S. NO.	SECURITY POINTS	WEIGHTAGE	YES / NO
1	Hosting in India Data Center	1	
2	Allow customers to view your third party audit reports?	1	
3	Conduct network penetration tests of your cloud service infrastructure regularly? If yes please elaborate on your test and remediation process	1	
4	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.	1	
5	Permit customers to perform independent vulnerability assessments?	1	
6	Policies and procedures in place describing what controls you have in place to protect customer's data marked as intellectual property?	1	
7	Provide the physical location/geography of storage of a customer's data upon request?	1	
8	Technical control capabilities to enforce customer data retention policies?	1	
9	Documented procedure for responding to requests for customer data from governments or third parties?	1	
10	Support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the customer?	1	
11	Provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of customer data once a customer has exited your environment or has vacated a resource?	1	
12	Procedures in place to ensure production data shall not be replicated or used in your test environments?	1	
13	Controls in place to prevent data leakage or intentional/accidental compromise between customers in a multi-customer environment?	1	
14	Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?	1	
15	Provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	1	
16	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background checks?	1	
17	Do you provide customers with documentation describing your Information Security Management System (ISMS)?	1	
18	Provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	1	
19	Documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?	1	
20	Controls in place ensuring timely removal of access rights and permissions which is no longer required?	1	
21	Conduct network- layer vulnerability scans regularly?	1	
22	Capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	1	
23	Incident response capability include the use of legally admissible forensic data collection and analysis techniques?	1	
24	Are systems in place to monitor for privacy breaches and notify customers expeditiously if a privacy event may have impacted their data?	1	
25	Do you ensure hardening of admin workstations and Role Based Access Control to enforce the 'least privilege' principle	1	
26	Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?	1	
27	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	1	
28	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?	1	
29	Do you have controls in place to ensure that standards of quality are being met for all software development?	1	
30	Controls in place to restrict and monitor the installation of unauthorized software onto your systems?	1	
31	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	1	
32	Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and counter measures applied?	1	
33	Do you provide customers with strong (multifactor) authentication options (digital certs, tokens, biometric, etc...) for user access?	1	

34	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	0.5	
35	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.)	0.5	
36	Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations?	0.5	
37	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?	0.5	
38	Is mobile code tested (in terms of security) before its installation and use and the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy?	0.5	
39	Cloud provider should offer fine- grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device.	0.5	
40	Cloud service should support multi- factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.	0.5	
41	Cloud service should support reporting a user’s access keys last use details.	0.5	
42	Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production.	0.5	
43	Cloud service should support a policy validator to automatically examine non-compliant access control policies.	0.5	
44	Cloud provider should support setting up a stand-alone directory in the cloud or connecting cloud resources with existing on- premises Microsoft Active Directory.	0.5	
45	Cloud service should support features such as user and group management.	0.5	
46	Cloud service should integrate with existing on-premise Active Directory.	0.5	
47	Cloud service should allow users to reset their password in a self- service manner.	0.5	
48	Cloud provider should offer a service to create and control the encryption keys used to encrypt user data.	0.5	
49	Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.	0.5	
50	Cloud service should support durability of keys, including storing multiple copies to ensure keys are available when needed.	0.5	
51	Cloud provider should offer a service to record history of API calls and related events for a user account.	0.5	
52	Cloud service should support notifications when new log files are available.	0.5	
53	Cloud service should support storing log files in a durable and inexpensive storage solution.	0.5	
54	Cloud service should support a variety of 3rd solutions.	0.5	
55	Cloud service should deliver API activity history within a Reasonable timeframe (<30 minutes) from the time API call is made.	0.5	
56	Cloud service should support receiving log files from multiple regions and accounts to a single location for ease of use.	0.5	
57	Cloud provider should offer a service that provides resource inventory, configuration history, and configuration change notifications to enable security and governance.	0.5	
58	Cloud service should automatically record a resource Configuration when it changes and make this information available.	0.5	
59	Customer should be able to obtain details of what a resource’s configuration looked like at any point in the past using this cloud service.	0.5	
60	Cloud service should notify every configuration change so customers can process these notifications programmatically.	0.5	
61	Cloud provider should offer the ability to create and manage catalogues of IT services that are approved for use.	0.5	
62	Cloud provider should offer a dashboard that displays up- to-the- minute information on service availability across multiple regions.	0.5	
63	Cloud provider should offer 365 days’ worth of Service Health Dashboard (SHD) history.	0.5	
64	Cloud provider should offer a service acts like a customized cloud expert and helps provision resources by following best practices.	0.5	

65	Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health.	0.5	
66	Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines. Ability to choose from a set of pre- built rules based on common best practices or custom rules (e.g., ensure Storage volumes are encrypted, Compute instances are properly tagged, and Public IP addresses are attached to instances) and continuously monitor configuration changes to the cloud resources and provides a new dashboard to track compliance status.	0.5	
67	Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing	0.5	
	Total	50	