply characteristic services and supply characteristic services are supply characteristic services.	Logical read (Indianational)  Copyou analogue area incidented conflicts or inconsistencies resulting from disputate supplier relationships?  Sopou provide insents with engine; a classifier year in growing of proving proving a form of apparent source in and a present (ILA) performance?  Sopou make standards beneated information security mentations. (ICA, CAMA, et al., 1997)  Sopou make standards and information security mentations. (ICA, CAMA, et al., 1997)  Sopou make standards and information security and inporting of your SA performance?  Sopou design management policies and providers and interest interest and service level conflicts of interest?  Sopou welview and standards where agreements in latest amounts/y?  Sopou welview and standards where agreements and seat amounts/y?  Sopou welview and standards where agreements and seat amounts/y?  Sopou welview and standards where agreements and seat amounts/y?  Sopou makes reasoned information security zones you will which your information supply and individual particular plans of the seat of your interest and seat of the particular seat and seat of your interest and seat of the particular seat and seat of your interest and your seat and seat of your interest and your seat of your interest and your interest and you progressions are seat of your interest and your your gladifications and enterests?  Sopoul have after indiance programs that support or consect to your cloud service affering installed on all of your ITT infeatracture released.	x x x x x	x	x	
Supply Chain Management Accountability Supply Chain Menagement Accountability Supply Chain Menagement, Samper sery, and Menagement, Samper sery, and Menagement, Transper sery, and Thirst and and Menagement Management Menagement Men	STA 08  STA 09  TVM 01	STA-07.3 STA-07.4 STA-07.5 STA-07.6 STA-07.7 STA-07.8 STA-08.1	Agreement. The revolves though result is actions to address control level conditions of the conditions are considered by the dispersion of the conditions of	Logorous control contr	x x x x x	x	x	
Topply Chain Management, Manag	STAGE STAGE STAGE STAGE IVMG1	STA-07-3 STA-07-4 STA-07-5 STA-07-5 STA-07-7 STA-07-8 STA-08-1 STA-08-2 STA-09-1 STA-09-2 TVM-01-1	agreement. The revolves though result is action to address sortice level on effects or reconstruction resulting from disparate supposer realizability.  Providers that assure reasonable information security across their information supply chan by profitming as innuit review. The review shall include all supply chan by profitming as innuit review. The review shall include all supply chan be profitmed as a review of the review shall recorded and across the review shall record an except the review shall rev	Logical read (Indianational)  Copyou analogue area incidented conflicts or inconsistencies resulting from disputate supplier relationships?  Sopou provide insents with engine; a classifier year in growing of proving proving a form of apparent source in and a present (ILA) performance?  Sopou make standards beneated information security mentations. (ICA, CAMA, et al., 1997)  Sopou make standards and information security mentations. (ICA, CAMA, et al., 1997)  Sopou make standards and information security and inporting of your SA performance?  Sopou design management policies and providers and interest interest and service level conflicts of interest?  Sopou welview and standards where agreements in latest amounts/y?  Sopou welview and standards where agreements and seat amounts/y?  Sopou welview and standards where agreements and seat amounts/y?  Sopou welview and standards where agreements and seat amounts/y?  Sopou makes reasoned information security zones you will which your information supply and individual particular plans of the seat of your interest and seat of the particular seat and seat of your interest and seat of the particular seat and seat of your interest and your seat and seat of your interest and your seat of your interest and your interest and you progressions are seat of your interest and your your gladifications and enterests?  Sopoul have after indiance programs that support or consect to your cloud service affering installed on all of your ITT infeatracture released.	x x x x x x	x	x	
Topply Chain Strongerson, and Ranaparency, and Accountability Supply Chain Management, Management, Management, Management, Management, Management	STAGE STAGE STAGE TVMG1	STA-07-3 STA-07-4 STA-07-5 STA-07-5 STA-07-7 STA-07-8 STA-08-1 STA-08-2 STA-09-1 STA-09-2 TVM-01-1	Agreement. The revolves though result is actions to address service level condictor or reconstruction resulting them dispers an experient relationship is condictor. The reconstruction resulting them dispers are supplied relationship in supplied to all several resourced is reformed as a contract person and third relationship approximation by portationing as annual review. The review shall include all partners without party provident policy which that in other mation supply chain the approximation of the party provident policy which that in other mation supply chain the approximation of the party provident in the party provident in the formation to see a green expension of the party provident in the party provident that could provide expension and the contract in the party provident for a provident provident in the provident provident in the party provident and technical resources in explainment of the provident the execution of indiance on which could provide the provident provident in the party provident provident provident provident provident provident provident provident provident provident provident provident provident provident provident provident provident p	Logical modification control modification in consideractics resulting from disparate supplier relationships?  Stoppe provide insents with engine; a sicilarly and regioning of your operational Service Low Agreement (ELA) performance?  Stoppes make attended to admit information according modifications (ELA) CAMAGE (ELA) and CAMAG	x x x x x x x x x x x x x x x x x x x	x	x	
Supply Chain Management, Transpersors, and Accountability Lippely Chain Metrics Management, Transpersors, and Management, Transpersors, and Lippely Chain Management, Transpersors, and Management Transpersors, and Management	STAGE STAGE STAGE TVMG1 TVMG2	STA07.3 STA07.4 STA07.5 STA07.6 STA07.6 STA07.7 STA08.1 STA08.2 STA08.2 STA08.2 STA08.1 STA08.2 STA09.1 STA08.2 TWM01.1 TWM01.1 TWM02.2 TWM02.3	agreement. The revolves though result is action to address service level on effects or receivalence or resulting from dispara as supprior relationships, and the control of	Logorous control contr	x x x x x x x x x x x x x x x x x x x	x	x	
Topply Chain Management, Transpersery, and Accountability Supply Chain Market Supply Chain Market Supply Chain Management, Man	51A08 51A09 7VM01	\$74.07.3 \$14.07.4 \$14.07.5 \$14.07.5 \$14.07.8 \$14.07.8 \$14.08.1 \$14.08.2 \$14.09.2 \$14.00.2 \$14	Agreement. The revolves though result is action to address service level used. Cut or reconstruction resulting from disparate supplier relationships, and confect or reconstruction resulting from disparate supplier relationships.  Providers shall assess transcended in thou media succurry years that in the resulting resulting the supplier relationships and the state of the supplier relationships and the supplier relationship	Super service from the confidence of the confide	x x x x x x x x x x x x x x x x x x x	x	x	
Lappy Chain Management, Temparaco, and Accordability Surphy Chain Management, Surphy Chain Management,	STAGE STAGE STAGE THAGE THAGE	\$74.07.3 \$74.07.4 \$14.07.5 \$74.07.5 \$74.07.5 \$74.07.8 \$74.08.1 \$74.08.2 \$74.09.1 \$74.09.2 \$74.09.1 \$74.09.2 \$74.09.1 \$74.09.2 \$74.09.1 \$74.09.2 \$74.0 \$74	Agreements. The revolves though term in actions to address service level under the control of th	Logorous contractions of the committee o	x x x x x x x x x x x x x x x x x x x	x	x	
Supply Chain Suppl	STAGE STAGE STAGE TRAGE	\$74.07.3 \$14.07.4 \$14.07.5 \$14.07.5 \$14.07.8 \$14.07.8 \$14.08.1 \$14.08.2 \$14.09.2 \$14.00.2 \$14	Agreement. The reviews should result in actions to address service level as locked for increasements resulting them disperals supplier relationships, and the control of	Super service from the confidence of the confide	x x x x x x x x x x x x x x x x x x x	x x x x x	x	
Lappy Chain Sangarane, and Sangarane	STAGE STAGE STAGE STAGE THAGE THAGE	\$74.07.3 \$74.07.4 \$14.07.5 \$74.07.5 \$74.07.5 \$74.07.8 \$74.08.1 \$74.08.2 \$74.09.1 \$74.09.2 \$74.09.1 \$74.09.2 \$74.09.1 \$74.09.2 \$74.09.1 \$74.09.2 \$74.0 \$74	Agreement. The revolves though result is actions to address service level and confect or increasement resulting them disparate supplier relationships, which is a service of the conference of	Logorous control contr	x x x x x x x x x x x x x x x x x x x	x x x x	x	
Supply Chain Suppl	STAGE STAGE STAGE TVMG1 TVMG2 TVMG2	\$74.07.3 \$74.07.4 \$14.07.5 \$74.07.5 \$74.07.5 \$74.07.8 \$74.08.1 \$74.08.2 \$74.09.1 \$74.09.2 \$74.09.1 \$74.09.2 \$74.09.1 \$74.09.2 \$74.09.1 \$74.09.2 \$74.0 \$74	Agreement. The reviews should result in actions to address service level as locked for increasements resulting them disperals supplier relationships, and the control of	Lipschese informationally  Copy or among an environment control in consistent con resulting from disputate supplier in altisoniships?  Copy or among an environment of the design of the control in consistent control in the control i	x x x x x x x x x x x x x x x x x x x	x x x		

The Charles (Louring Visions) "Continues Assuments the United Associations of Cold Weeks 1.2" in the July New Conditions regulation are a state of the following julg life Continues Assuments to Institute Associations (Vision 1.2" in the Louring Life Continues Associations (Vision 1.2" in the Continues Associations (Vision 1.