

**EMBASSY OF INDIA
DOHA**

**REQUEST FOR PROPOSAL FOR MAINTENANCE OF
THE WEBSITE OF THE EMBASSY OF INDIA, DOHA**

No. EoI Doha/ Website/ RFP/2017

Dated 17 May, 2017

1. Introduction

1.1. The website of the Embassy of India, Doha (hereinafter referred to as “Embassy”) can be accessed at www.indianembassyqatar.gov.in. The website provides a vast amount of information through various sections/ web pages. The website provides latest updates for the benefit of the Indian community in Qatar. In addition, it has pertinent information about various consular services rendered by the Embassy. The site also provides information related to RTI and Press Releases, Announcements, Advisories etc. The Embassy intends to avail the services of firms/ agencies having experience in developing and maintaining websites.

1.2. This RFP is being issued with no financial commitment and the Embassy reserves the right to change or vary any part thereof of the RFP at any stage. The Embassy also reserves the right to withdraw the RFP, should it become necessary at any stage.

1.3. The Embassy’s decision on the pre-qualification of the agencies and selection of the website manager shall be firm and final. No further queries will be entertained in this regard.

1.4. The objectives of the RFP are:

- Redesign and upgradation of the existing website of the Embassy as a dynamic and responsive website
- Hosting the website
- HTTPS/ SSL for the hosting of the website
- Security auditing
- Providing Virtual Private Cloud Infrastructure for the Mission’s website
- Indian citizen registration and communication facilities
- Publishing Embassy e-Newsletters as required
- 24 X 7 website content updates
- Search engine optimizing
- Multilingual websites (Subject to Embassy needs)
- Helping Manage the Embassy’s Social Media handles & updates

2 Scope of Work. The primary focus of the website is to provide clear and easily understandable information to citizens of India and foreigners about the Embassy’s services. Broadly the scope of work includes:

- (a) *Redesign and Upgradation of the website as per MEA and NIC website guidelines, to make it a responsive website*
- (b) *Website to be hosted by the vendor with hack-proof server*
- (c) *Redesign Content Management System of the website for contents like visa information, Passport , Press releases, galleries, events , live feeds, social media contents, if any and periodic archiving of the old contents automatically, etc.*
- (d) *Providing 24 X 7 unlimited update of the content with Embassy officials for all the tasks related to the website design and maintenance and updates respectively.*
- (e) *Agency would be required to provide Warranty, Maintenance, and Technical Support from the date of issue of completion certificate, and Annual maintenance of website/ application with onsite technical support as required.*
- (f) *Ensure that the website is security audited by a CERT-IN empanelled agency or STQC or MEA referring security auditing companies.*
- (g) Undertake measures to strengthen the security of the Mission 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:-
 - (i) Web Server Security Guidelines
 - (ii) Guidelines for Auditing and Logging (list of empanelled auditors is also available at <https://www.cert-in.org.in/PDF/Epanel.org.pdf>)
- (h) *Identify and execute training requirements for successful execution of project along with preparation of User Manual.*
- (i) *Creation of manuals and documents for the project executed.*
- (j) *Social Media updates such as Facebook/Twitter, YouTube and other Embassy required Social Media updates*
- (k) *To ensure that website comply with the “Guidelines for Indian Government Websites (GIGW)” <http://guidelines.gov.in/>*
- (l) *To migrate Missions website on **Virtual Private Cloud infrastructure** for dedicated hosting. Detailed instructions/ scope of work on this issue are covered under Annexure VIII.*
- (m) *To assist the Embassy in bringing out its e-Newsletters on a regular basis.*

2.1 Detailed Scope of Work

This section provides indicative scope of work for vendors. However, the work listed below is only indicative and can vary depending upon actual requirements of the Embassy.

2.1.1 Redevelopment and Maintenance of Customized Web-Based application/portal solutions/ Web designing:

- (a) *Redevelop the website for contents like visa information, Passport, Press releases, galleries, events , live feeds, social media contents, if any and periodic archiving the old contents automatically, etc.*
- (b) *Multilingual website (English, Hindi and Arabic)*
- (c) *Study and analysis of existing /similar websites and include best practices in draft design.*
- (d) *Coordination and collection of required content for website updates.*
- (e) *Design should comply with all parameters with guidelines issued by Government of India for websites.*
- (f) *Comply with website security guidelines issued by NIC, GOI.*
- (g) *The website should have features like an event calendar which would be updated from time to time.*
- (h) *The page download response should be quick and fast.*
- (i) *The website should be 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.*
- (j) *Develop an application through which the Embassy is able to upload contents remotely. Approval rights will be with the Embassy.*
- (k) *In the CMS, provide front-end user interface/ network login details that allows a user, even with limited expertise, to add, modify and remove content from a website.*

2.1.2 Website Maintenance

- (a) *Upgrade/update content and structure of current Embassy's website.*
- (b) *Update Content on the website on a regular basis, as provided by the Embassy.*
- (c) *Develop banners/images/info graphics/flyers or any other graphics as may be needed from time to time.*

- (d) *Manage and maintain all Embassy's domains, including hosting facility with secure server.*
- (e) *Regular monitoring of the website with 24 X 7 monitoring tools and intrusion detection system facility*
- (f) *Complete regular repairs as needed to scripting languages, basic HTML, broken images, broken links and all other malfunctioning code or components.*
- (g) *Periodic full backup of website through the duration of the contract.*
- (h) *Provide a report on site traffic statistics and search engine analysis reports on a monthly basis.*
- (i) *Give monthly updated reports to Embassy about the number of visitors, geographical distribution of visitors, average time spent on the website, most visited sections/pages etc. besides other analysis.*
- (j) *Show number of visitors to the website, on the homepage.*
- (k) *Apart from uploading the contents the CMS will also enable the user to assign specific timeline for the contents to be displayed on the website.*
- (l) *Provide Embassy with three off site coordinator for all the tasks related to website design and maintenance and repairs respectively.*

2.1.3 Content Management System

- (a) *Content Management - Redesign the CMS, edit, revise, update or create new textual content and graphics on existing pages based on Embassy's request. The content (Text & Graphics) updates will be on a weekly basis.*
- (b) *Layout/homepage to be redesigned according to Embassy strategy periodically.*
- (c) *Provide links to all useful websites indicated by the Embassy*

2.1.4 Database Management

- (a) *Maintain registered Indian citizen database.*
- (b) *Content archiving in a local server for periodic review of the content upon need from the Embassy.*
- (c) *Database - requires periodic bug fixing, troubleshooting and the periodic update of searchable data.*
- (d) *Maintain Site Search Engine by ensuring that any content updates and new pages are searchable.*

- (e) *Advanced search option to be incorporated.*
- (f) *Automated reconciliation and generate necessary reports etc.*
- (g) *Maintain a queryable database of Trade Enquiries received from India and from Qatar.*

2.1.5 Adherence to Web Application Audit/ Compliance and Approval / Security Features.

Getting the Security Audit by CERT-IN empanelled agency or STQC or MEA referred companies and obtaining all necessary certificates will be the responsibility of the service provider including the cost involved.

2.1.6 Design and development of the Electronic form application in Secure & Usable format

Websites may include development of a complete online form for electronic Feedback, tracking visa, Passport and other information, MIS reporting for Embassy and Monitoring and managing the various applications involved.

2.1.7 Indicative Deliverables

- *High Level Design/ Architecture Document*
- *Provide a report on site traffic statistics and search engine analysis reports on a monthly basis.*
- *Give monthly updated reports to Embassy about no. of new visitors, geographical distribution of visitors, average time spent on the website, most visited sections/pages etc. besides other analysis.*
- *Show number of visitors to the website, on the homepage.*
- *Development and implementation of the online web strategy with major upgrades in the design and content of the current website.*
- *Editing and proof reading of the website content.*
- *Development of new content for the website as per the advice from the Embassy.*
- *Regular updates on the website.*
- *Prompt and Proper Maintenance of website.*
- *Registered and online information database.*
- *Source code will be handed over to Embassy, whenever requested.*
- *Preparation of e-Newsletters of the Embassy.*

3 PRE-QUALIFICATION CRITERIA

Minimum Eligibility Criteria

3.1 The Agency should be able to provide a qualified web designing, building and maintenance team, for undertaking this assignment. The Agency team would work closely with the Embassy, with face-to-face meetings whenever required. A confirmation letter from the Agency for being able to provide the qualified team should be attached. Details of the team dedicated to the Embassy should be provided.

3.2 **Competencies:**

- (a) *Past experience in creating and maintaining very professionally and exceptionally creative websites for Indian missions.*
- (b) *Excellent I.T. skills and project management skills*
- (c) *Strong editorial team with communications skills to write clearly and compellingly in English and other languages.*
- (d) *Ability to juggle priorities and deadlines and perform well under pressure;*
- (e) *Ability to respond quickly to the maintenance requirement in the post commissioning phase.*
- (f) *Awareness on the latest smart technologies for website development.*
- (g) *Ability to regularly maintain, update the developed website.*

3.3 **Essential knowledge and experience:**

- (a) *Good information technology skills, with previous experience of website maintenance, management, editing, and/or development.*
- (b) *Expertise with HTML and content-management systems and latest trends and technology in website content and social media.*
- (c) *Strong analytical and research skills, including the ability to analyze audiences, attitudes, communications products and messages and to translate them into the design and implementation of effective websites.*
- (d) *Knowledge of the mandate and work of a government department website would be desirable.*

4. **Eligibility Criteria**

Interested Agencies are invited to submit their proposals for the assignment, which must include the following, as detailed subsequently in this document:

- (a) Technical Proposal &
- (b) Financial Proposal

The original proposal (Technical Proposal and Financial Proposal in separate envelopes and correctly labeled) shall be prepared in indelible ink. It shall contain no interlineations or overwriting, except as necessary to correct errors made by the firm itself. Any such corrections must be authenticated by the persons or person who sign(s) the proposals.

4.1 **Technical proposal**

The Agencies are expected to provide the Technical Proposal as specified in the RFP Document. Material deficiencies in providing the information requested for may result in rejection of the proposal.

The Technical Proposal shall contain the following documents:

<i>Ser</i>	<i>Description</i>	<i>Document / Proof</i>

Ser	Description	Document / Proof
1	<i>Details of agency mentioning the name address Email and mobile phone number of the bidder/authorized representative.</i>	<i>Details are to be submitted in the format given in Tech Bid: Details of the Bidder Organization</i>
	<i>The agency should have an office/ branch in Qatar</i>	<i>Proof of the same along with license/ local govt approvals/ etc</i>
3	<i>The agency should produce Articles of Association in case of registered firms) , By-laws and certificates for registration issued by the Registrar of Companies.</i>	<i>Certificate of incorporation issued by the Registrar of companies along with Memorandum of Understanding</i>
4	<i>Proof of agency's turnover during the last three financial years, to establish financial strength of the company.</i>	<i>A certificate to this effect from Chartered Accountant in original must be submitted. And Copies of Income Tax returns for the last three financial years.</i>
5	<i>An undertaking (self-certificate) that the agency hasn't been blacklisted by a central/state Government institution and missions. Also there has been no litigation with any government department on account of IT Services.</i>	<i>Declaration that the bidder has not been blacklisted.</i>
6	<i>Certificate from any Government body that the agency has resources having domain knowledge in web Development Governance applications. Agency need to have a documentary proof of Guidelines for Indian Government Websites (GIGW) Compliance expertise.</i>	<i>Certificate from any Government body as proof.</i>
7	<i>Earnest Money Deposit (EMD) for amount of QAR 10,000.00 (QAR Ten Thousand only) along with Technical bid.</i>	<i>The EMD may be submitted in the form of Bank Guarantee from any of the Public sector banks or a private sector bank authorized to conduct government business as per format. EMD is to remain valid for a period of forty-five days beyond the date of opening of the tender.</i>

- (i) Letter of Technical Proposal Submission.
- (ii) Profile and Track Record of the agency.
- (iii) Detail of award winning web designing and building assignment(s) handled, if any.
- (iv) **Defined deliverables have to be mentioned in the technical proposal with timelines.**
- (v) Detail of the team proposed to be deployed to work with the Embassy, with qualifications and experience of the team members must be provided.
- (vi) An undertaking on the letterhead of the Agency and signed by an authorized signatory, that the Agency will undertake the assignment, in accordance with the Scope of Work detailed in the RFP document and at the cost submitted by the Agency in the financial proposal **(the cost is not to be indicated in the undertaking)**. The above undertaking submitted by the agencies would be binding on the Agency.

Note: **The Technical Proposal shall not include any financial information.**

4.2 Financial Proposal

4.2.1 In preparing the Financial Proposal, Agencies are expected to take into account the requirements and conditions outlined in the RFP document. Letter of Financial Proposal should include:

Ser	Description of Work	Annual Cost (in QAR)
(a)	Redesign and upgradation of the existing website of Embassy as a dynamic and responsive website	
(b)	Technical Maintenance of Website	
(c)	Hosting Charges of Website	
(d)	Any other charges with detailed break-up	
(e)	Assistance in social media and other digital works	
(f)	Assistance in bringing out e-Newsletters of the Embassy	
(g)	Taxes (if any)	
	Grand Total Cost	

It is to be noted that:-

- a) The cost quoted for the works included in the scope of this RFP will be firm and fixed for the duration of performance of the contract. At no point of time will any deviation from the quoted rate be entertained by the Embassy.
- b) The Financial Bid shall not include any conditions attached to it and any such conditional financial proposal shall be rejected summarily.

c) All prices should be quoted in Qatari Riyals (QAR) and indicated both in figures and words. Figures in words will prevail.

d) 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.

5 Submission of Bids

5.1. Tenders must be submitted in two parts, i.e. (i) Technical Bid and (ii) Financial Bid to Embassy of India, Doha, Villa No 86 & 90, Street No. 941, Al Eithra Street, Zone 63, Onaiza PO Box Number 2788, Doha, Qatar, so as to reach the Embassy latest by **Monday, 19 June, 2017, up to 1200 hrs.**

5.2 The Embassy may, at its discretion, extend the deadline for submission of bids by issuing an Addendum in which case all rights and obligations of the proposed project and the agencies will thereafter be subject to the deadlines as extended.

5.3 Embassy will not accept delivery of bid by fax or e-mail. Bid received by fax or e-mail shall be treated as defective, invalid and rejected.

5.4 Bidder should prepare the EMD as per the instructions specified in the tender document. The original should be posted/ couriered/ given in person to the Embassy, latest by the last date of bid submission or as specified in the tender documents.

5.5 The EMD will be issued in favour of 'Embassy of India, Doha, Qatar'

5.6 Financial bids of only those bidders who qualify the technical criteria would be opened.

5.7 Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable.

5.8 The Proposal should be submitted on or before **19 June, 2017.**

5.9 The bid should contain the following documents in two separate packets.
Note: Both the packets – should be submitted together in an overall envelope, superscribed:

“Technical & Financial Bids for Redevelopment and Maintenance of Website for Embassy of India, Doha”.

5.10 No Proposal will be accepted after the deadline for submission.

5.11 The validity of the bids must be for **six months** with effect from the date of opening of the bids.

6. Pre- bid meeting

6.1 In no event will the Embassy be responsible for ensuring that Agency inquiries have been received by it. Mission will endeavor to provide a timely response to all

questions and would provide information to the extent it is currently available to the best of its knowledge. The responses will be communicated through email or a Pre-Bid Meeting will be called, if necessary. The last date for receiving the clarification requests is **31 May, 2017**. Any query received beyond the specified timeline would not be entertained.

7. Opening of bids

There will be two bid-opening process (i) for Technical Bids and (ii) for the Financial Bids:

(a) Embassy will open Technical Bids and list them for further evaluation at **1200 hrs on 19 June, 2017**. The 'Financial Bid' covers shall not be opened until the evaluation of the Qualification cum Technical Bids is complete.

(b) After evaluation of Technical Bids, the Financial bids of only those Agencies, who qualify in the Technical Bids Evaluation process, will be opened. Bidders who qualify in the Technical bid evaluation stage will be informed by email.

(c) Total transparency will be observed while opening the proposals. The Embassy reserves the right at all times to postpone or cancel a scheduled bid opening, as mentioned in the Schedule. In the event of the specified date of bid opening being declared a holiday, the bids shall be opened at the appointed time and location on the next working day.

(d) Bidders can be present at the time of opening of Technical Bids. Advance intimation has to be given by email at hoc.doha@mea.gov.in, with a copy to da@qatar.net.qa.

8. Selection Process

8.1 **Earnest Money Deposit:** Bidders are required to submit Earnest Money Deposit(EMD) for amount of **QAR 10,000.00** (QAR Ten Thousand only) along with Technical Bid. EMD should be issued in favour of 'Embassy of India, Doha'. The EMD may be submitted in the form of a Bank Guarantee from any of the public sector banks or a private sector bank authorized to conduct government business as per format. EMD is to remain valid for a period of forty-five days beyond the date of opening of the tender. No interest will be payable to the Bidder on the amount of the EMD. Bids without Earnest Money would be rejected and no further correspondence shall be entertained in this regard. Unsuccessful Bidder's EMD will be discharged/returned as promptly as possible.

8.2 In the Second Stage, the financial proposals of bidders will be compared amongst the technically qualified bidders.

8.3 The contract will be awarded to the bidder on the basis of the least financial outgo.

8.4 The Successful Bidder will be informed of the decision and he/she will be required to sign an agreement with the Embassy.

9. Payment conditions

(a) Payment will be made in Qatari Riyals (QAR) by the Embassy, by means of a cheque as per the agreed contract terms.

(b) Payments shall be subject to deductions of any amount for which the Bidder is liable as per the penalty clauses of this tender document.

9.2 General Terms and Conditions

(a) Getting the Security Audit by CERT-IN empanelled agency or STQC or MEA Referred companies and obtaining all necessary certificates and to ensure that websites comply with the 'Guidelines for Indian Government Websites (GIGW)' {<http://guidelines.gov.in/> in full}, will be the responsibility of the service provider, including the cost involved.

(b) Identify and execute training requirements, along with preparation of User Manual if any, will be the responsibility of the service provider including the cost involved.

(c) Mere submission of RFP shall not confer any right whatsoever on the submitting entity.

(d) The RFP shall remain valid for a period of 6 months from the date of publication of RFP.

(e) It shall be obligatory on part of the submitting entity to furnish any further information as may be sought by the Embassy.

(f) Every page of RFP must be self-attested by the bidder.

(g) Neither the issue of this invitation for RFP nor any part of its contents is to be taken as any form of commitment or acknowledgement on part of the Embassy to proceed with any RFP or any entity and the Embassy reserves the rights to annul or terminate the process or reject any RFP at anytime or stage without assigning any reason.

(h) Incomplete proposals are liable to be rejected.

(i) If the service provider does not deliver the work to the satisfaction of the Customer within the stipulated time, a penalty of QAR 500/- per calendar week shall be imposed on the service provider. An additional penalty of QAR 100/- per calendar day shall be imposed on the service provider if the work is not completed in additional period of two weeks i.e. by after applying penalty of QAR 500/- per week.

(j) This RFP is not an agreement and is neither an offer nor invitation by Embassy to the prospective Bidders or any other person. The purpose of this

RFP is to provide interested parties with information that may be useful to them in preparing their proposal pursuant to this RFP (the "Bid"). This RFP includes statements, which reflect various assumptions and assessments arrived at by the Embassy in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for the Embassy, its employees to consider the investment objectives, financial situation and particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigation and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP and obtain independent advice from appropriate sources.

(k) The Embassy may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP.

(l) The issue of this RFP does not imply that the Embassy is bound to select a Bidder or to appoint the Selected Bidder, as the case may be, for the Project and Embassy reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

(m) Further, all information/ data/ reports/ pitches/ data or other material submitted to Embassy under this Tender/ RFP by the Applicant shall become the property of the Embassy. The Bidder hereby agrees that they shall not have any right claim, authority whatsoever over the submitted information/ reports/ pitches/ data or other material to the Embassy. The Bidder further agrees and undertakes that the Embassy may use the aforesaid information/ data/ reports/ pitches/ data or other material at its sole discretion and the Bidder shall not have any objection whatsoever in the Embassy using the same.

(n) The firm shall be a legal entity as per GOI rules/ regulations and laws of the land.

(o) The firm should not have been blacklisted by any Government organization

(p) Embassy shall not be liable for any cost incurred by the respondents in preparing responses to this RFP or negotiations associated with award of a contract.

(q) **Force Majeure** - If, at any time, during the continuance of this contract, the performance in whole or in part by either party of any obligation under this contract is prevented or delayed by reasons of any war or hostility, act of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, quarantine restrictions, strikes, lock outs or act of God (hereinafter referred to as force majeure events) provided notice of happenings of any such eventuality is given by either party to the other within 21 days from the date of occurrence thereof, neither party shall, due to such event, be entitled to terminate this

contract nor shall either party have any claim for damage against the other in respect of such non-performance or delay in performance, and deliveries under the contract shall be resumed as soon as practicable after such event comes to an end or ceases to exist, and the decision of the Embassy as to whether the deliveries have been so resumed or not shall be final and conclusive. Further that if the performance in whole or part any obligation under this contract is prevented or delayed by reasons of any such event for a period of exceeding 60 days, both parties may, at their option, terminate the contract.

(r) **Settlement of Disputes and Arbitration-** All disputes, differences and questions arising out of or in any way touching or concerning this agreement or subject matter thereof or the representative rights, duties or liability of the parties shall be referred to the sole arbitration of the Ministry of External Affairs or any person nominated by it. The arbitration shall be in accordance with the Arbitration and Conciliation Act, 1996 or any other law that takes place in this regard. The arbitrator shall be entitled to extend the time of arbitration proceedings with the consent of the parties.

10 Termination of Contract

10.1. The Embassy reserves the right to terminate the contract at any time by giving 3 months advance notice. However, the Embassy 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., and encashing the bank Guarantee for premature termination of Contract. The Service Provider may terminate the contract by giving three months advance notice with justification for termination of services. The Embassy reserves the right to impose a financial penalty in Qatari Riyals equivalent to the service charges for one year, in case the latter terminates the contract without providing six months termination notice.

10.2. **SIGN AND SEAL**: 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 technical bid: "I/We accept the above terms and conditions of tender".

Embassy of India,
Doha, Qatar

AUTHORIZATION LETTER

To

*Embassy of India
Doha, Qatar*

Subject: Proposal for Redevelopment and Upgradation of the website of the Embassy of India, Doha

Sir,

1. We, the undersigned vendor, having read and examined in detail the Specifications and all the bidding documents do propose to provide the Services as specified in the bidding document no.
2. All the prices mentioned in our proposal are in accordance with the terms as specified in the bidding 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 opening of the Bids.
4. We, do hereby confirm that our Bid prices include all taxes, levies etc.
5. We have carefully read and understood the terms and conditions of the contract applicable to the tender and we do hereby undertake Services as per these terms and conditions.
6. We declare that our prices are as per the technical specifications and bid documents. These prices are indicated in Annexure(s) attached with our proposal as part of the commercial bid.
7. We do hereby undertake that, in the event of acceptance of our bid, the Services shall be completed as stipulated in the tender document.
8. We enclose herewith the complete Technical Bid as required by Embassy. This includes:
 - Authorization Letter (Annexure I)
 - Vendor Information (Annexure II)
 - Vendor's –Detailed Experience (Annexure III-A)
 - Past Experience Summary – (Annexure III-B)
 - Technical bid (Annexure IV)
 - Financial bid(Annexure V)
 - EMD (Annexure VI)
 - Sample Website & technical document to be submitted at the time of tender
9. Certified that we are:

A sole proprietorship firm and the person signing the tender is the sole proprietor/constituted attorney of the sole proprietor,

Or

A partnership firm, and the person signing the tender is a partner of the firm and he has authority to refer to arbitration disputes concerning the business of the partnership by virtue of the partnership agreement by virtue of general power of attorney.

Or

A Company and the person signing the tender is the constituted attorney.

(NOTE: Delete whatever is not applicable. All corrections/deletions should invariably be duly attested by the person authorized to sign between us.)

10. We do hereby undertake, that until a contract is prepared and executed, this bid, together with the Embassy's written acceptance thereof, the tender document and placement of letter of intent awarding the contract, shall constitute a binding contract between us.

Signature of vendor representative

Full Address:

Detail of enclosures:

Telephone No:

Annexure II

VENDOR PARTICULARS

Ser	Item	Details	
1	Company Name		
2	Year Established (Copy of Incorporation)	Reg. Certificate attach	
3	Corporate & Address Head Office:	Address Telephone: Fax No. : website Email Address: Mobile No.	
4	Qatar Office: Contact Address Email Address:	Address Telephone: Fax No:	
5	Contact Person	Name Designation Mobile: Email Address:	
6	Financial Turnover Information	Financial Year	Amount (INR equivalent)
		(Copy of Turnover Certificate for the three financial years duly certified by Chartered Accountant Attached as	

Annexure III-A:

VENDOR'S EXPERIENCE

S.No	Item	Details
1.	Name of the project (Also specify the name of website/portal/web application AND URL of the website/portal/Web application)	
2.	Client Details	
3.	Name, Title & Address of the Client who can be contacted	
4.	Project Duration	
5.	Start Date & End Date	
6.	Scope of work	
7.	Relevant work domain	
8.	Software Tools & Technology used	
9.	Total Efforts in Man months	
10.	Contract Value (In Lakhs)	

**** Attach LOI/Work Order/ Contract copy (Mandatory)**

Letter from the Client for satisfactory completion of the project /
Appreciation letter from Client / CERT-in Certificate/ STQC Certification
would be given additional weightage

Annexure III B:

Experience Summary

SL	Project Name	Client Name	Start & End Date	Activities Relevant to scope	Contract Value (USD)	Efforts in Man Months
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						

Technical bid

Sl. No.	Description for Document / Proof to be submitted with Technical bid	Type
(i)	Letter of Technical Proposal Submission.	.pdf
(ii)	Details of agency as per given format a) Profile and Track Record of the Agency. b) Case studies of large brands handled, with focus on results achieved through web designing and development. c) Detail of award winning web designing and building assignment (s) handled, if any.	.pdf
(iii)	<i>Certificate of incorporation issued by the Registrar of companies</i>	.pdf
	<i>along with Memorandum of Articles of Association</i>	
(iv)	<i>Proof of agency's turnover during the last three years</i>	.pdf
	<i>A certificate to this effect from Chartered Accountant in original must be submitted.</i>	
(v)	<i>Copies of Income Tax return for last three financial years</i>	.pdf
(vi)	<i>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.</i>	.pdf
(vii)	<i>Copies of purchase orders in last three financial years' linked satisfactory completion certificates may be submitted as supporting documents.</i>	.pdf
(viii)	Defined deliverables with timelines.	.pdf
(ix)	Detail of the team proposed to be deployed to work with the Embassy, with qualifications and experience of the team members must be provided	.pdf

(x)	An undertaking on the letterhead of the Agency and signed by an authorized signatory, that the Agency will undertake the assignment, in accordance with the Scope of Work detailed in the RFP document and at the cost submitted by the Agency in the financial proposal (the cost is not to be indicated in the undertaking). The above undertaking submitted by the agencies would be binding on the Agency.	.pdf
(xi)	Details of the team dedicated to the Embassy should be provided.	.pdf
(xii)	Earnest Money Deposit (EMD) for the amount of QAR 10,000.00 (QAR Ten Thousand only) along with Technical Bid. The EMD may be submitted in the form of Bank Guarantee from any of the public sector banks or a private sector bank authorized to conduct government business as per format. EMD is to remain valid for a period of forty-five days beyond the date of opening of the tender.	.pdf

Annexure -V

Financial Bid Format

Prices in Financial Bid should be quoted in the following format.

Sl.No.	Document
1.	Letter of Financial Bid Submission
2.	Total fee, include all costs/expenses of the Agency for undertaking work as detailed in the Scope of Work.
3.	Break-up of costs for each of the items of work listed in the Scope of Work are to be submitted on a separate sheet of paper.

Ser	Description of Work	Annual Cost (in QAR)
(a)	Redesign and development of existing website of Embassy as dynamic and responsive website	
(b)	Technical Maintenance of Website	
(c)	Hosting Charges of Website, indicating cost of Virtual Private Cloud Infrastructure	
(d)	Any other charges with detailed break-up	
(e)	Assistance in social media and other digital works	
(f)	Assistance in preparing e-Newsletters of the Embassy	
(g)	Taxes (if any)	
	Grant Total Cost	

It is to be noted that

- a) The cost quoted for the works included in this RFP will be firm and fixed for the duration of performance of the contract. At no point of time will any deviation from the quoted rate be entertained by the Embassy.
- b) The Financial Bid shall not include any conditions attached to it and any such conditional financial proposal shall be rejected summarily.
- c) All prices should be quoted in Qatari Riyals (QAR) and indicated both in figures and words. Figures in words will prevail.
- d) 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.

Date
Place

Signature of Authorised Signatory ...
Name of the Authorised Signatory ...
Designation ...
Name of the Organisation ...
(Seal)

**EMD / PERFORMANCE SECURITY FORM
(Sample Format - TO BE EXECUTED ON A NON-JUDICIAL STAMPED PAPER)**

To: **Embassy of India, Doha, Qatar**

WHEREAS (Name of Bidder) (hereinafter called the "the Bidder") has undertaken, in pursuance of Request for Proposal (RFP) No. ***** dated....., 2017 for "Redevelopment and Maintenance of the Website for Embassy of India, Doha. (hereinafter called the "the RFP").

Our obligation to make payment under this Guarantee shall be a primary, independent and absolute obligation and we shall not be entitled to delay or withhold payment for any reason. Our obligations hereunder shall not be affected by any act, omission, matter or thing which but for this provision might operate to release or otherwise exonerate us from our obligations hereunder in whole or in part, including and whether or not known to us or Embassy of India, Doha:

- (i) any time or waiver granted to the Bidder;
- (ii) the taking, variation, compromise, renewal or release of or refusal or neglect to perfect or enforce any rights, remedies or securities against the vendor;
- (iii) any Variation of or amendment to the RFP or any other document or security so that references to the Contract in this Guarantee shall include each such Variation and amendment;
- (iv) any unenforceability, invalidity or frustration of any obligation of the Bidder or any other person under the RFP or any other document or security waiver by Embassy of any of the terms provisions conditions obligations UNDER RFP or any failure to make demand upon or take action against the Bidder;
- (v) any other fact, circumstance, provision of statute or rule of law which might, were our liability to be secondary rather than primary, entitle us to be released in whole or in part from our undertaking; and;
- (vi) any change in constitution of the Bidder;
- (vii) any petition for the winding up of the Bidder has been admitted and a liquidator or provisional liquidator has been appointed or an order of bankruptcy or an order for the winding up or dissolution of the Bidder has been made by a Court of competent jurisdiction;

This guarantee is valid until the day of <validity date> and a claim in writing is required to be presented to us within one months from <validity date> i.e. on or before <claim period> failing which all MEA rights will be forfeited and we shall be relieved of and discharged from all our liabilities mentioned hereinabove.

Signature and Seal of Guarantors (Bidder's Bank)

.....

Date.....

Address

.....

VIRTUAL PRIVATE CLOUD INFRASTRUCTURE

1. There have been incidents of targeted Distributed Denial of Service (DDoS) and attacks against source code vulnerabilities. This entails that portal and its sub-domains should be hosted on a platform which provides enhanced security, auto-failover and redundancy features.

2. **Objective** To migrate Mission’s website/ main portal and other sub-domain portals/websites on Virtual Private Cloud infrastructure for dedicated hosting.

3. **Scope of Work**

(a) The portal/website maintenance agency will host the Mission/Post main portal and sub-domain websites on Virtual Private Cloud Infrastructure.

(b) The portal/website maintenance agency will 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 Mission/Posts pay for or procure additional system/software licenses.

(c) The portal/website maintenance agency shall provision for computing, storage and bandwidth requirements which may be auto-scaled (additional capacity based on the demand and auto-scaling rules) over the period of contract in line with the transaction load to meet the requirements.

(d) The portal/website maintenance agency shall provision for Cloud services which possess Anti DDoS feature.

(e) The portal/website maintenance agency will carry out migration process to transfer all content from previous hosting Servers to new Cloud Servers within 7x24 hours at data center in India.

(f) The portal/website maintenance agency will provide Non-Disclosure Agreement (NDA).

(g) The portal/website maintenance agency provisioning for the Cloud services shall comply with the following requirements:-

Category	S.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, low latency 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	Cloud provider should offer instances that run on

		instances – Dedicated	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 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 long term 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 and IPs between instances	Cloud service should support the ability to create a network interface, attach it 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	Cloud service should support NAT instances that

		server (NAT instance) at network level	can route traffic from internal-only instances to the Internet.
Networking	31	Multiple VPN Connections per Virtual Network	Cloud service should support creating 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 10 GB 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 – Block Storage	43	Encryption using provider managed keys	Cloud service should support 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 crossregion 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 authentication	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	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 and Management	97	Auto scaling	Cloud service should support 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-the-minute 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