भारत का प्रधान कौंसलावास, जांजीबार
CONSULATE GENERAL OF INDIA
8, MIGOMBANI, P.O.BOX 871
ZANZIBAR (TANZANIA)

No. ZAN/551/01/2021

May 09, 2023

Subject: Proposal for re-designing, VPC web hosting and maintaining of the website of the Consulate General of India, Zanzibar.

The Consulate General of India, Zanzibar invites quotation for re-designing, VPC web hosting and maintaining of its website www.cgizanzibar.gov.in as per STQ Certification (www.stqc.gov.in) and MEA (www.mea.gov.in) design with SSL Certificate. The website is to be hosted to a Virtual Private Cloud (VPC) with data centre in India as per Ministry of External Affairs (MEA) guidelines.

Reputed firms having experience in developing/designing website of Indian Embassy/Consulate abroad and Government websites may send their proposal along with supporting documents to the Consul General, Consulate General of India, 8, Migombani, Zanzibar (hoc.zanzibar@mea.gov.in) by 1500 hours (IST) on 31.05.2023.

The Consulate reserves the right to accept or reject any proposal without assigning reason (s).

Kumar Praveen

(Dr. Kumar Praveen)
Consul General

Email: cg.zanzibar@mea.gov.in
Email: hoc.zanzibar@mea.gov.in
Website: www.cgizanzibar.gov.in
Tel No's: +255 24 2232711, 2230720, 2231904
Fax No: +255 24 2230001

सत्यमेव जयते

Consulate General of India
Zanzibar

No. ZAN/551/01/2021

May 09, 2023

Subject: Proposal for re-designing, VPC web hosting and maintaining of the website of the Consulate General of India, Zanzibar.

1.0 OBJECTIVE

1.1 To re-design/develop multi-lingual website as per STQ Certification and MEA design with SSL Certificate, maintain and host to a Virtual Private Cloud (VPC) infrastructure **with data centre in India for dedicated hosting**.

2.0 GENERAL

2.1 The Bidder shall necessarily be a legally valid entity and in existence for a minimum period of 3 years in the business as on the date of tendering, satisfying the following conditions:-

a) It should be able to provide a qualified web designing, building and maintenance team, for undertaking the same assignment.

b) A confirmation letter from the Agency for being able to provide the qualified team should be attached. Details of the team dedicated to the Consulate General of India, Zanzibar should be provided and their skills/ certification should be submitted.

c) An undertaking (self-certificate) will have to be given by the Agency that it has never been blacklisted by a Central/ State Government institutions or Missions/ Posts abroad.

d) There should not be any litigation with any government department on account of IT services at the time of bidding.

2.2 Company/ firm must be a registered company and legally valid entity. It should fulfill following requirements and submit supported documents in this regard:-

a) Past experience in creating and maintaining very professionally and exceptionally creative websites.

b) Excellent IT skills and project management skills.

c) Ability to respond quickly to the maintenance requirement in the post-commissioning phase.

d) Awareness and use of the latest smart technologies for website development.

e) Ability to regularly maintain and update the developed website.

f) Employees with security certification in website design, development and auditing.

g) Employees with proficiency and certification in secure hosting and management of hosting platform.

h) Website development, audit and security tools/software used by the Firm/ Company.

2.3 It is expected that the bidder who wish to bid for the tender have highest standards of ethics. The Consulate shall reject a bid if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices while competing for this contract. The Consulate may declare a bidder ineligible, either indefinitely or for a stated duration, if it at any time, determine that the bidder has engaged in corrupt and fraudulent practices during the execution of contract.

2.4 The Consulate General of India, Zanzibar reserves the right to accept or reject any proposal without assigning reason(s).

3.0 SCOPE OF WORK

The Service Provider shall:

3.1 Re-design/develop in Laravel Framework, mobile optimised, maintain and host the Consulate's website on Virtual Private Cloud (VPC) infrastructure with data centre in India for dedicated hosting. The website should multi-lingual and as per STQ Certification and MEA design.

3.2 Incorporate the Secure Socket Layer (SSL) Certificate in the website. The website shall not be hosted and made live without SSL Certificate.

3.3 Not host the website in any shared server hosting platform. In no case website hosting space is to be shared with other websites of private entities or any websites of Government organisations/ agencies. The website must have a dedicated IP Address with a minimum web server specifications of 2GB RAM, 20 GB storage capacity, etc.

3.4 Allot the default capacity/ space of 20 Gigabytes [GB]; Hosting Environment-Linux; Cloud Type-Block Level Dynamic; on Virtual Private Cloud Server which can be further up-scaled or customised as per the Consulate website's data requirement.

3.5 Maintain the website in a database driven/ modular so that it can store & handle all the information and be able to handle the documents that would get uploaded on it on a regular basis. There should be periodic full backup (Code

4/21

along with the data) of website during the contract period. The custodian of entire backup should be the Consulate General of India, Zanzibar, including Source Code of the website.

3.6 Be responsible for provisioning of underlying system software, software licenses, infrastructure, bandwidth and Cloud Services for deployment and hosting of applications which includes hardware requirements (No. of CPU, Cores, No. of machines, RAM per machine and HDD). In no case will the Consulate pay for or procure additional system/ software licences.

3.7 Provision for compute, storage and bandwidth requirements which may be auto-scaled (additional capacity base on the demand and auto scaling rules) over the period of contract in line with the transaction load to meet the requirements.

3.8 Provision for Cloud services which posses Anti Distributed Denial of Services (DDoS) feature.

3.9 Provide Non-Disclosure Agreement (NDA).

3.10 Comply with all 109 requirements as mentioned in **Annexure-I**.

3.11 Undertake measures to strengthen the security of the Consulate's website from issues related to website vulnerabilities. Security guidelines available on the CERT-In website (www.cert-in.org.in) shall be referred and strictly complied, with regard to the following:-

a) Web Server Security Guidelines;
b) Guidelines for Auditing and Logging (list of empanelled auditors is also available at https://www.cert-in.org.in/PDF/Epanel.org.pdf;
c) To ensure that website comply with the "Guidelines for Indian Government Websites (GIGW)" http://guidelines.gov.in/.

3.12 Adhered to the following points related to database management:-

a) Database-requires periodic bug fixing, troubleshooting and the periodic update of searchable data;
b) Maintain Site search engine by ensuring any content updates and new pages are searchable;
c) Advanced search option to be incorporated;
d) Automated reconciliation and generation of necessary reports etc.;
e) Logs of database access need to be maintained.

3.13 Complied to the following security measures:-

a) To perform complete regular repairs as needed to scripting languages, basic HTML, broken images, broken links and all other malfunctioning code or components;

b) To provide a report on site traffic statistics and search engine analysis reports on monthly basis or as and when required including updated reports to the Consulate about number of visitors, geographical distribution of visitors, average time spent on the website, most visited sections/pages etc. besides other analysis;

c) To conduct regular audit of the website at their level to ensure website Source Code is free from any potential vulnerability;

d) The website framework to be kept as per desired security standard. In this regard necessary security path management and security update to be carried out on regular basis.

3.14 Re-design/develop, host and maintain website which will have:

a) Web 2.0 and web usability;

b) more informative about Mission and its services such as Visa, Passport, PIO and other Consular Services;

c) information about tourism, education and healthcare facilities in India;

d) information about India's history, politics, economics, foreign policies, bilateral relations between India and Tanzania;

e) facility to add / modify / delete content;

f) facility to upload pictures, documents, audio and video formats;

g) search facilities within website;

h) complete administrative control to manage users with flexible access and activity controls;

i) facility to modify fonts, colours, size and layout pages;

j) facility to have events (past and forthcoming events) with prior approval upon needed;

k) e-newsletter and bulk e-mail blasting;

l) facility to register online for public to get information about events and programmes of Mission;

m) facility to update social media.

3.15 Regularly monitor the website with 24x7 monitoring tools and intrusion detection system facility.

3.16 Deploy adequate manpower to meet 24x7 support to the Consulate. Provide Warranty, Maintenance and Technical Support for the period of contract for all matters related to website management, website security and website hosting.

4.0 SERVICE FEES & PAYMENT TERMS

4.1 Service Provider shall receive from the Consulate annual payment for the said services from the Consulate **after** the end of every contract year.

4.2 The payment shall be made within 30 days of receipt of invoice submitted by the service provider for the concerned service period.

5.0 TERMS & CONDITIONS:

5.1 Service Provider shall insure to the fullest extent possible, that the Consulate General of India, Zanzibar shall own any & all rights, titles & interest, including copyrights, trademarks, trade secrets, patent & other intellectual property rights, over works created by the Service Provider.

5.2 The contract, if awarded, shall be valid for a period of **three (03) years** from the date of award, however, subject to satisfactory performance and technical/ security compliance which will be reviewed on annual basis.

5.3 In case of breach of contract or in the event of not fulfilling the minimum requirements, the Consulate shall have the right to terminate the contract with immediate effect in addition to initiating administrative actions for blacklisting, etc. solely at the discretion of the Competent Authority of the Consulate.

6.0 TERMINATION

6.1 The Consulate reserves the right to terminate the contract at any time by giving sixty (60) days advance notice. However, the Consulate shall also have the right to terminate the Contract by giving a lesser period of Notice under special circumstances, such as security considerations, violation of privacy laws, compromise of personal information, etc., for premature termination of Contract. The Service Provider may terminate the contract by giving sixty (60) days advance notice with justification for termination of services.

6.2 The Consulate reserves the right to impose a financial penalty in Indian Rupee equivalent to the service charges for one year, in case the latter terminates the contract without providing sixty (60) days termination notice.

6.3 On termination of contract agreement, the Service Provider agrees that any Web Development or idea prepared by Service Provider and submitted to the Consulate (whether submitted separately or in confirmation with or as a part of other material) shall remain as the property of the Consulate. The Service Provider will hand over all the credentials, source codes and associated data, if any, with an undertaking that the Service Provider is not retaining any data in any form and credentials related to the Consulate.

7.0 FORCE MAJURE:

7.1 The parties shall not be responsible or liable for any kind of loss whatsoever sustained by any of the parties by the extraordinary event beyond the control of the parties, such as flood, war, riots, act of God and other natural calamities

which prevents one of the parties for fulfilling obligations rising out of the instant Agreement.

8.0 ARBITRATION

8.1 Neither Party, either in this agreement, or in any act related to the agreement, shall act unjustifiably or arbitrary to injure particular persons or entities or particular categories of persons or entities.

8.2 Both parties shall act in a non-arbitrary and reasonable manner with respect to the integrity of this agreement.

8.3 Any dispute, difference or question which may arise at any time hereafter between the parties relating to the true construction of this agreement or the rights and liabilities of the parties, which is not solved amicably between the parties within 30 (thirty) days, that dispute, difference or question arising shall, in the absence of agreement to the contrary between the parties, be referred to arbitration.

9.0 JURISDICTION

9.1 This Agreement shall be governed by, and construed in accordance with, Indian law in the territory 'New Delhi' only.

10.0 SIGN AND SEAL

10.1 The Bidder must sign and affix his seal on every page of the Tender Document and the complete Signed Tender Document must be submitted along with the bid to the Consulate.

8/21

No. ZAN/551/01/2021 May 09, 2023

TECHNICAL DETAILS TO BE PROVIDED BY THE FIRM

1	Letter of Proposal submission	*.pdf
2	Name, address, telephone number and e-mail of the firm	*.pdf
3	Name of responsible person for this project with mobile number and e-mail	*.pdf
4	Certificate of incorporation / Registration	*.pdf
5	Proof of Annual Turn Over of last three years (certified by Chartered Accountant)	*.pdf
6	Copies of Income Tax Return of last 3 years	*.pdf
7	Certificate from any Government body that the agency has resources having domain knowledge in Web Development Governance applications. Agency needs to have documentary proof of Guidelines for Indian Government Websites (GIGW) Compliance expertise.	*.pdf
8	Previous experience for similar work (Please attaché copy of award of work from 3 different clients)	*.pdf

Signature of authorized signatory.....
Name.....
Company Seal & Date.....

9/21

To,
The Consul General
Consulate General of India
Zanzibar, Tanzania

Subject: Proposal for re-designing/developing, VPC web hosting and maintaining of the website of the Consulate General of India, Zanzibar.

Sir,

1. We, the undersigned vendor, having read and examined in detail the Specifications and all the documents do propose to provide the services as specified in the document No. ZAN/551/01/2021 dated 09.05.2023. We shall comply with all the 109 requirements mentioned in Annexure-I of this said document.

2. All the prices mentioned in our proposal are in accordance with the terms as specified in the documents.

3. All the prices and other terms and conditions of this proposal are valid for a period of 120 calendar days from the date of submission of proposal.

4. We, do hereby confirm that our prices include all taxes, levies etc.

5. We have carefully read and understood the terms and conditions of the proposal and we do hereby undertake services as per these terms and conditions.

6. We do hereby undertake that, in the event of acceptance of our proposal, the services shall be completed as stipulated in the proposal.

Signature of authorized signatory.....
Name.....
Company Seal & Date.....

10/21

No. ZAN/551/01/2021

May 09, 2023

Subject: Financial Proposal for re-designing/developing, VPC web hosting and maintaining of the website of the Consulate General of India, Zanzibar.

Sl No.	Description	Annual Cost (`)
1	Re-designing/developing of website of Consulate as dynamic and responsive website as per SQT Certification and MEA design and technical maintenance of website, with SSL certificate	
2	Hosting of Website to Virtual Private Cloud Infrastructure with data centre in India	
3	Maintenance charges, Technical Support 24 x 7 Support	
	Total	

Total in words: .....

.....

Note:

1. The Financial Bid shall not include any conditions attached to it and any such conditional financial proposal shall be rejected summarily.

2. All prices should be quoted in Indian Rupees and indicated both in figures and words. Figures in words will prevail.

3. The cost should include all travel costs, shipping/mail, telephone/fax charges and agency administrative costs that may be incurred by the agency as part of this contract.

Signature of authorized signatory.....
Name.....
Company Seal & Date.....

Annexure - I

Category	Sl. No.	Requirement	Description
Regulatory	1	Data center locations should be in India	Cloud provider should offer cloud services from within India.
Regulatory	2	Maintain and ensure data locality	Cloud provider should ensure that customer data resides only in the Region they specify.
Regulatory	3	Protect your applications from the failure of a single location	Cloud provider should offer data centers engineered to be isolated from failures in other data centers, and to provide inexpensive, lowlatency network connectivity to other data centers in the same region.
Computer	4	Compute instances – Burstable performance	Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.
Computer	5	Compute instances – Dedicated	Cloud provider should offer instances that run on hardware dedicated to a single customer.
Computer	6	Resize virtual cores, memory, storage seamlessly	Customer must be able to specify and modify server configuration (CPU, memory, storage) parameters seamlessly and without outage.
Computer	7	Local disk/Instance store	Cloud service should support local storage for compute instances to be used for temporary storage of information that changes frequently.
Computer	8	Provision multiple concurrent instances	Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.
Computer	9	Auto Scaling support	Cloud service should be able to automatically increase the number of instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
Computer	10	Bring your own image/Instance Import	Customer should be able to import their existing image and save it as a new, privately available image that can then be used to provision instances in the

12/21

			future.
Computer	11	Export Instance Image	Cloud service must support the ability to take an existing running instance or a copy of an instance and export the instance into a VMDK or VHD image format.
Computer	12	Instance failure recovery	Cloud service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails.
Computer	13	Instance restart flexibility	Cloud provider must be able to schedule events for customer's instances, such as a reboot, stop/start, or retirement. Depending on the event, customer might be able to take action to control the timing of the event.
Computer	14	Support for Docker containers	Cloud service should support containers, including Docker and/or other containerization platforms.
Computer	15	Highly scalable, high performance container management service	Cloud provider should offer a highly scalable, high performance container management service.
Computer	16	Event-driven computing that runs code in response to events	Cloud service should be able to run customer code in response to events and automatically manage the compute resources.
Computer	17	Pay-as-you-go pricing	Cloud provider should offer a simple pay-as-you-go pricing where customers can pay for compute capacity by the hour with no longterm commitments.
Networking	18	Multiple network interface/instance	Cloud service should be able to support multiple (primary and additional) network interfaces.
Networking	19	Multiple IP addresses/instance	Cloud service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network interface.
Networking	20	Ability to move network interfaces	Cloud service should support the ability to create a network interface, attach it

		and IPs between instances	to an instance, detach it from an instance, and attach it to another instance.
Networking	21	Network traffic logging - Log traffic flows at network interfaces	Cloud service should support capturing information about the IP traffic going to and from network interfaces.
Networking	22	Auto-assigned public IP addresses	Cloud service should be able to automatically assign a public IP to the instances.
Networking	23	IP Protocol support	Cloud service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols.
Networking	24	Static public IP addresses	Cloud provider must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.
Networking	25	Subnets within private network	Customer should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block.
Networking	26	Subnet level filtering (Network ACLs)	Cloud service should support subnet level filtering – Network ACLs that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
Networking	27	Ingress filtering	Cloud service should support adding or removing rules applicable to inbound traffic (ingress) to instances.
Networking	28	Egress filtering	Cloud service should support adding or removing rules applicable to outbound traffic (egress) originating from instances.
Networking	29	Disable source/destination checks on interfaces	Cloud service should support the ability to disable source/destination check on network interfaces. By default, compute instances perform source/destination checks.
Networking	30	Configure proxy server (NAT instance) at network level	Cloud service should support NAT instances that can route traffic from internal-only instances to the Internet.
Networking	31	Multiple VPN	Cloud service should support creating

		Connections per Virtual Network	multiple VPN connections per virtual network.
Networking	32	DNS based global load balancing	Cloud service should support Load balancing of instances across multiple host servers.
Networking	32	DNS based global load balancing	
Networking	33	Load balancing supports multiple routing methods	Cloud service should support multiple routing mechanism including round-robin, failover, sticky session etc.
Networking	34	Front-end Load Balancer	Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.
Networking	35	Back-end Load Balancer	Cloud service should support an internal load balancer that routes traffic to instances within private subnets.
Networking	36	Health checks - monitor the health and performance of application	Cloud service should support health checks to monitor the health and performance of resources.
Networking	37	Integration with Load Balancer	Cloud service should support integration with load balancer.
Networking	38	Low Latency	The CSP should be able to provide a 10GB network connectivity between the servers if required.
Storage – Block Storage	39	Support for storage allocated as local disk to a single VM	Cloud provider should offer persistent block level storage volumes for use with compute instances.
Storage – Block Storage	40	Storage volumes > 1 TB	Cloud provider should offer block storage volumes greater than 1 TB in size.
Storage – Block Storage	41	SSD backed storage media	Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies.
Storage – Block Storage	42	Provisioned I/O support	Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
Storage –	43	Encryption using	Cloud service should support

Block Storage		provider managed keys	encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
Storage – Block Storage	44	Encryption using customer managed keys	Cloud service should support encryption using customer managed keys.
Storage – Block Storage	45	Durable snapshots	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.
Storage – Block Storage	46	Ability to easily share snapshots globally	Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data center migration, and disaster recovery.
Storage – Block Storage	47	Attach more than one compute instance to a single volume	Cloud service should support adding more than one compute instance to a single storage volume in R/W mode so that many users can access and share a common data source.
Storage – Block Storage	48	Consistent Input Output per second (IOPS)	Cloud service should support a baseline IOPS/GB and maintain it consistently at scale.
Storage – Block Storage	49	Annual Failure Rates <1%	Cloud service should be durable and support annual failure rates of less than 1%
Storage – File Storage	50	Simple, scalable file storage service	Cloud provider should offer a simple scalable file storage service to use with compute instances in the cloud.
Storage – File Storage	51	SSD backed storage media	Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads.
Storage – File Storage	52	Grow file systems to petabyte scale	Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections.
Storage – File Storage	53	Consistent low latency performance (T50-T99)	Cloud service should support consistent low latency performance between 5-15 ms at any scale.
Storage – File Storage	54	Scalable IOPS and throughput performance (/TB)	Cloud service should support scalable IOPS and throughput performance at any scale.
Storage – File Storage	55	Sharable across thousands of instances	Cloud service should support thousands of instances so that many users can access and share a common

			data source.
Storage – File Storage	56	Fully elastic capacity (no need to provision)	Cloud service should automatically scale up or down as files are added or removed without disrupting applications.
Storage – File Storage	57	Highly durable	Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple data centers.
Storage – File Storage	58	Read-after-write consistency	Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).
Relational Database	59	Managed relational database service	Cloud provider should offer a service that makes it easy to set up, operate, and scale a relational database in the cloud.
Relational Database	60	Support for MySQL	Cloud service should support the last two major releases of MySQL (versions 5.6, 5.5) as a database engine.
Relational Database	61	Support for Oracle	Cloud service should support the last two major releases of Oracle (11g and 12c) as a database engine.
Relational Database	62	Support for Microsoft SQL Server	Cloud service should support all the editions (Express, Web, Standard, Enterprise) of SQL Server 2012 as a database engine.
Relational Database	63	Support for PostgreSQL	Cloud service should support the last two major releases of PostgreSQL (9.4.x, 9.3.x)
Relational Database	64	Low latency, synchronous replication across multiple data centers in a region	Cloud service should support synchronous replication of a primary database to a standby replica in a separate physical datacenter to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
Relational Database	65	Read Replica support	Cloud service should support read replicas that make it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads.
Relational Database	66	Manual Failover	Cloud service should support a manual failover of the DB instance from primary to a standby replica.

Relational Database	67	Provisioned IO support	Cloud service should support the needs of database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
Relational Database	68	Bring your own SQL, Oracle licenses	Cloud service should support customers who prefer to use their existing Oracle and SQL Server database licenses in the cloud.
Relational Database	69	Cross region Snapshots	Cloud service should support copying snapshots of any size between different cloud provider regions for disaster recovery purposes.
Relational Database	70	Cross region Read Replica	Cloud service should support creating multiple in-region and cross region replicas per database instance for scalability or disaster recovery purposes.
Relational Database	71	High Availability	Cloud Service should support enhanced availability and durability for database instances for production workloads.
Relational Database	72	Point in time restore	Cloud service should support restoring a DB instance to a specific date and time.
Relational Database	73	User snapshots and restore	Cloud service should support creating a DB snapshot and restoring a DB instance from a snapshot.
Relational Database	74	Modifiable DB parameters	Cloud service should allow the DB parameter to be modified.
Relational Database	75	Monitoring	Cloud service should allow monitoring of performance and health of a database or a DB instance.
Relational Database	76	Encryption at rest	Cloud service should support encryption using the industry standard AES-256 encryption algorithm to encrypt data.
Security and administration	77	Control access to your cloud resources at a granular level	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.
Security and administration	78	Utilize multi-factor	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.
Security and administration	78	authentication when accessing cloud resources	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.
Security and administration	79	Identify when an access key was last used to rotate old keys and remove inactive users	Cloud service should support reporting a user's access keys last use details.
Security and administration	80	Policy Simulator to test policies	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.
Security and administration	80	before committing to production	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.
Security and administration	81	Policy validation to ensure policies match intentions	Cloud service should support a policy validator to automatically examine non-compliant access control policies.
Security and administration	82	Directory as a service	Cloud provider should support setting up a stand-alone directory in the cloud or connecting cloud resources with existing on-premises Microsoft Active Directory.
Security and administration	83	User and Group management	Cloud service should support features such as user and group management.
Security and administration	84	Managed service to create and control the encryption keys used to encrypt your data	Cloud provider should offer a service to create and control the encryption keys used to encrypt user data.
Security and administration	85	Audit of all action on keys	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.

Security and administration	86	Key Durability	Cloud service should support durability of keys, including storing multiple copies to ensure keys are available when needed.
Security and administration	87	Durable and inexpensive log file storage	Cloud service should support storing log files in a durable and inexpensive storage solution.
Security and administration	88	Choice of partner solution	Cloud service should support a variety of 3rd party solutions.
Security and administration	89	Automatically records a resource's configuration when it changes	Cloud service should automatically record a resource configuration when it changes and make this information available.
Security and administration	90	Examine the configuration of your resources at any single point in the past	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.
Security and administration	91	Receive notification of a configuration change	Cloud service should notify every configuration change so customers can process these notifications programmatically.
Security and administration	92	Create and manage catalog of pre-approved services for use	Cloud provider should offer the ability to create and manage catalogs of IT services that are approved for use.
Deployment and Management	93	Service to quickly deploy and manage applications in the cloud	Cloud provider should offer a service to quickly deploy and manage applications in the cloud by automatically handling the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.
Deployment and Management	94	Supported OS	Cloud Service should support Windows, Linux, and Docker containers.
Deployment and Management	95	Deployment Mechanism	Cloud service should support various deployment mechanisms, including a Git repository, or an integrated development environment (IDE) such as Eclipse or Visual Studio.
Deployment and Management	96	Support for SSL connections	Cloud service should support SSL connections.
Deployment	97	Auto scaling	Cloud service should support

and Management			automatically launching or terminating instances based on the parameters such as CPU utilization defined by users.
Deployment and Management	98	Swap virtual IP between staging and production environments	Cloud service should support swapping IP addresses between staging and production environments so that a new application version can be deployed with zero downtime.
Deployment and Management	99	Integration with caching solution	Cloud service should be integrated with a caching solution such as Redis cache.
Deployment and Management	100	Service to create a collection of related resources and provision them using a template	Cloud provider should offer a service to create a collection of related resources and provision them in an orderly and predictable fashion using a template.
Deployment and Management	101	Single JSON based template to declare your stack	Cloud service should use a template, a JSON-format, text-based file that describes all the resources required for an application. The resources in the template should be managed as a single unit.
Deployment and Management	102	Allow parametrization and specific configurations	Cloud service should support parameterization for specific configuration.
Deployment and Management	103	Integration with the portal	Cloud service should be integrated with the portal.
Support	104	Service Health Dashboard	Cloud provider should offer a dashboard that displays up-to-theminute information on service availability across multiple regions.
Support	105	365 day service health dashboard and SLA history	Cloud provider should offer 365 days' worth of Service Health Dashboard (SHD) history.
Support	106	Service to compare resource usage to best practices	Cloud provider should offer a service acts like a customized cloud expert and helps provision resources by following best practices.
Support	107	Monitoring Tools	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.
Support	108	Governance and Compliance	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 Elastic IP addresses (EIPs) are attached to instances) and continuously monitor configuration changes to the cloud resources and provides a new dashboard to track compliance status.
Support	109	Audit Trail	Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing