Annex 5

Cloud Service Provider Assessment Questionnaire

Annex 5: Cloud Service Provider Assessment Questionnaire

No	Control Domain	Assessment	Answer	Reference
1.	Independent Audits	Do you allow customers to view your third party audit reports?		
		Do you conduct network penetration tests of your cloud service infrastructure regularly? If yes please elaborate on your test and remediation process.		
		Do you conduct regular application penetration tests of your cloud infrastructure according to the industry best practices? If yes please elaborate on your test and remediation process.		
		Do you conduct internal audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.		
		Do you conduct external audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.		
		Are the results of the network penetration tests available to customers at their request?		
		Are the results of internal and external audits available to customers at their request?		
2.	Third Party Audits	Do you permit customers to perform independent vulnerability assessments?		
3.	Contact/Authority Maintenance	Do you maintain updated liaisons and points of contact with local authorities? If yes then how frequently you validate the contacts?		
4.	Information System Regulatory Mapping	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single customer only, without inadvertently accessing another customer's data?		
		Do you have capability to logically segment, isolate and recover data for a specific customer in the case of a failure or data loss?		
5.	Intellectual Property	Do you have policies and procedures in place describing what controls you have in place to protect customer’s data marked as intellectual property?		

No	Control Domain	Assessment	Answer	Reference
		If utilization of customers services housed in the cloud is mined for cloud provider benefit, are the customers' defined IP rights preserved?		
		If utilization of customers services housed in the cloud is mined for cloud provider benefit, do you provide customers the ability to optout?		
6.	Ownership	Do you follow or support a structured data-labelling standard (ex. ISO 15489, Oasis XML Catalogue Specification, CSA data type guidance)? If yes please specify		
7.	Classification	Do you provide a capability to identify virtual machines via policy tags/metadata?		
		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags?		
		Do you have a capability to use system geographic location as an authentication factor?		
		Do you allow customers to define acceptable geographical locations for data routing or resource instantiation?		
8.	Handling / Labelling / Security Policy	Do you consider all customer data to be "highly sensitive "and provide the same protection and controls across the board or you apply the controls according to the data specific classification or label?		
		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data		
9.	Retention Policy	Do you have technical control capabilities to enforce customer data retention policies?		
		Do you have a documented procedure for responding to requests for customer data from governments or third parties?		
10.	Secure Disposal	Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the customer?		
		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of		

No	Control Domain	Assessment	Answer	Reference
		customer data once a customer has exited your environment or has vacated a resource?		
11.	Nonproduction Data	Do you have procedures in place to ensure production data shall not be replicated or used in your test environments?		
12.	Information Leakage	Do you have controls in place to prevent data leakage or intentional/accidental compromise between customers in a multi-customer environment?		
		Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?		
13.	Policy	Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?		
14.	User Access	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background checks?		
15.	Controlled Access Points	Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?		
16.	Secure Area Authorization	Do you allow customers to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?		
17.	Unauthorized Persons Entry	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?		
18.	Offsite Authorization	Do you provide customers with documentation that describes scenarios where data may be moved		

No	Control Domain	Assessment	Answer	Reference
		from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)		
19.	Offsite equipment	Do you provide customers with documentation describing your policies and procedures governing asset management and repurposing of equipment?		
20.	Asset Management	Do you maintain a complete inventory of all of your critical assets?		
21.	Employment Agreements	Do you specifically train your employees regarding their role vs. the customer's role in providing information security controls?		
		Do you document employee acknowledgment of training they have completed?		
22.	Employment Termination	Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?		
23.	Management Program	Do you provide customers with documentation describing your Information Security Management System (ISMS)?		
24.	Management Support / Involvement	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?		
25.	IS Policy	Do your information security and privacy policies align with particular standards (ISO27001, NIA, CoBIT, etc.)?		
		Do you have agreements which 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?		
26.	Baseline Requirements	Do you have documented information security baselines for every component of your infrastructure (ex.		

No	Control Domain	Assessment	Answer	Reference
		Hypervisors, operating systems, routers, DNS servers, etc.)?		
		Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?		
		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		
27.	Policy Reviews	Do you notify your customers when you make material changes to your information security and/or privacy policies?		
28.	Policy Enforcement	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?		
		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?		
29.	User Access Policy	Do you have controls in place ensuring timely removal of access rights and permissions which is no longer required?		
		Do you provide metrics which track the speed with which you are able to remove access rights following a request from us?		
30.	User Access Restriction / Authorization	Do you document how you grant and approve access to customer data?		
		Do you have a method of aligning provider and customer data classification methodologies for access control purposes?		
31.	User Access Revocation	Is timely de-provisioning, 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 third parties?		
32.	User Access Reviews	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your customers)?		

No	Control Domain	Assessment	Answer	Reference
		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?		
		Will you share user entitlement remediation and certification reports with your customers, if inappropriate access may have been allowed to customer data?		
33.	Training/ Awareness	Do you provide or make available a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to customer data?		
		Are administrators properly educated on their legal responsibilities with regard to security and data integrity?		
34.	Industry Knowledge/ Benchmarking	Do you participate in industry groups and professional associations related to information security?		
		Do you benchmark your security controls against industry standards?		
35.	Roles / Responsibilities	Do you provide customers with a role definition document clarifying your administrative responsibilities vs. those of the customer?		
36.	Management Oversight	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?		
37.	Segregation of Duties	Do you provide customers with documentation on how you maintain segregation of duties within your cloud service offering?		
38.	User Responsibility	Is your staff made aware of their responsibilities for maintaining awareness and compliance with our published security policies, procedures, standards and applicable regulatory requirements?		
		Are users made aware of their responsibilities for maintaining a safe and secure working environment?		

No	Control Domain	Assessment	Answer	Reference
		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?		
39.	Workspace	Do your data management policies and procedures address customer and service level security requirements?		
		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to customer data?		
		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?		
40.	Encryption	Do you have a capability to allow creation of unique encryption keys per customer?		
		Do you support customer generated encryption keys or permit customers to encrypt data to an identity without access to a public key certificate. (e.g. Identity based encryption)?		
41.	Encryption Key Management	Do you encrypt customer data at rest (on disk/storage) within your environment?		
		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?		
		Do you have a capability to manage encryption keys on behalf of customers?		
		Do you maintain key management procedures?		
42.	Vulnerability / Patch Management	Do you conduct network layer vulnerability scans regularly?		
		Do you conduct application layer vulnerability scans regularly?		
		Do you conduct local operating system-layer vulnerability scans regularly?		
		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?		

No	Control Domain	Assessment	Answer	Reference
		Will you provide your risk based systems patching timeframes to your customers upon request?		
43.	Antivirus / Malicious Software	Do you deploy multi antimalware engines in your infrastructure?		
		Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?		
44.	Incident Management	Do you have a documented security incident response plan?		
		Do you integrate customized customer requirements into your security incident response plans?		
		Do you have a CERT function (Computer Emergency Response Team)?		
		Do you publish a roles and responsibilities document specifying what you vs. your customers are responsible for during security incidents?		
45.	Incident Reporting	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?		
		Does your logging and monitoring framework allow isolation of an incident to specific customers?		
46.	Incident Response Legal Preparation	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?		
		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 customer without freezing other customer data?		
		Do you enforce and attest to customer data separation when producing data in response to legal subpoenas?		

No	Control Domain	Assessment	Answer	Reference
47.	Acceptable Use	Do you provide documentation regarding how you may utilize or access customer data and/or metadata?		
		Do you collect or create metadata about customer data usage through the use of inspection technologies (search engines, etc.)?		
		Do you allow customers to optout of having their data/metadata accessed via inspection technologies?		
48.	Asset Returns	Are systems in place to monitor for privacy breaches and notify customers expeditiously if a privacy event may have impacted their data?		
		Is your Privacy Policy aligned with industry standards and Sri Lankan's Law		
49.	e-Commerce Transactions	Do you provide standard encryption methodologies (3DES, AES, etc.) to customers in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)		
		Do you utilize standard encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?		
50.	Audit Tools Access	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)		
51.	Source Code Access Restriction	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?		
		Are controls in place to prevent unauthorized access to customer application, program or object source code, and assure it is restricted to authorized personnel only?		
52.	Nondisclosure Agreements	Are requirements for nondisclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational		

No	Control Domain	Assessment	Answer	Reference
		details identified, documented and reviewed at planned intervals?		
53.	Third Party Agreements	Can you provide a list of current 3rd party organization that will have access to the customer's (My) data?		
54.	Equipment Maintenance	If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery capabilities including offsite storage of backups?		
		If using virtual infrastructure, do you provide customers with a capability to restore a Virtual Machine to a previous state in time?		
		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		
		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?		
		Do you share reports on your backup/recovery exercise results?		
		Does your cloud solution include software / provider independent restore and recovery capabilities?		
55.	Assessments	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?		
		s the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?		
56.	Mitigation / Acceptance	Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?		
		Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?		

No	Control Domain	Assessment	Answer	Reference
57.	Business / Policy Change Impacts	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?		
58.	Third Party Access	Do you monitor service continuity with upstream internet providers in the event of provider failure?		
		Do you have more than one provider for each service you depend on?		
		Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?		
		Do you provide the customer the ability to declare a disaster?		
		Do you provide a customer triggered failover option?		
		Do you share your business continuity and redundancy plans with your customers?		
59.	New Development / Acquisition	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?		
60.	Production Changes	Do you provide customers with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?		
61.	Quality Testing	Do you have controls in place to ensure that standards of quality are being met for all software development?		
		Do you have controls in place to detect source code security defects for any outsourced software development activities?		
62.	Unauthorized Software Installations	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?		
63.	Impact Analysis	Do you provide customers with on-going visibility and reporting into your operational Service Level Agreement (SLA) performance?		

No	Control Domain	Assessment	Answer	Reference
		Do you provide customers with on-going visibility and reporting into your SLA performance?		
64.	Business Continuity Planning	Are you BS25999 or ISO 22301 certified?		
		Do you provide customers with geographically resilient hosting options?		
65.	Business Continuity Testing	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?		
66.	Environmental Risks	Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?		
67.	Equipment Power Failures	Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?		
68.	Power / Telecommunications	Do you provide customers with documentation showing the transport route of their data between your systems?		
		Can customers define how their data is transported and through which legal jurisdiction?		
69.	Customer Access Requirements	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?		
		Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a customer) if requested?		
		Do you provide customers with strong (multifactor) authentication options (digital certs, tokens, biometric, etc…) for user access?		
		Do you allow customers to use third party identity assurance services?		

No	Control Domain	Assessment	Answer	Reference
		Do you utilize an automated source-code analysis tool to detect code security defects prior to production?		
		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		
70.	Data Integrity	For your PaaS offering, do you provide customers with separate environments for production and test processes?		
		For your IaaS offering, do you provide customers with guidance on how to create suitable production and test environments?		
71.	Audit Logging / Intrusion Detection	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?		
		Is Physical and logical user access to audit logs restricted to authorized personnel?		
		Can you provide evidence that due diligence mapping of currently applicable regulations and standards to your controls/architecture/processes has been done?		