Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Independent Audits	CO-02	CO-02.2	How often do you conduct network penetration tests of your cloud service infrastructure.
		CO-02.3	How often do you conduct regular application penetration tests of your cloud infrastructure?
		CO-02.4	How often do you conduct internal audits?
		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?
		CO-02.6	Are the results of the network penetration tests available to tenants at their request?
		CO-02.7	Are the results of internal and external audits available to tenants at their request?
Third Party Audits	CO-03	CO-03.1	Will you permit DPS to conduct vulnerability scans on hosted applications and your network?
		CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?
Audit Tools Access	IS-29	IS-29.1	How do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)
Information System Regulatory Mapping	CO-05	CO-05.1	How do you ensure customer data is logically segmented that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?
		CO-05.2	Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?
Intellectual Property	CO-06	CO-06.1	Describe the controls you have in place to protect tenants intellectual property?
Data Governance			

Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Ownership / Stewardship	DG-01	DG-01.1	Do you follow a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?
Classification	DG-02	DG-02.4	Can you provide the physical location/geography of storage of a tenant's data upon request?
		DG-02.5	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?
Handling / Labeling / Security Policy	DG-03	DG-03.1	Are Polices and procedures established for labeling, handling and security of data and objects which contain data?
Retention Policy	DG-04	DG-04.1	Describe technical control you have in place to enforce tenant data retention policies?
Secure Disposal	DG-05	DG-05.1	Describe your process for secure disposal or destruction of physical media and secure deletion or sanitization of all computer resources of DPS data once DPS has
Nonproduction Data	DG-06	DG-06.1	How do you ensure production data is be replicated or used in non-production environments?
Information Leakage	DG-07	DG-07.1	Describe the controls in place to prevent data leakage or intentional/accidental compromise between tenants.
		DG-07.2	What a Data Loss Prevention (DLP) or extrusion prevention solution is in place for all systems which interface with your cloud service offering?
Facility Security			
Controlled Access Points	FS-03	FS-03.1	Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?
Unauthorized Persons Entry	FS-05	FS-05.1	How are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled or isolated from data storage and process?
Asset Management	FS-07	FS-07.1	What are your procedures governing asset management and repurposing of equipment used to support DPS hosted services or data?
Human Resources Security			

Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Background Screening	HR-01	HR-01.1	Are state of residency and national fingerprint-based record checks conducted on employees or contractors who have access to DPS's data, applications or the networks supporting DPS's data and or applications?
Employment Agreements	HR-02	HR-02.1	Do you specifically train your employees regarding their role vs. the tenant's role in providing information security controls?
		HR-02.2	Do you document employee acknowledgment of training they have completed?
Employment Termination	HR-03	HR-03.1	Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?
Information Security			
Management Program	IS-01	IS-01.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?
Management Support / Involvement	IS-02	IS-02.1	Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?
Policy	IS-03	IS-03.1	Do your information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?
		IS-03.2	Do you have agreements which ensure your providers adhere to your information security and privacy policies?
	IS-04	IS-04.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?
Policy Reviews	IS-05	IS-05.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?
Policy Enforcement	IS-06	IS-06.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?
		IS-06.2	Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures?

Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
User Access Policy	IS-07	IS-07.1	What controls do you controls in place to ensure timely removal of systems access which is no longer required for business purposes?
User Access Restriction /	IS-08	IS-08.1	Describe process for granting and approving access to DPS data or hosted services.
User Access Revocation	IS-09	IS-09.1	Describe process for timely deprovisioning, revocation or modification of user access to the DPS data or hosted services upon any change in status of employees, contractors, customers, business partners or third parties?
User Access Reviews	IS-10	IS-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?
		IS-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?
Training / Awareness	IS-11	IS-11.1	Do you provide annually a formal security awareness training program for cloud-related access and data management issues for all persons with access to DPS or hosted services?
	IS-12	IS-12.2	Do you benchmark your security controls against industry standards?
Segregation of Duties	IS-15	IS-15.1	How do you maintain segregation of duties within your cloud service offering?
Encryption	IS-18	IS-18.1	Do you have a capability to allow creation of unique encryption keys per tenant?
		IS-18.2	Do you support tenant generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate. (e.g. Identity based encryption)?
Encryption	IS-19	IS-19.1	What encryption method and level of encryption is applied to DPS's data at rest and does it meet FIPS 140-2?
		IS-19.3	For DPS data in transport, what encryption level is applied and is the cryptographic module FIPS 140-2 ceritified.
		IS-19.4	Describe your key management procedures?
Encryption Key Management			
Vulnerability / Patch Management	IS-20	IS-21.1	Describe your patch management process?

Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Antivirus / Malicious Software	IS-21	IS-21.1	Do you have anti-malware programs installed on all systems which support DPS hosted services and data?
		IS-21.2	How do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components which support DPS's hosted services.
Incident Management	IS-22	IS-22.1	Do you have a documented security incident response plan
			Do you have processes for handling and rporting of security incidents that include preparation, detection, analysis, containment eradication, and recovery?
			What steps are taken to ensure all employees are made aware of the incident reporting procedures?
Incident Reporting	IS-23	IS-23.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?
Network Monitoring	IS-27	IS-27.1	List the tools used to monitor network events, detect attacks, and provide identification of unauthorized use.
Source Code Access Restriction	IS-33	IS-33.1	Describe the controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?
Utility Programs Access	IS-34	IS-34.1	How are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?
Release Management			
Production Changes	RM-02	RM-02.1	Do you have documented change management procedures?
Quality Testing	RM-03	RM-03.1	Do you provide your tenants with documentation which describes your quality assurance process?
Outsourced Development	RM-04	RM-04.1	Do you have controls in place to ensure that standards of quality are being met for all software development?
		RM-04.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?
Unauthorized Software Installations	RM-05	RM-05.1	What controls do you have in place to restrict and monitor the installation of unauthorized software onto your systems?

Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
Resiliency			
Business Continuity Testing	RS-01	RS-01.1	Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event?
	RS-04	RS-04.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?
Equipment Power Failures	RS-07	RS-07.1	How are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?
Security Architecture			
Customer Access Requirements	SA-01	SA-01.1	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?
User ID Credentials	SA-02	SA-02.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?
Password			Describe password requirements
Application Security	SA-04	SA-04.2	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?
Data Integrity	SA-05	SA-05.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?
Remote User Multifactor Authentication	SA-07	SA-07.1	Describe multi-factor authentication method required for all remote user access.
Segmentation	SA-09	SA-09.4	Are system and network environments logically separated to ensure protection and isolation of sensitive data?
Wireless Security	SA-10	SA-10.1	Are policies and procedures established and mechanisms implemented to protect network environment peremeter and configured to restrict unauthorized traffic?

Consensus Assessments Initiative Questionnaire

Control Group	CGID	CID	Consensus Assessment Questions
		SA-10.2	Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)
		SA-10.3	Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?
Clock Synchronization	SA-12	SA-12.1	Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?
Audit Logging / Intrusion Detection	SA-14	SA-14.1	What file integrity controls and network intrusion detection (IDS) tools are deployed to help facilitate timely detection, investigation by root cause analysis and response to incidents?
		SA-14.2	Is Physical and logical user access to audit logs restricted to authorized personnel?