Government of Bermuda

Ministry of Economy and Labour

Addenda

For

Bermuda Digital Identity

Procurement No.: **BND12026**

Issued: **Monday 5th October 2026**

Submission Deadline: **Friday 27th November 2026 10.00 AM Bermuda local time.**

Addenda No, **01**

Addenda Type: Questions and Responses

The following addendum supersedes information contained in the solicitation document issued for this procurement to the extent referenced. This Addendum forms part of the solicitation documents and will be subject to all of the conditions set out in the contract conditions.

Questions and Reponses to Questions

Question 1:	Mandatory technical requirements in a joint submission. Where a joint submission names one party as prime contractor, may the mandatory requirements for a proven production implementation and for ISO/IEC 27001 (or equivalent) certification be satisfied by another member of the joint submission, such as a named technology partner?
Answer 1:	Yes. In a joint submission, a mandatory technical requirement may be satisfied by any member of the joint venture or consortium, provided that the submission clearly identifies the relevant party, its role in delivering the proposed solution, and demonstrates that the party's capabilities will be available throughout delivery and operation of the solution. The submission must identify the prime contractor, which will retain overall responsibility and accountability for contract performance.

Question 2:	Special purpose vehicle. May a respondent be a special purpose vehicle or joint venture formed for this programme? If so: (a) may it rely on its members' experience, references and certifications; (b) may it be incorporated in Bermuda after the RFSQ submission but before contract award; and (c) what should be provided in place of the Certificate of Incorporation and Certificate of Incumbency at the RFSQ stage?
Answer 2:	The RFSQ permits joint submissions provided that a prime contractor is identified. Documentation submitted by the prime contractor and all other members of the joint venture will be evaluated in accordance with the criteria set out in Section F of the RFSQ. Respondents should submit their response based on their current legal and operating structure at the time of submission. If respondents intend to establish a special purpose vehicle or alternative delivery structure for any potential subsequent procurement stage, they may outline their proposed approach within their submission. All corporate documentation required under the RFSQ should be provided for the entities participating in the submission. Any requirements relating to future delivery structures, including any special purpose vehicle arrangements, will be addressed as part of any potential subsequent procurement stage.

Question 3:	Experience and capability. Will the Relevant Experience and Capability criterion be assessed on the joint submission as a whole, or on the prime contractor alone?
Answer 3:	Relevant Experience and Capability will be assessed by reference to the respondent's proposed delivery model, including the prime contractor, consortium members and identified subcontractors, taking account of the role each party will perform in delivering the solution.

Question 4:	Local benefits. Will the Local Benefits criterion be assessed across all members of a joint submission and their subcontractors, or only the prime contractor?
Answer 4:	Local Benefits will be assessed based upon the information provided in the completed Local Benefits Form. The form should be completed by the prime contractor using its entity details and should identify any local businesses, subcontractors, suppliers or partners that will be engaged as part of the proposed delivery model. Respondents should clearly indicate the nature and extent of any local benefits and the entities responsible for delivering them.

Question 5:	Hosting and data residency. Will the Government's mandatory hosting, data residency and cross-border transfer requirements be published before the submission deadline? Is on-island hosting and cryptographic key custody in Bermuda acceptable, or preferred?

Answer 5:	Hosting and Cross-Border Data Transfer Compliance and Accessibility Requirements are identified as Mandatory Technical Requirements. At this stage, respondents should describe their capabilities and proposed approach to hosting, security, privacy and cross-border data transfer requirements based on industry best practice. Detailed hosting, data residency, cybersecurity, cryptographic key management and information classification requirements will be provided to shortlisted respondents during any potential subsequent procurement stage. Respondents should note that personal information stored in, or accessed from, a location outside Bermuda may constitute a transfer to an overseas third party under section 15 of the Personal Information Protection Act 2016 (PIPA). The Government remains responsible for PIPA compliance in relation to any such personal information (sections 5(3) and 15(1)) and must assess the level of protection provided by the overseas third party before any transfer is made (section 15(2)). Biometric information is sensitive personal information (sections 2 and 7(1)), and safeguards must be proportionate to its sensitivity (section 13(2)(b)). Nothing in the RFSQ or in these Addenda approves, or indicates the acceptability of, hosting, storage, replication, backup or support access outside Bermuda. Respondents must disclose each location from which personal information would be stored, processed or accessed, as required by Annex B (Privacy), Q1.2. On-island hosting, and Government custody of cryptographic keys in Bermuda, are acceptable; the Government has not indicated a preference at this stage. At this stage, respondents should describe their proposed approach and any relevant capabilities based on industry best practices.

Question 6:	Intellectual property. In the intended PPP model, will the Government require ownership of the platform's intellectual property, or would a licence combined with source code escrow, data portability and step-in rights meet the Government's continuity and exit requirements?

Answer 6:	Intellectual property and commercial arrangements will be addressed during any potential subsequent procurement stages. Respondents are encouraged to describe their proposed approach to intellectual property ownership, licensing, data portability, continuity of service and exit management based on industry best practices. Any detailed intellectual property, licensing and contractual requirements will be addressed during any potential subsequent RFP and contract negotiation stages.

Question 7:	Multiple submissions. May a technology provider take part in more than one joint submission?
Answer 7:	Yes**.** A technology provider may participate in more than one joint submission. Respondents and participating technology providers remain subject to all conflict-of-interest, confidentiality, non-collusion and procurement integrity requirements of the RFSQ. Any such participation should be fully disclosed within the relevant submissions.

Question 8:	Section 1.3 permits joint submissions with a named prime. Appendix B, Sections C and D require a named production reference and case study, and ISO/IEC 27001 certification. Please confirm whether, in a joint submission or where a named technology partner or subcontractor is proposed, that partner's: 1. Production reference and case study, 2. ISO/IEC 27001 (or equivalent) certification, and 3. Experience and references for the Section F rated criteria may be relied on to meet the requirements, and whether the prime must satisfy any of them directly.

Answer 8:	In a joint submission, the production references, case studies, certifications, experience and references of a named joint venture member may be relied upon to meet the applicable requirements, provided that: • the relevant party is clearly identified; • the prime contractor is identified; • the relevant experience, certification or reference relates to the services that party will deliver; and • the submission demonstrates that the party will have an active role in delivering and operating the proposed solution. Accordingly: • Production references and case studies may be provided by a joint venture member that delivered the referenced solution. • ISO/IEC 27001 certification (or equivalent) may be provided by the joint venture member responsible for the relevant services. • Experience and references submitted under the rated criteria may be provided by the joint venture members that will contribute to delivery. Requirements may be satisfied collectively by the identified members of a joint submission, provided the roles and responsibilities of each participating entity are clearly described. At contract stage, any joint venture member, consortium member or subcontractor that provides the core platform, holds a certification relied upon to meet a mandatory requirement, or is able to access or otherwise use Government personal information will be required to be a direct party to the Government's security schedules and Data Processing Agreement (see Annex B (Privacy), Q1.3 and Q1.5).

Question 9 :	The RFSQ does not explicitly state whether participation is limited to Bermuda-registered entities or whether foreign/international companies may participate. Kindly confirm whether foreign companies are permitted to submit a response independently, through a consortium/joint venture, or through a subcontracting arrangement with a local partner
Answer 9:	Yes. Foreign companies are permitted to submit a response independently, through a consortium/joint venture, or through a subcontracting arrangement with a local partner.

Question10 :	The Government has established the minimum evaluation weight regarding Local Benefits for this procurement at 30% of the total points. Could the Government please clarify whether there are any mandatory requirements regarding the employment or engagement of Bermudian personnel during project implementation, or whether local workforce participation is considered solely as part of the evaluation criteria?
Answer 10:	Local Benefits will be assessed in accordance with the criteria set out in Appendix B, Section F, Category 7 and through the completion of the Local Benefit Form contained in Annex C. The Local Benefits evaluation considers factors including, but not limited to, local workforce utilisation, the number of Bermudians employed by the respondent, the percentage of Bermudian participation during the project, and the use of local specified businesses within the respondent's supply chain and subcontracting arrangements.

Question 11 :	Appendix A – Submission Form requires respondents to provide a Social Insurance Number, Payroll Tax Number, and Registration Number issued by the Bermuda Registrar of Companies (if incorporated). Kindly clarify whether these requirements are mandatory for all respondents, including foreign/international companies. 1. In the case of a Joint Venture/Consortium, would it be acceptable for only the Bermuda-based partner to provide the above-referenced Bermuda registration and tax details, while the foreign partner submits its incorporation and statutory registration documents from its country of incorporation? 2. Additionally, if foreign companies are permitted to participate independently, please confirm what equivalent documents may be provided in lieu of the Bermuda-issued Social Insurance Number, Payroll Tax Number, and Company Registration Number.
Answer 11:	Appendix A requests respondents to provide applicable registration and tax information relevant to their organisation. Respondents should provide the information that is applicable to their circumstances and legal status. Where a respondent is incorporated in Bermuda, the applicable Bermuda registration, payroll tax, and other requested details should be provided. Where a respondent is incorporated outside Bermuda, equivalent incorporation and registration information from the respondent's jurisdiction of incorporation may be provided. The mandatory submission requirements relating to corporate

	status are set out in Appendix B, Section C, including the requirement to provide a Certificate of Incorporation and Certificate of Incumbency where applicable. For joint venture or consortium submissions, participating entities should provide the corporate registration and incorporation documentation applicable to their respective jurisdiction. Where a Bermuda-based entity forms part of the proposed delivery structure, any applicable Bermuda-issued registration and tax information should be provided for that entity.

Question: 12	May a company wholly owned by the Brazilian Government participate, including as prime contractor in a joint submission?
Answer: 12	Yes. Subject to compliance with the requirements of the RFSQ, a company wholly owned by the Brazilian Government may participate either independently or as part of a joint submission, including as the identified prime contractor.

Question 13:	Is registration in Bermuda required at prequalification, or only before contract award? Are equivalent Brazilian corporate documents accepted?
Answer: 13	Please refer to the response to Question 11.

Question: 14	Are indicative details available on the PPP's funding and remuneration model, particularly the supplier's initial investment obligations?
Answer:14	The RFSQ does not prescribe a detailed funding, remuneration, or investment model at this stage.

Question 15:	For the “Proven Digital Identity Solution” mandatory requirement and the three project references, may the experience and named client references come from any member of a joint submission (including the proposed technology vendor), or must they be held by the prime contractor?
Answer 15:	Please refer to the response to Question 8.

Question 16:	In a joint submission, may the ISO/IEC 27001 requirement be met by a consortium member rather than the prime?
Answer 16:	Please refer to the response to Question 1 and 8.

Question 17:	Must a non-Bermudian respondent be registered in Bermuda, or will home-jurisdiction equivalents of the Certificate of Incorporation and Incumbency be accepted?
Answer 17:	Please refer to the response to Question 11.

Question 18:	Could the Government confirm the definition of a "local specified business" for the purposes of this evaluation, including the legislation or policy on which it is based?
Answer 18:	Specified Business is defined in Annex C – Local Benefits Form.

Question 19:	Where a joint submission is made with a clearly identified prime contractor that is not a local specified business, and one or more members of the team are Bermudian businesses, will local benefits be assessed across the full respondent team or only against the prime contractor?

Answer 19:	Please refer to the response to Questions 4.

Question 20:	Would the Government assess different partnership structures (for example a joint venture, a consortium, or a prime contractor with Bermudian subcontractors) differently under the local benefits criterion?
Answer 20:	Please refer to the response to Question 4.

Question 21:	If a respondent intends to establish a Bermuda-registered entity or subsidiary to deliver the contract, would a documented commitment to do so be considered under the local benefits criterion, or must the entity exist at the time of submission?
Answer 21:	The Government will evaluate the information provided in the submission. Respondents may include details of proposed future arrangements; however, evaluations will be conducted on the basis of the evidence submitted in response to the RFSQ.

Question 22:	Does this measure refer to Bermudians employed by the respondent at the time of submission, or will committed future employment over the term of the contract also be considered? Do Bermudians employed by partners or subcontractors on the engagement count towards this measure?
Answer 22:	The Government will consider information provided regarding both current and proposed employment arrangements associated with the delivery of the Services. Respondents should clearly identify the basis of any figures submitted and the role of any partners or subcontractors.

Question 23:	Will proposed arrangements with Bermudian suppliers or subcontractors be considered at the qualification stage, and if so, what evidence would the Government expect (for example letters of intent or teaming agreements)?
Answer 23:	Respondents may provide details of proposed arrangements with Bermudian suppliers or subcontractors. Any supporting information demonstrating the nature and credibility of such arrangements should be included as part of the submission.

Question 24:	Will commitments to training, skills development, and structured knowledge transfer to Bermudian professionals be considered under the local benefits criterion?
Answer 24:	Yes. Respondents may include details of proposed training, skills development, knowledge transfer, and other capacity-building initiatives that would provide benefits to Bermuda.

Question 25:	Could the Government indicate how the 30% weighting for local benefits is distributed across its component measures?
Answer 25:	The Government does not intend to publish a further breakdown of the Local Benefits weighting beyond that set out in the RFSQ documentation.

Question 26:	The Submission Form requests a Bermuda Social Insurance number, Payroll Tax number, and company registration number. How should a respondent that is not yet registered in Bermuda complete these fields, and would leaving them blank be treated as a deficiency at Stage I?
Answer 26:	Where a respondent does not possess a requested Bermuda registration or identification number, it may indicate "Not Applicable" or "N/A" in the relevant field. This will not, in itself, constitute a deficiency at Stage I.

Question 27:	Section D of the RFSQ Particulars requires ISO/IEC 27001 certification or an equivalent independently audited information security certification. Would a SOC 2 Type II attestation be considered an acceptable equivalent? If so, what evidence should respondents include?
Answer 27:	A SOC 2 Type II attestation may be considered as evidence of an equivalent independently audited information security framework. Respondents should provide sufficient supporting documentation to enable the Government to assess the scope, currency, and relevance of the certification or attestation.

Question 28:	For a joint submission, may the mandatory production digital identity deployment be demonstrated by a named member of the respondent team (such as a partner or subcontractor), rather than by the prime contractor alone?
Answer 28:	Please refer to the response to Question 8.

Question 29:	Where a client reference is subject to confidentiality obligations, may the client be identified to the Government on a confidential basis?
Answer 29:	Yes. Respondents may provide confidential information, subject to the provisions of section 3.5.2 Confidential Information of the Respondent in the RFSQ. It should clearly identify any information they consider confidential. The Government reserves the right to seek additional information where necessary to verify a respondent's qualifications and experience. Any information provided remains subject to the Public Access to Information Act 2010 (PATI); see the response to Question 42.

Question 30:	Section 1.5.3 states that sealed packages will not be opened before 20 November 2026, while the Submission Deadline is 27 November 2026. Could the Government confirm the correct dates?

Answer 30:	The reference to 20 November 2026 is amended to read 10.00am, 27 November 2026. Submissions will not be opened before the Submission Deadline.

Question 31:	Section 1.5.3 refers to "0 signed original hard copies." Could the Government confirm whether any hard copies are required, or whether electronic submission alone is sufficient?
Answer 31:	No hard copies are required. Electronic submission in accordance with the instructions set out in the RFSQ is sufficient.

Question 32:	The submission instructions refer to including "the RFP title" in the email subject line. Could the Government confirm that respondents should use the RFSQ title and number?
Answer 32:	Yes. Respondents should include the RFSQ title and number in the email subject line when submitting their response.

Question 33:	With reference to Section 1.3 of the RFSQ and Section IV (Customer Experiences) of Annex A (Company Profile Form), please confirm whether the requirement to provide information for at least three (3) clients, together with corresponding reference letters: (a) must be satisfied individually by each party to the joint submission; or (b) may be satisfied collectively by the parties to the joint submission.
Answer 33:	Please refer to the response to Question 8.

Question 34:	Section 1.4.1 states that the Submission Deadline is Friday, 27 November 2026 at 10:00 AM Bermuda local time. Section 1.5.3 states that responses

	will not be opened until Friday, 20 November 2026 at 10:00 AM, which is seven days before the Submission Deadline.
Answer 34:	Please refer to the response to Question 30.

Question 35:	Please confirm that PDF is an acceptable submission format and that the Respondent may submit one ZIP file containing the complete set of PDF, as applicable. Please also identify any prescribed forms that must be submitted in Microsoft Word format.
Answer 35:	Yes. Respondents may submit their response in Adobe PDF format. Where file size limitations apply, respondents may submit the response as a compressed ZIP file. Unless otherwise expressly stated in the RFSQ, there is no requirement for any document to be submitted in Microsoft Word format.

Question 36:	We understand that each category will be scored against the questions listed in Section F. Please provide the scoring methodology, including any applicable sub-weightings and score descriptors for each rated category.
Answer 36:	The Government does not intend to publish any additional scoring methodology, sub-weightings, or score descriptors beyond those set out in the RFSQ documentation.

Question 37:	We understand that the 30 points will be allocated across the Local Benefits factors in Section F.7 and Annex C. Please confirm the point allocation and the evidence required for each sub-factor.
Answer 37:	Please refer to the response to Question 4, 10 and 25.

Question 38:	We understand that the combined experience and capability of the Respondent and its named partners will be considered in scoring. Please confirm.
Answer 38:	Please refer to the response to Question 8.

Question 39:	Please confirm that, for a joint submission, the mandatory submission requirements, the mandatory technical requirements and the rated criteria on the combined capability of the joint-submission team (lead bidder and named members/key subcontractors) will be evaluated. Project references, production case studies, certifications and key personnel of a named member will count towards the joint response.
Answer 39:	Please refer to the response to Question 8.

Question 40:	Please confirm that, if a signed reference letter is unavailable, the Respondent may instead provide the client's name and contact details for reference checks, without the submission being deemed non-compliant.
Answer 40:	Respondents are encouraged to provide reference letters where available. Where a reference letter cannot reasonably be obtained, respondents may provide client contact information and sufficient project details to enable the Government to undertake reference checks. The Government reserves the right to determine what information is necessary to verify a respondent's experience and qualifications.

Question 41:	Please confirm whether Appendix A and Appendix C must be signed by every member of a joint submission or by the prime contractor on behalf of all members.
Answer 41:	For joint submissions, the Submission Form and Certificate of Non-Collusion should be completed and executed by the prime contractor. The Government reserves the right to request additional documentation from any member of

	the respondent team. This does not affect the requirements that will apply to joint venture or consortium members at contract stage (see the response to Question 8).

Question 42:	Please confirm that commercially sensitive, security-sensitive and proprietary information identified as confidential will be handled in accordance with Public Access to Information Act 2010, including consultation with the affected Respondent or joint-submission member before any disclosure. Please also confirm that evaluators will be subject to confidentiality obligations and that particularly sensitive evidence may be submitted separately, on request, under a non-disclosure agreement.
Answer 42:	Respondents may provide confidential information, subject to the provisions of section 3.5.2 Confidential Information of the Respondent in the RFSQ. The Government reserves all rights and obligations arising under the Public Access to Information Act 2010 and does not agree in advance to any additional confidentiality arrangements not expressly provided for in the procurement documents. The Government is subject to PATI, and records it holds, including RFSQ submissions, may be the subject of a request for access under section 13. Identifying information as confidential does not of itself exempt it from disclosure: whether a record is exempt is determined under Part 4 of PATI, including the exemptions for commercial information (section 25) and information received in confidence (section 26), each of which is subject to a public interest override (sections 25(3) and 26(2)). Where the Government intends to disclose a record that might contain information of a type referred to in section 23, 25 or 26, it must give notice to the third party who gave the information or to whom it relates, who may consent in writing or make written representations within fourteen days, and the Government must consider those representations before deciding the request (section 39). Respondents should also note that records held by an independent contractor relating to a contract with the Government are deemed to be held by the Government (section 3(4)), and that details of contracts valued at $50,000 or more are required to be published in the Gazette (section 6(6)). The contents of submissions are kept confidential to the members of the evaluation panel until a decision is made to award the contract (Code of Practice for Project Management and Procurement, section 26.2), and evaluators are subject to the conflict-of-interest requirements of the Code. Respondents may identify particularly sensitive evidence that they wish to provide separately, and the Government will consider any such request, but cannot agree to arrangements that would conflict with its obligations under PATI.

Question 43:	Please confirm if the prequalified status is granted to the joint-submission team or lead bidder and whether the team composition (for example a sub-contractor) may be changed before the second stage.
Answer 43:	Prequalification relates to the respondent team identified in the submission. Any material change to the composition of the respondent team following submission may be subject to Government review and approval.

Question 44:	Please confirm (a) one Annex B should be completed for the proposed joint solution, not one per member; and (b) Capability of the solution to meet the requirements will be considered sufficient at this stage. No other additional evidence or documentation / proof is required at this stage of RFSQ.
Answer 44:	Respondents should submit one completed Annex B relating to the proposed solution. Responses should be based on the proposed solution's current capabilities and the respondent's ability to satisfy the stated requirements. The Government reserves the right to request additional information or supporting documentation at any stage of the procurement process.

Question 45:	Please confirm a) an independent third-party penetration test, carried out within the last 24 months on the core platform/products proposed (either in an existing production deployment or on the current product release), satisfies Q1.4. b) Penetration test reports available may be made available under confidentiality agreement during the pre-award security assessment.
Answer 45:	Yes. An independent third-party penetration test undertaken within the last 24 months on the core platform, product, or solution proposed to the Government may be used to satisfy this requirement. The Government may request

	additional information or supporting evidence, including penetration testing results, at a later stage of the procurement process. Respondents may provide confidential information, subject to the provisions of section 3.5.2 Confidential Information of the Respondent in the RFSQ.

Question 46:	Please confirm (a) the members of a joint submission and the sub-processors named in the response, once approved at contract award, are treated as having the Government's prior written consent; and (b) licensors of software components deployed inside the Government-controlled environment, who have no access to Government personal information, are not sub-processors for Q1.1a and Q1.5.
Answer 46:	The Government will assess compliance with these requirements based on the proposed delivery model and solution architecture. Naming a joint-submission member or sub-processor in a response does not constitute the Government's prior written consent for the purposes of Annex B (Privacy), Q1.5; any consent will be given in writing after the Government has assessed the proposed sub-processor. Under section 5(3) of the Personal Information Protection Act 2016 (PIPA), the Government remains responsible for ensuring compliance with PIPA at all times where a third party is engaged in connection with the use of personal information, and consent to a sub-processor does not reduce that responsibility. Whether a third party, including a software licensor, is a sub-processor will be determined by whether it is able to store, access, retrieve or otherwise make available personal information (each of which is a form of “use” under section 2 of PIPA), and not by its commercial description. Any final determination regarding sub-processors, third-party providers, and consent requirements will be addressed during contract negotiations and implementation planning.

Question 47:	Please confirm a) the facial portrait shown on the digital credential or permit is excluded from Q1.1. b) the Government, as data controller, may decide to keep encrypted source biometric images in a Government-controlled register for adjudication, audit

	and template regeneration, with the supplier keeping no copies, or whether discarding all raw captures immediately is a fixed requirement.
Answer 47:	Respondents should answer the requirement based on the capabilities and design of their proposed solution. The Government cannot confirm that a facial portrait shown on a credential is excluded from Annex B (Biometric Data), Q1.1: “biometric information” is defined in section 2 of the Personal Information Protection Act 2016 (PIPA) to include facial images that allow the unique identification of an individual, and biometric information is sensitive personal information under section 7(1). Respondents should answer Annex B (Biometric Data), Q1.1 and Q1.2 as written and use the comments field to describe any difference in their solution; no variation is accepted in advance Respondents are encouraged to favour architectures that minimise the biometric data held by the supplier, such as match-on-device or encrypted, revocable template approaches (PIPA section 11). Supplier storage of raw facial images or other raw biometric captures is not accepted (Annex B (Biometric Data), Q1.1 and Q1.2); retention for legal or audit purposes is not an exception available to the supplier, and any such retention would be a decision for the Government. Any retention of source images by the Government in its own register would be a decision for the Government, as the organisation responsible for the personal information, and would need to comply with PIPA, including sections 11 (proportionality), 12(2) (retention no longer than necessary) and 13 (security safeguards). Specific decisions relating to biometric data governance, retention, storage, and operational policies will be determined by the Government during future project phases.

Question 48:	Please confirm which approaches the Government accepts as 'equivalent', for example: protected/revocable templates using keyed transformations, cryptographic binding of templates to credentials with key rotation and re-issuance, and template re-generation from Government-held source images.
Answer 48:	The Government is not prescribing a specific technical approach at this stage. Respondents should describe how their proposed solution satisfies the stated requirement, including any equivalent mechanisms that support the invalidation and re-establishment of biometric credentials following compromise.

Question 49:	Please confirm that the applicable Credential standards should be listed by the bidder as part of the proposal for example: W3C Verifiable Credentials Data Model 2.0, SD-JWT VC, OpenID for Verifiable Credential Issuance (OID4VCI) and Presentations (OID4VP), DID, etc.
Answer 49:	Yes. Respondents should identify the credential, identity, interoperability, and related standards supported by their proposed solution and explain their relevance to the proposed implementation.

Question 50:	Please confirm that (a) experience assessing against other recognised frameworks (e.g., NIST SP 800-63, eIDAS /EUDI ARF, ISO/IEC 29115, the World Bank ID4D Principles, or national trust frameworks) meets the 'demonstrate experience' requirement; (b) the UK DIATF gap assessment is a deliverable of the future contract and not of this RFSQ response; and a formal UK DIATF assessment may be mutually agreed after the contract signed.
Answer 50:	Experience with recognised digital identity trust frameworks may be included as part of a respondent's submission. The assessment contemplated by the RFSQ will form part of the Services and is not required to be completed as part of the RFSQ response.

Question 51:	Please consider extending to at least 20 business days from the date of issuance of addenda for submission of bids, in the event of any delays in issuance of addenda beyond November 6, 2026.
Answer 51:	The Government appreciates the request. At this time, the Submission Deadline remains unchanged. Any amendment to the procurement timetable will be communicated through a formal addendum.

Question 52:	Are there any existing digital identity platforms, digital credentials, identity records, or related services that must be migrated, reused, or integrated with

	the proposed solution, or is the supplier expected to provide a new Digital Identity Platform?
Answer 52:	The Government is seeking a Digital Identity Platform capable of supporting Bermuda's Digital Identity Programme. The Government intends to implement a Digital Identity Platform and associated Digital Wallet capability. Respondents should propose a solution capable of integrating with relevant Government systems and authoritative data sources as described in the RFSQ. Any requirements relating to migration, reuse of existing technologies, or legacy system integration will be further defined during any potential subsequent procurement stages.

Question 53:	Could the Government please clarify the expected scope of the initial implementation, particularly the work permit and resident permit use cases? Which processes must be supported by the Digital Identity Platform, and which will remain within existing immigration systems?
Answer 53:	The programme is expected to be implemented in phases, initially focusing on immigration-related use cases, with particular emphasis on work permits and resident permits. Detailed business process requirements, allocation of responsibilities between the Digital Identity Platform and existing Government systems, and implementation scope will be provided during any potential subsequent procurement stage.

Question 54:	Could the Government provide an indicative list of the systems expected to be integrated with the proposed platform, including their owners, available APIs or interfaces, technical documentation, and the respective responsibilities of the Government and supplier for facilitating these integrations?
Answer 54:	Detailed integration requirements, system inventories, technical specifications, interface requirements and responsibilities will be provided during any potential subsequent procurement stage.

Question 55:	Could the Government share its indicative implementation roadmap, including the anticipated programme phases, key milestones, and expected timing of the initial immigration rollout and subsequent expansion? We understand that these dates may be subject to change.
Answer 55:	The Government anticipates a phased implementation approach, initially focusing on immigration-related use cases before expanding to additional public and private sector services. Detailed implementation planning, milestones, priorities and timelines will be developed following completion of the procurement process and may be refined throughout the programme lifecycle.

Question 56:	Could the Government please confirm whether companies incorporated outside Bermuda may apply directly for this procurement? Is local incorporation, establishing a local office, or partnering with a Bermudian company mandatory at the prequalification stage or before contract award?
Answer 56:	Please refer to the responses to Questions 9, 11, 13 and 17.

Question 57:	Could the Government clarify when the cybersecurity and privacy assessment and Interim Authority to Operate process are expected to commence, the documentation and evidence required, and the anticipated assessment and approval timelines before contract award?
Answer 57:	The successful respondent will be required to complete the Government's cybersecurity and privacy assessment processes and obtain an Interim Authority to Operate before contract award. The detailed requirements, evidence, assessment methodology and timelines will be communicated to shortlisted respondents during any potential subsequent procurement stages.

Question 58:	Could the Government clarify the expected digital wallet capabilities and supported channels? Are separate native Android and iOS applications required in addition to web access, and are any specific digital credential standards, formats, or interoperability profiles mandatory for the initial implementation?
Answer 58:	The Government expects the future solution to include digital wallet functionality supporting identity and attribute credentials across mobile and web channels. The Government is not mandating specific implementation approaches at this stage. Respondents should describe the channels, capabilities, standards and interoperability frameworks supported by their proposed solution.

Question 59:	Could the Government clarify the identity verification requirements for the initial immigration use cases, including the identity documents and government databases to be supported, whether biometric verification is mandatory, and the required identity assurance levels?
Answer 59:	Respondents should describe their identity proofing and verification capabilities, including document verification, biometric and non-biometric options, assurance levels and fraud controls. Detailed identity assurance requirements, supported evidence sources, and any biometric requirements will be defined during future procurement and implementation phases.

Question 60:	Could the Government clarify the expected scope, deliverables, methodology, and timeline for the gap assessment against the UK Digital Identity and Attributes Trust Framework? Please also confirm the expected level of alignment and when the assessment is expected to be completed.
Answer 60:	Please refer to the response to Question 50. The gap assessment against the UK Digital Identity and Attributes Trust Framework forms part of the contemplated Services and is not required as part of the RFSQ response.

	Detailed requirements, deliverables, methodology and implementation timelines will be addressed during any potential subsequent procurement stages.

Question 61:	Could the Government clarify the anticipated hosting and data residency requirements, including permitted hosting locations, cloud hosting arrangements, backup and disaster recovery locations, cross-border data transfers, and Transfer Impact Assessments? Would approved offshore hosting arrangements be considered, subject to the Government's security and regulatory requirements?
Answer 61:	Please refer to the response to Question 5.

Question 62:	The RFSQ requires suppliers to propose a commercially sustainable model that ensures residents are not charged for access to essential digital identity services. Could the Government please clarify the level of detail expected regarding the proposed commercial model at the current prequalification stage? Please also confirm whether detailed funding and revenue arrangements, the allocation of financial and operational risks, and the contractual terms of the proposed PPP will be addressed during any potential subsequent procurement stage, should the programme proceed.
Answer 62:	Please refer to the response to Question 14. At this stage, respondents should demonstrate an understanding of the proposed PPP delivery model and describe their high-level commercial approach.

Question 63:	Could the Government clarify how the financial checks set out in Section E will apply to overseas suppliers that have no existing Social Insurance, Payroll Tax, or other Government payment obligations in Bermuda? Please confirm what evidence of corporate and financial good standing would be required from such suppliers.
Answer 63:	Please refer to the responses to Questions 11, 17 and 26.

Question 64:	Could the Government please confirm the official submission deadline for this RFSQ? Section 1.4 specifies Friday, 27 November 2026, at 10:00 AM Bermuda local time, whereas Section 1.5.3 refers to responses being opened on 20 November 2026. Please clarify the reference to 20 November and confirm the applicable submission deadline.
Answer 64:	Please refer to the response to Question 30.

Question 65:	Could the Government please clarify the accepted submission method for responses? Section 1.5.1 states that email submissions are accepted, whereas Section 1.5.3 refers to a sealed package and specifies zero signed original hard copies or one electronic copy. Could the Government confirm whether submission by email in Microsoft Word and/or PDF format is sufficient and whether any physical submission is required?
Answer 65:	Please refer to the responses to Questions 31, 32 and 35.

Question 66:	Where biometric verification is proposed as part of the solution, could the Government please clarify whether independent biometric accuracy and demographic-bias testing reports must be submitted at the current RFSQ stage or may be provided during any potential subsequent procurement or implementation stage? Would existing independent test results for the proposed biometric technology be acceptable, and are there any specific testing standards or evidence requirements that suppliers must meet?
Answer 66:	Respondents whose solution uses facial recognition, facial matching or liveness detection must answer Annex B (Biometric Data), Q1.3. The Government is not prescribing specific biometric testing standards at the RFSQ stage, and independent accuracy and demographic-bias test reports need not be submitted with the response but may be requested at a later stage.

	Respondents should describe the biometric capabilities of their proposed solution and may include any relevant independent testing, certifications, assurance reports or supporting evidence they consider appropriate. The Government reserves the right to request additional biometric, privacy, security, performance or assurance information during any potential subsequent procurement, assessment or implementation stages.

Question 67:	We understand that the requested solution must cover the complete identity lifecycle, including enrollment, issuance, update, suspension, recovery, and revocation. Based on this understanding, we assume that there is currently no existing identity database that could be used for authentication purposes without an initial enrollment process. Is our understanding correct?
Answer 67:	The Government anticipates that individuals will be required to enroll in the Digital Identity Programme before they can obtain and use a Digital Identity or associated credentials. Respondents should propose solutions capable of supporting the full digital identity lifecycle, including enrolment, credential issuance, maintenance, recovery, suspension and revocation. The Government expects the solution to integrate with relevant authoritative data sources for identity verification and attribute validation. Detailed enrolment, identity proofing and credential issuance requirements will be further defined during any potential subsequent procurement and implementation stages.

Question 68:	If the first understanding is right; is onboarding expected to be self-service, in-person, or both?
Answer 68:	The Government anticipates that the Digital Identity Programme will support accessible and inclusive enrolment processes for all eligible users. Respondents should describe the enrolment channels supported by their proposed solution, including self-service, assisted and in-person enrolment options where available. The Government expects the solution to be capable of supporting varying levels of identity assurance and user accessibility requirements.

	Detailed enrolment, onboarding and identity proofing requirements, including the balance between self-service and in-person processes, will be determined during any potential subsequent procurement and implementation stages.

Question 69:	Is the issuance of a physical identity card or document within scope, or is the programme exclusively digital (wallet-based)?
Answer 69:	The Government's current objective is the establishment of a Digital Identity Platform and associated Digital Wallet capability as described in the RFSQ. Respondents may describe any capability within their proposed solution to support physical credentials or identity documents; however, the Government is not mandating the issuance of a physical identity card as part of this RFSQ.

Question 70:	Can the Government provide indicative volumes: target enrolled population (residents, work-permit holders, non-residents), expected transaction volumes.
Answer 70:	The Government has not established or published definitive enrolment or transaction volume estimates for the Digital Identity Programme at this stage. Respondents should describe the scalability of their proposed solution and its ability to support adoption across Bermuda's resident population, work permit holders and other eligible users as the programme expands.

Question 71:	Could the Government please confirm the expected contract duration?
Answer 71:	The Government has not prescribed a fixed contract duration at the RFSQ stage.

Question 72:	Is there an existing identity register or legacy system (e.g., immigration case management) that must be migrated or integrated?
Answer 72:	The Government anticipates that the Digital Identity Platform will integrate with relevant Government systems and authoritative data sources as required to support identity verification, attribute validation and service delivery. The Government has not prescribed specific migration requirements or identified any mandatory legacy systems for migration as part of the RFSQ. Respondents should describe their solution's ability to integrate with existing and future Government systems through appropriate interfaces and standards. Detailed integration requirements, system inventories, data migration requirements and technical specifications will be provided during any potential subsequent procurement and implementation stages where applicable.

Question 73:	If Bermuda's Government determines that the solution could be cloud-based or SaaS, and considering that PIPA law requires that databases and citizens' personal information remain within the country, is our understanding correct?
Answer 73:	PIPA does not contain a general requirement that personal information be stored or processed only in Bermuda. It regulates the transfer of personal information to an overseas third party (section 15), and the Government remains responsible for compliance with PIPA in relation to any such personal information (sections 5(3) and 15(1)). Hosting and data residency requirements for the programme will be set by the Government, having regard to PIPA and its security and information-classification requirements, as described in the response to Question 5. The Government's primary concern is that any proposed solution complies with applicable legal, privacy, security and regulatory requirements, including PIPA. Subject to the foregoing, respondents may propose cloud-based, SaaS, on-premises or hybrid hosting models and should clearly describe their approach to data protection, security, data residency, cross-border transfers and regulatory compliance.

Question 74:	Could you please confirm if you have an estimate of the number of identities to be generated per year, as well as the number of authentication and verification transactions you would have annually?
Answer 74:	The Government has not established or published definitive estimates for the number of digital identities to be issued annually, nor for anticipated authentication, verification or credential transaction volumes at this stage. Respondents should demonstrate that their proposed solution is capable of operating at scale and supporting increased adoption and transaction volumes as the Digital Identity Programme evolves across Government services and other approved use cases. Detailed volume estimates, growth projections and performance requirements will be further developed and communicated during any potential subsequent procurement and implementation stages. Respondents are encouraged to identify any volume-related assumptions used in preparing their submissions.

Question 75:	Considering that the following matters may have a material impact on the solution design, implementation approach, contractual obligations, pricing, and ongoing operational responsibilities, we kindly request clarification on the specific requirement: *"Suppliers must demonstrate capacity to operate solutions in accordance with Government-defined classification controls."* Could you please specify which controls this requirement refers to? In particular, we would appreciate clarification regarding any applicable cybersecurity, cryptographic, resilience, availability, logging, monitoring, audit, backup, disaster recovery, and business continuity requirements that suppliers are expected to comply with?
Answer 75:	The reference to Government-defined classification controls reflects the Government's requirement that any proposed solution be capable of operating in accordance with applicable Government information security, privacy, data handling and risk management requirements. At the RFSQ stage, the Government is not prescribing a detailed set of technical, operational or cryptographic controls. Respondents should describe the security, privacy, resilience and governance capabilities of their proposed solution, including cybersecurity controls, encryption, access management, audit logging, monitoring, incident management, backup,

	disaster recovery, business continuity and operational resilience arrangements.

Question 76:	Considering that the following matters may have a material impact on the solution design, implementation approach, contractual obligations, pricing, and ongoing operational responsibilities, we kindly request clarification on the specific requirement: Please confirm: the minimum security controls, availability targets, recovery objectives, monitoring requirements, cryptographic standards, and incident response obligations
Answer 76:	At the RFSQ stage, the Government is not prescribing minimum security controls, service availability targets, recovery time objectives (RTO), recovery point objectives (RPO), monitoring requirements, cryptographic standards or incident response obligations. This does not affect the specific requirements already stated in Annex B, including Annex B (Security), Q1.2 and Q1.7 and Annex B (Privacy), Q1.4, which requires contractual notification of a security breach or suspected breach to the Government's Privacy Officer within a defined maximum timeframe so that the Government can meet its own obligations under section 14 of the Personal Information Protection Act 2016 (PIPA) to notify the Commissioner and affected individuals without undue delay. Respondents should describe the security, resilience, operational support and governance capabilities of their proposed solution, including availability commitments, backup and disaster recovery arrangements, monitoring and alerting capabilities, incident management processes, encryption standards and cybersecurity controls.

Question 77:	Considering that the following matters may have a material impact on the solution design, implementation approach, contractual obligations, pricing, and ongoing operational responsibilities, we kindly request clarification on the specific requirement: Could you please provide further details regarding the authoritative government systems referenced in this requirement? Greater clarity on the scope of these integrations is important, as they may significantly impact the solution architecture, implementation effort, dependencies, timelines, and operational model.
Answer 77:	At the RFSQ stage, the Government is not providing a definitive inventory of authoritative systems, data sources or integration endpoints.

	The Digital Identity Platform is expected to be capable of integrating with relevant Government systems and authoritative data sources required to support identity proofing, verification, credential issuance, attribute validation and related service delivery functions. Respondents should therefore demonstrate the flexibility of their proposed solution to integrate with a range of existing and future systems through standard interfaces and integration methods.

Question 78:	Regarding the requirement: “The successful supplier will be expected to assist with legislative gap analysis, regulatory enablement, and related advisory activities.” Could you please clarify whether bidders are expected to provide legislative and regulatory advisory services as part of the project scope? If so, can these services be priced separately on a time-and-materials basis (e.g., consulting hours), rather than being included in the fixed-price proposal?
Answer 78:	The Government anticipates that the successful respondent may be required to support legislative gap analysis, regulatory enablement and related advisory activities associated with the implementation of the Digital Identity Programme. At the RFSQ stage, respondents should demonstrate relevant experience and capability in these areas where applicable. The Government is not requiring detailed pricing proposals as part of the prequalification process.

Question 79:	Considering that the following matters may have a material impact on the solution design, implementation approach, contractual obligations, pricing, and ongoing operational responsibilities, we kindly request clarification on the specific requirement: *"Government will establish mandatory requirements relating to hosting arrangements, data residency, cross-border transfers of personal information, and Transfer Impact Assessments (TIAs), which suppliers will be required to satisfy."* Could you at least provide a basic list of items that the vendor should consider for the solution?
Answer 79:	Please refer to the responses to Questions 5.

Question 80:	Considering that the following matters may have a material impact on the solution design, implementation approach, contractual obligations, pricing, and ongoing operational responsibilities, we kindly request clarification on the specific requirement: For the immigration first use case, which use cases are in scope: work permit and residency permit applications, renewals, physical credential issuance, or digital credentials only?
Answer 80:	The Government anticipates that the initial implementation will focus on immigration-related use cases, including work permits and resident permits. However, the detailed scope of the initial phase, including specific processes, user journeys, credential types and implementation priorities, has not yet been finalised. Respondents should demonstrate how their proposed solution can support digital identity, credential issuance, verification and lifecycle management for immigration-related services. The Government is not mandating physical credential issuance as part of the current RFSQ.

Question 81:	Could you confirm whether there is a plan for the process of adding new use cases, given that the first one will be immigration? If there are, could you share them?
Answer 81:	The Government anticipates that the Digital Identity Programme will be implemented through a phased approach, with immigration-related services forming the initial use case. While the Government expects the programme to expand over time to support additional Government and potentially private-sector services, a definitive roadmap, prioritised use case catalogue or implementation sequence has not been finalised at this stage.

Question 82:	Could you confirm what the Government-defined classification controls would be?
Answer 82:	At the RFSQ stage, the Government has not prescribed specific information classification levels or a detailed set of associated classification controls. Annex B is currently marked “Restricted”. Respondents should design to their

	proposed solution's own stated security and resilience capabilities. The Government's will confirm the classification and the final control requirements and may require architectural adjustment (see the response to Question 126).

Question 83:	Considering that the following matters may have a material impact on the solution design, implementation approach, contractual obligations, pricing, and ongoing operational responsibilities, we kindly request clarification on the specific requirement: Approximately how many government applications and digital services are expected to federate with the Identity Platform as the Government IdP, both at go-live and in the target-state architecture?
Answer 83:	At the RFSQ stage, the Government has not established or published a definitive number of applications, systems or digital services that will federate with the Digital Identity Platform at go-live or within the target-state architecture. The Government anticipates a phased implementation approach, with initial integration focused on priority immigration-related services and subsequent expansion to additional Government services and, potentially, approved external relying parties. Respondents should demonstrate that their proposed solution is capable of supporting a scalable federated identity model and accommodating the onboarding of additional applications, services and relying parties over time. Detailed integration roadmaps, onboarding priorities, federation requirements and target-state architecture information will be provided during any potential subsequent procurement and implementation stages.

Question 84:	Considering that the following matters may have a material impact on the solution design, implementation approach, contractual obligations, pricing, and ongoing operational responsibilities, we kindly request clarification on the specific requirement: Are there existing Identity Providers, IAM platforms, or federation services that must be integrated with or migrated to the proposed solution?
Answer 84:	At the RFSQ stage, the Government is not prescribing any specific Identity Providers, Identity and Access Management (IAM) platforms, federation services or authentication systems that must be integrated with or migrated to the proposed solution.

	The Government expects the proposed Digital Identity Platform to be capable of integrating with relevant Government systems, authoritative data sources and, where required, existing or future identity, authentication and federation services through appropriate standards-based interfaces. Respondents should describe the flexibility and interoperability of their proposed solution, including its ability to support integration, coexistence and migration scenarios where required.

Question 85:	According to the requirement, the provider must support activities to promote and encourage the adoption of digital identity among the public in accordance with the plan established by the Government of Bermuda. Is our understanding correct?
Answer 85:	Yes. The Government anticipates that the successful respondent may be required to support adoption, awareness, education and change management activities associated with the implementation of the Digital Identity Programme. The Government expects overall programme direction, policy and public engagement objectives to remain Government-led. Respondents should describe any relevant capabilities, experience, tools or services they can provide to support user onboarding, stakeholder engagement, awareness campaigns, communications, training and adoption initiatives. The detailed scope, responsibilities and deliverables relating to public adoption, change management and stakeholder engagement activities will be further defined during any potential subsequent procurement and implementation stages.

Question 86:	Which biometric modalities are expected to be used by the solution? Facial, fingerprint or both?
Answer 86:	Please refer to the responses to Questions 47, 59 and 66.

Question 87:	Could you please confirm whether our understanding is correct that the tender requires the bidder to hold a valid ISO 27001 certification at the organizational/company level?
Answer 87:	Yes. The RFSQ requires Respondents to demonstrate compliance with the information security requirements set out in the procurement documents. Where ISO/IEC 27001 certification, or an equivalent independently audited information security certification, is referenced as a mandatory requirement, the certification is expected to be held at the organisational/company level by the bidding entity or the entity responsible for providing the relevant services. Where a Respondent is submitting as a joint venture, consortium, or with key subcontractors, the Respondent should clearly identify which organisation holds the certification and explain how the certified controls, processes, and governance arrangements apply to the delivery of the Services. Any such organisation will be required to be a direct party to the Government's security schedules and Data Processing Agreement at contract stage (see the response to Question 8).

Question 88:	Given that "Does the respondent demonstrate that its Digital Identity platform is capable of supporting privacy-enhancing capabilities, including selective disclosure, consent management, data minimization, and user control of personal information to meet the Government's requirements, regulations, and legislation?", could you please confirm what the Government's requirements are regarding the control of personal data?
Answer 88:	At the RFSQ stage, the Government's detailed requirements regarding control of personal information have not been prescribed beyond the need to comply with applicable legislation (including the Personal Information Protection Act 2016 (PIPA), in particular Part 2 (sections 5 to 16) and Part 3 (sections 17 to 21)), regulations, privacy obligations, and Government policies. Respondents should demonstrate how their proposed solution supports privacy-by-design principles and enables individuals to exercise appropriate control over their personal information, including capabilities such as consent management, selective disclosure, data minimization, transparency regarding data use, and user access to personal information. Consent is one of several conditions for using personal information under section 6(1) of PIPA, and the Government will determine the condition or conditions on which the programme relies.

Question 89:	Given that "Does the respondent demonstrate that its Digital Identity platform is capable of the flexibility and scalability required to support future services, additional relying parties, new credential types, and evolving legal, regulatory, and business requirements?", could you please confirm what the business requirements are?
Answer 89:	At the RFSQ stage, the Government has not prescribed a definitive set of future business requirements. The reference to "business requirements" is intended to recognise that the Digital Identity platform may need to support evolving Government programmes, service delivery objectives, operational processes, user needs, and future use cases that are not yet fully defined. Respondents should therefore demonstrate how their proposed solution can accommodate changing business requirements through configurable workflows, integration capabilities, flexible credential management, support for additional relying parties, and the ability to introduce new services and use cases without significant redesign.

Question 90:	Given that "Does the respondent demonstrate they are capable of supporting the ongoing monitoring, maintenance, management, and support of the solution throughout its operational lifecycle in line with the Government's requirements?", could you please confirm what the Government's requirements are regarding the operational lifecycle?
Answer 90:	At the RFSQ stage, the Government has not prescribed detailed operational lifecycle requirements beyond the expectation that the proposed solution can be effectively operated, supported, maintained, monitored, and enhanced throughout its useful life. Respondents should demonstrate their capability to provide appropriate operational services, including service management, technical support, incident management, problem management, change management, security monitoring, maintenance, patching, upgrades, performance monitoring, backup and recovery, and business continuity capabilities.

Question 91:	Given that "in compliance with applicable legal, regulatory, privacy, security, and trust framework requirements?", could you please confirm what are the minimum requirements that must be met?
Answer 91:	At the RFSQ stage, the Government has not established a definitive minimum set of legal, regulatory, privacy, security, or trust framework requirements beyond those identified in the procurement documentation and applicable laws and regulations. Respondents should demonstrate how their proposed solution can support compliance with applicable Bermuda legislation, including, but not limited to, privacy, (the Personal Information Protection Act 2016 (PIPA)), public access to information (the Public Access to Information Act 2010 (PATI)), cybersecurity, records management, and other relevant statutory and regulatory obligations, as well as recognised industry standards and best practices for digital identity solutions. Respondents should also describe how their solution aligns with established trust framework principles, including identity assurance, authentication, credential management, security, privacy protection, auditability, governance, and risk management.

Question 92:	Given that "Does the respondent demonstrate that its proposed Digital Identity solution is supported by an appropriate security architecture and privacy-by-design framework, including cryptographic controls, key management and safeguards aligned with Bermuda's Personal Information Protection Act (PIPA), sufficient to protect identity data and meet the Government's requirements?", could you confirm what the minimum amount would be to meet the Government's requirements?
Answer 92:	At the RFSQ stage, the Government has not prescribed a minimum set of technical security controls, cryptographic standards, key management requirements, or privacy-by-design measures beyond the requirements set out in the procurement documentation and applicable laws, regulations, and policies. Respondents should demonstrate that their proposed solution incorporates industry-recognised security and privacy practices appropriate for a national-scale Digital Identity platform, including the protection of identity data throughout its lifecycle. This should include, where applicable, robust security architecture, cryptographic protections, key management processes, access controls,

	audit logging, monitoring, privacy-by-design principles, data protection safeguards, and controls supporting compliance with the Personal Information Protection Act 2016 (PIPA) and other applicable legal and regulatory requirements.

Question 93:	Given that "Does the respondent's proposed solution and delivery approach demonstrate its ability to support compliance with the Personal Information Protection Act (PIPA), anti-money laundering and anti-terrorist financing (AML/ATF) obligations, cybersecurity requirements, and other applicable legal, regulatory, and governance requirements?" could you please confirm what other applicable legal, regulatory, and governance requirements are contemplated?
Answer 93:	At the RFSQ stage, the Government has not prescribed an exhaustive list of applicable legal, regulatory, and governance requirements beyond those expressly identified in the procurement documentation and applicable laws and regulations. The reference is intended to recognise that the Digital Identity programme may be required to support a range of current and future legislative, regulatory, policy, operational, and governance obligations that may evolve over time and may vary depending on the specific use cases adopted by the Government. In addition to PIPA, AML/ATF, and cybersecurity requirements, respondents should demonstrate how their proposed solution can support compliance with applicable requirements relating to information governance, records management, audit and accountability, data protection, identity assurance, digital trust, risk management, public sector governance, and other relevant legal or regulatory obligations that may apply to the operation of the Digital Identity ecosystem.

Question 94:	Could you confirm what level of support is expected for consulting on legislative reforms, regulations, or policy development for digital identity initiatives or similar programs, and their ability to meet the Government's requirements?

Answer 94:	At the RFSQ stage, the Government is not prescribing a specific level of effort, resource commitment, or scope of advisory services relating to legislative reform, regulatory development, or policy design. The intent of this requirement is to assess whether respondents have the capability and relevant experience to provide advisory support, guidance, and subject matter expertise where required to assist the Government in the development, implementation, and operation of a Digital Identity programme. Respondents should describe their experience supporting legislative, regulatory, governance, trust framework, policy, or digital identity enablement initiatives, including any comparable engagements undertaken for governments, public sector entities, or regulated industries.

Question 95:	What requirements would the Government need to establish to support vulnerable, digitally excluded, underserved, or at-risk populations and ensure equitable access to the Digital Identity ecosystem?
Answer 95:	At the RFSQ stage, the Government has not prescribed detailed requirements relating to vulnerable, digitally excluded, underserved, or at-risk populations. The intent of this requirement is to assess whether respondents can support inclusive and accessible adoption of Digital Identity services across all user groups. Respondents should demonstrate how their proposed solution can support equitable access through inclusive service design, accessibility features, alternative enrollment and authentication methods, assisted service models, and both digital and non-digital access channels where appropriate.

Question 96:	Can a non-Bermuda company respond to this RFSQ? If so, how should the respondent address the following Bermuda-specific requirements: Certificate of Incorporation, Certificate of Incumbency, Social Insurance number, payroll tax number, and Registrar of Companies number?
Answer 96:	Please refer to the response to Question 11.

Question 97:	Please clarify the intended submission and opening arrangements. Section 1.4.1 states that the Submission Deadline is Friday, 27 November 2026 at 10:00 a.m. Bermuda local time, and Section 1.5.1 permits submissions by email. However, Section 1.5.3 states that sealed packages "will not be opened until Friday November 20, 2026 10:00:00 AM," which precedes the stated submission deadline. Please confirm the correct date and time for opening responses and whether the sealed-package requirement applies to this procurement given that electronic email submissions are expressly accepted.
Answer 97:	Please refer to the response at Question 30.

Question 98:	Please confirm that respondents may submit their response solely by email in accordance with Section 1.5.1, and that no hard-copy originals, sealed packages, or physical delivery are required. Section 1.5.3 states that respondents shall submit "0 signed original hard copies … or one (1) electronic copy," but also provides that a hard copy will prevail if both formats are submitted and requires sealed-package marking. Please clarify whether the reference to "0 signed original hard copies" is intentional, confirm the acceptable electronic signature and authorization requirements for an email-only submission, and confirm that the hard-copy precedence and sealed-package provisions do not apply where only an electronic submission is made.
Answer 98:	Please refer to the responses to Questions 31, 32, 35 and 65

Question 99:	Please confirm whether the mandatory production Digital Identity reference must relate to a solution implemented and operated directly by the respondent/prime contractor, or whether a reference held by a named subcontractor or consortium member may be relied upon to satisfy this requirement. If subcontractor or consortium references are permitted, please specify the required evidence of the respondent's responsibility, control, and role in the referenced implementation.
Answer 99:	Please refer to the response to Question 8

Question 100:	Please describe the current Government Identity Provider, IAM, directory, single sign-on, and access-management capabilities supporting the One Stop Shop programme and other Government services. Please identify the relevant platforms, their ownership, current integrations, and planned changes.
Answer 100:	Please refer to the response to Question 83.

Question 101:	Please confirm the intended target relationship between the Digital Identity Platform and any existing Government IdP/IAM capabilities. Is the Digital Identity Platform expected to replace, integrate with, federate to, or coexist with the existing environment? Please identify any transition-state architecture and migration requirements.
Answer 101:	Please refer to the responses to Questions 52, 53, 77 and 84.

Question 102:	Please define the required functional boundary between the Digital Identity Platform, the Government IdP, OSS, and departmental applications. In particular, please clarify which component will be responsible for authentication, authorization, account management, credential management, consent, attribute release, session management, and audit logging.
Answer 102:	The Authority has not prescribed a specific target operating model or functional allocation between the Digital Identity Platform, Government Identity Provider (IdP), One Stop Shop (OSS), and departmental applications. Respondents should propose an architecture and operating model that clearly defines the allocation of responsibilities for authentication, authorization, account management, credential management, consent management, attribute release, session management, audit logging, and related identity services, in accordance with the requirements set out in the RFSQ.

Question 103:	Please confirm the user populations within scope for Government-wide IAM capabilities. Does the requirement apply only to residents and businesses accessing OSS and public-facing services, or also to Government employees, contractors, service providers, administrators, and other workforce identities?
Answer 103:	Respondents are encouraged to demonstrate how their proposed solution could support broader identity and access management use cases, including Government employees, contractors, administrators, service providers, and other workforce identities, should the Authority elect to expand the scope of the solution in the future.

Question 104:	Please clarify the account-ownership and data-controller model for resident accounts, authentication credentials, identity attributes, consent records, and authentication/audit data. Please also identify the expected responsibilities of the Government, the supplier, and relying parties.
Answer 104:	Respondents should assume that the Government is the organisation responsible under the Personal Information Protection Act 2016 (PIPA) for personal information used in the programme, and that the supplier will act as a third party engaged by the Government in connection with the use of that personal information (section 5(3)), using it solely on the Government's instructions and not for its own purposes, as set out in Annex B (Security), Q1.5 and Annex B (Privacy), Q1.1. The supplier will not acquire ownership of, or independent rights to use, that personal information. Relying parties that receive personal information will be responsible, as organisations, for their own compliance with PIPA (sections 2 and 5). Within that framework, respondents should propose an operating model that clearly identifies ownership, stewardship, and management responsibilities for resident accounts, authentication credentials, identity attributes, consent records, authentication data, audit logs, and other identity-related information, consistent with applicable legal, regulatory, privacy, security, and trust framework requirements referenced in the RFSQ.

Question 105:	Please describe the required approach for matching, linking, and resolving duplicates between existing OSS accounts and newly verified Digital Identity accounts. This should include matching attributes, confidence thresholds,

	exception handling, user-assisted matching, manual review, remediation of mismatches, and responsibility for data correction.
Answer 105:	Respondents should describe their proposed approach for identity matching, account linking, duplicate detection, exception handling, manual review processes, mismatch remediation, and data correction procedures. The proposed approach should support accuracy, security, privacy, auditability, and an appropriate user experience.

Question 106:	Please confirm the mandatory authentication, authorization, federation, credential, API, and lifecycle standards. The RFSQ refers to OpenID Connect, OAuth 2.0, SAML, and applicable credential standards; please specify which are mandatory at go-live, the required profiles and versions, and any requirements for Verifiable Credentials, DIDs, SCIM, FIDO2/WebAuthn, or other protocols.
Answer 106:	The RFSQ identifies a range of standards and protocols that may be relevant to the proposed Digital Identity solution, including OpenID Connect (OIDC), OAuth 2.0, SAML, and applicable credential standards. However, the Authority has not prescribed mandatory versions, profiles, or implementation specifications for these standards at go-live. Respondents should demonstrate how their proposed solution supports recognised industry standards and best practices for authentication, authorization, federation, credential management, interoperability, lifecycle management, and secure integration, in accordance with the requirements of the RFSQ.

Question 107:	Please define the required identity and authentication assurance levels for each anticipated Government transaction and service category. Please identify the assurance framework to be applied, requirements for identity proofing and authentication factors, step-up authentication triggers, credential-recovery requirements, and any different standards for residents, businesses, and workforce users.
Answer 107:	The Government has not prescribed specific identity assurance levels, authentication assurance levels, or a mandatory assurance framework for individual Government transactions, services, or user populations.

	Respondents should describe their proposed approach to identity proofing, authentication assurance, credential management, account recovery, step-up authentication, and risk-based access controls, and explain how these capabilities can support varying levels of assurance across different services and use cases.

Question 108:	Please confirm whether the supplier is expected to provide authorization services in addition to authentication. If so, please clarify the required authorization model, including role-based or attribute-based access control, delegated authority, organisation/business representation, and the source of entitlement data.
Answer 108:	The RFSQ does not prescribe a specific authorization model or require a particular allocation of responsibilities between authentication and authorization services. Respondents should describe the authorization capabilities of their proposed solution and explain how these capabilities support Government requirements, including role-based access control (RBAC), attribute-based access control (ABAC), delegated authority, organisational or business representation, and other access-management use cases where applicable.

Question 109:	Please provide an inventory or classification of in-scope OSS and Government applications, including their current authentication methods and integration readiness. Please indicate which applications can support modern federation protocols and which require legacy integration patterns, such as headers, agents, reverse proxies, custom connectors, or shared credential transition arrangements.
Answer 109:	Please refer to the responses to Questions 77, 83 and 84.

Question 110:	Please confirm whether support for legacy applications that cannot consume modern federation protocols is mandatory. If it is, please specify the applications in scope, expected duration of support, permitted compensating

	controls, ownership of remediation, and whether legacy integration is to be included in the initial implementation phase.
Answer 110:	Please refer to the responses to Questions 52, 54, 72, 77 83 and 84

Question 111:	Please specify the availability, performance, resilience, recovery, and support requirements for the IdP and related authentication services. This should include service availability targets, transaction volumes, peak-load assumptions, recovery time objective, recovery point objective, multi-site or multi-region requirements, planned-maintenance windows, incident severity definitions, and 24/7 support expectations.
Answer 111:	Please refer to the response to Question 76.

Question 112:	Please confirm the hosting, data-residency, cross-border transfer, and cryptographic-key-management requirements that will apply to resident identity, authentication, credential, consent, and audit data. The RFSQ states that these requirements will be Government-defined; please clarify whether baseline requirements are available for this RFSQ response and which requirements will be finalised only in subsequent procurement stage.
Answer 112:	Please refer to the response to Question 5.

Question 113:	Please clarify the Government's expectations for stakeholder engagement, public education, and adoption activities. In particular, please identify: The stakeholder groups, priority user segments, relying parties, and Government departments to be engaged.
Answer 113:	Please refer to the responses to Questions 70 and 85.

Question 114:	Please clarify the Government's expectations for stakeholder engagement, public education, and adoption activities. In particular, please identify: The stakeholder groups, priority user segments, relying parties, and Government departments to be engaged.
Answer 114	Please refer to the responses to Questions 70 and 85.

Question 115:	Please clarify the Government's expectations for stakeholder engagement, public education, and adoption activities. In particular, please identify: The respective responsibilities of Government and the supplier for communications, public education, outreach, trust-building, and relying-party onboarding.
Answer 115:	Please refer to the responses to Questions 70, 83, 85 and 89

Question 116:	Please clarify the Government's expectations for stakeholder engagement, public education, and adoption activities. In particular, please identify: Any existing engagement strategy, communications standards, research, or adoption baseline that the supplier must use.
Answer 116:	Please refer to the responses to Questions 70, 83, 85 and 89

Question 117:	Please clarify the Government's expectations for stakeholder engagement, public education, and adoption activities. In particular, please identify: The expected treatment of vulnerable, digitally excluded, underserved, and at-risk users.
Answer 117:	Please refer to the response to Question 95

Question 118:	Please clarify the Government's expectations for stakeholder engagement, public education, and adoption activities. In particular, please identify: The adoption, accessibility, user-satisfaction, and onboarding measures that will be used to assess success.
Answer 118:	Please refer to the responses to Questions 70, 83, 85, 89 and 95

Question 119:	Please clarify the Government's expectations for stakeholder engagement, public education, and adoption activities. In particular, please identify: Please confirm the if and indicative plan needs to be provided at the RFSQ stage and the level of detail expected.
Answer 119:	Respondents must comply with the requirements of the detailed Other Mandatory Submission Requirements as outlined in the RFSQ.

Question 120:	Please clarify the supplier's obligations under Appendix B, Section C – "Digital Identity Trust Framework Assessment." In particular, please confirm: whether the UK Digital Identity and Attributes Trust Framework is to be used solely as a benchmark or as a required target state for the Bermuda solution.
Answer 120:	Please refer to the responses to Questions 50 and 60.

Question 121:	Please clarify the supplier's obligations under Appendix B, Section C – "Digital Identity Trust Framework Assessment." In particular, please confirm: The specific version, principles, profiles, certification requirements, and assessment criteria to be applied.
Answer 121:	Please refer to the responses to Questions 50, 60 and 91.

Question 122:	Please clarify the supplier's obligations under Appendix B, Section C – "Digital Identity Trust Framework Assessment." In particular, please confirm: Whether the gap assessment will cover the platform, digital wallet, identity proofing, credential issuance, authentication, governance, privacy, security, operations, and relying-party ecosystem.
Answer 122:	Please refer to the responses to Questions 50, 60 and 91.

Question 123:	Please clarify the supplier's obligations under Appendix B, Section C – "Digital Identity Trust Framework Assessment." In particular, please confirm: Whether the gap assessment will cover the platform, digital wallet, identity proofing, credential issuance, authentication, governance, privacy, security, operations, and relying-party ecosystem.
Answer 123:	Please refer to the responses to Questions 50, 60 and 91

Question 124:	Please clarify the supplier's obligations under Appendix B, Section C – "Digital Identity Trust Framework Assessment." In particular, please confirm: Whether Government expects recommendations only, or a costed and phased remediation roadmap for alignment.
Answer 124:	Please refer to the responses to Questions 50, 60 and 91

Question 125:	Please clarify the supplier's obligations under Appendix B, Section C – "Digital Identity Trust Framework Assessment." In particular, please confirm: How any conflicts between the UK framework, Bermuda law, PIPA, and Government-specific requirements should be addressed.
Answer 125:	The UK Digital Identity and Attributes Trust Framework is intended to be used as a recognised reference framework for assessment and gap analysis purposes. Where any conflict exists between the UK framework, Bermuda legislation (including PIPA), Government policies, regulatory requirements, or

	Government-defined controls, respondents should assume that Bermuda legal and regulatory requirements and Government requirements will prevail.

Question 126:	Please clarify how respondents are expected to demonstrate capacity to comply with Government-defined information-classification controls at the RFSQ stage, given that the formal information-classification assessment and resulting requirements will be completed only before the subsequent procurement stage: please confirm whether respondents should provide evidence of capability to meet a range of potential information-classification levels and the associated cybersecurity, cryptographic, resilience, availability, logging, monitoring, and recovery controls.
Answer 126:	At the RFSQ stage, respondents are expected to demonstrate that their proposed solution and organisation have the capability and capacity to support a range of Government information-classification requirements and associated security controls. Respondents should describe how their solution can be configured and operated to meet differing levels of information sensitivity, including appropriate cybersecurity, cryptographic, resilience, availability, logging, monitoring, audit, backup, business continuity, and disaster recovery controls. The formal information-classification assessment and any resulting mandatory control requirements will be completed prior to any potential subsequent procurement stage. Specific classification levels, security requirements, and compliance obligations applicable to the selected use cases will be provided at that stage. Therefore, respondents are not required to demonstrate compliance with classification requirements that have not yet been defined but should provide evidence of their capability to meet such requirements where required.

Question 127:	"Please clarify how respondents are expected to demonstrate capacity to comply with Government-defined information-classification controls at the RFSQ stage, given that the formal information-classification assessment and resulting requirements will be completed only before the subsequent procurement stage: please confirm whether respondents should provide a formal commitment to comply with the final information-classification control baseline once it is issued."

Answer 127:	Yes. Respondents should confirm their willingness and ability to comply with the final Government-defined information-classification requirements and associated control baseline once these have been established.

Question 128:	"Please clarify how respondents are expected to demonstrate capacity to comply with Government-defined information-classification controls at the RFSQ stage, given that the formal information-classification assessment and resulting requirements will be completed only before any potential subsequent procurement stage: please confirm whether respondents should provide a response against an interim information-classification control baseline to be provided by Government.
Answer 128:	No. Respondents are not required to provide a response against an interim information-classification control baseline at the RFSQ stage. As set out in the RFSQ, the formal information-classification assessment and the resulting security and control requirements will be completed prior to any potential subsequent procurement stage. At this stage, respondents should demonstrate the flexibility and capability of their organisation and proposed solution to support Government-defined information-classification requirements and associated controls once these are established.

Question 129:	Please identify the legislation, regulations, policies, trust frameworks, and Government entities expected to be within scope of the legislative gap analysis and regulatory enablement work.
Answer 129:	Respondents should assume that the assessment may include applicable Bermuda legislation, regulations, Government policies and standards relevant to digital identity, privacy, cybersecurity, data protection, electronic transactions, immigration, and related Government service delivery. This would include consideration of the Personal Information Protection Act (PIPA) and any applicable trust frameworks, standards, or assurance frameworks adopted by the Government. Respondents should demonstrate their capability to perform such assessments across multiple legislative and regulatory domains. The specific scope, stakeholders, Government entities, and applicable frameworks will be

	confirmed during any potential subsequent phases of the programme as requirements are further defined.

Question 130:	Please confirm whether the supplier is expected to provide high-level advisory input only, or detailed legal and policy analysis, drafting instructions, draft legislative or regulatory instruments, consultation support, and implementation guidance.
Answer 130:	The RFSQ does not prescribe the specific level of effort or deliverables required for legislative, regulatory, or policy advisory activities. Respondents should demonstrate their capability to support legislative gap analysis, regulatory enablement, and related advisory services as required by the Government. The precise scope of these activities, associated deliverables, and the extent of supplier involvement will be determined during any potential subsequent phases of the programme and may vary based on Government requirements and the selected use cases.

Question 131:	Please clarify the respective responsibilities of Government, its legal advisers, regulators, and the supplier for policy decisions, legal interpretation, drafting, stakeholder consultation, and formal approvals.
Answer 131:	Respondents should assume that the supplier's role is to provide legislative gap analysis, regulatory enablement support, recommendations, and subject-matter expertise to inform Government decision-making. Responsibility for policy decisions, legal interpretation, regulatory determinations, drafting approval, stakeholder consultation governance, and the approval or enactment of legislation and regulations will remain with the Government and its authorised legal, policy, and regulatory representatives.

Question 132:	Please confirm the anticipated timing, phases, and dependencies for the legislative gap analysis, regulatory enablement, and related advisory activities.
Answer 132:	Respondents should assume that these activities will be undertaken as required to support the design, implementation, deployment, and operation of the Digital Identity programme and its associated use cases. The timing and scope of such activities may depend on programme priorities, solution design decisions, policy development, stakeholder engagement, governance approvals, and the implementation roadmap. Detailed planning, milestones, dependencies, deliverables, and resource requirements for legislative and regulatory activities will be defined by the Government during any potential subsequent phases of the programme as requirements mature and implementation planning progresses.

Question 133:	Please specify the required outputs, acceptance criteria, and assurance or review arrangements for this work.
Answer 133:	The RFSQ does not prescribe detailed outputs, acceptance criteria, assurance activities, or review arrangements for the legislative gap analysis, regulatory enablement, and related advisory services. Respondents should demonstrate their capability to produce appropriate deliverables in support of these activities, which may include assessments, gap analyses, recommendations, implementation roadmaps, supporting documentation, and advisory reports. Deliverables should be of a standard suitable for Government review and decision-making. The specific outputs, acceptance criteria, quality assurance requirements, governance arrangements, review processes, stakeholder involvement, and approval mechanisms will be defined by the Government during subsequent phases of the programme and may vary depending on the nature of the work being undertaken and the applicable use cases.

Question 134:	Legal & Regulatory Readiness. Please confirm whether this capability should be evidenced at the RFSQ stage only, or included as a separately scoped and priced workstream in the subsequent procurement stage.

Answer 134:	The capability should be evidenced at the RFSQ stage as part of the respondent's qualifications, experience, and ability to support legislative gap analysis, regulatory enablement, and related advisory activities where required.

Question 135:	Material Disclosures identifies immigration as the initial use case, with emphasis on work permits and resident permits. Please provide the expected volumes of work permits and resident permits that will be in scope for the initial immigration phase, including annual volumes for new applications and renewals. Please also confirm the specific permit types and categories to be included at launch.
Answer 135:	Respondents should assume that the initial immigration use case will be defined in greater detail during any potential subsequent phases of the programme. The specific permit types, user populations, transaction volumes, onboarding forecasts, and implementation priorities for the initial roll-out will be confirmed by the Government as requirements are further developed. Until such information is provided, respondents should demonstrate that their proposed solution is capable of supporting a range of immigration-related identity verification, credential issuance, and lifecycle management requirements at Government scale, and can accommodate varying permit categories, volumes, and future expansion to additional use cases.

Question 136:	Please confirm the required hosting jurisdiction and data-residency boundaries, including whether remote administrative or support access from another country constitutes a cross-border transfer. Please also identify the required Transfer Impact Assessment methodology, approved transfer mechanisms, and applicable accessibility standard.
Answer 136:	Please refer to the response to Question 5. Remote administrative or support access to personal information from outside Bermuda ‘may’ constitute a transfer to an overseas third party under section 15 of the Personal Information Protection Act 2016 (PIPA), because “use” of personal information under section 2 includes retrieving, consulting and otherwise making available personal information. Respondents should assume that any

	such access falls within the Government's assessment under section 15(2) and the requirements referred to in the response to Question 5. The Government has not prescribed a Transfer Impact Assessment methodology or approved transfer mechanisms at this stage; the mechanisms provided for in section 15 include reliance on a comparable level of protection (section 15(4)) and contractual or other mechanisms (section 15(5)).

Question 137:	Please confirm whether the requirement that essential digital identity services be provided at no charge applies exclusively to residents. If non-residents are eligible to access these services, please clarify whether suppliers may propose a separate fee structure or commercial model for non-resident enrollment, credential issuance, renewal, recovery, and use. Please also confirm whether any Government-defined pricing limits, approval requirements, or exemptions would apply to fees charged to non-residents.
Answer 137:	The RFSQ only states that residents will not be charged for essential Digital Identity services. The Government has not yet defined eligibility categories, charges applicable to any non-resident populations, or the future commercial model. These matters will be addressed during any potential subsequent procurement stages.

Question 138:	Please define "**resident**" for the purposes of this requirement, including the applicable eligibility criteria and whether the term includes citizens ordinarily residing in Bermuda, permanent residents, spouses or dependents of Bermudians, work-permit holders, and other individuals legally residing in Bermuda. Please also confirm what documentation or authoritative Government data source will be used to verify an individual's residency status and eligibility for no-charge essential digital identity services.
Answer 138:	The Government will determine eligibility, residency criteria and entitlement rules during any potential subsequent phases of the programme and/or any potential subsequent procurement stage. Eligibility may extend to different categories of individuals lawfully resident in Bermuda, as defined by applicable legislation, policy and programme requirements. The treatment of children and persons lacking legal capacity has not yet been determined. Respondents should explain how their solution can support

	parental or guardian consent where required, including compliance with section 16 of the Personal Information Protection Act 2016 (PIPA). The Government will also define the authoritative data sources, verification processes, evidential requirements and data-sharing arrangements used to establish eligibility and residency. Respondents should therefore demonstrate that their solution can support flexible eligibility, identity proofing, verification and entitlement models based on Government-defined business rules and authoritative data sources.

Question 139:	Appendix B, Section B – Material Disclosures identifies a single-provider PPP model and requires a sustainable commercial model with no charge to residents for essential services, but it does not state the Government's funding commitment or financial contribution. Please clarify the anticipated Government funding and commercial-support arrangements for the Digital Identity Programme under the proposed single-provider PPP model. In particular, please confirm whether Government expects to provide any capital funding, implementation funding, ongoing service payments, minimum-revenue or volume commitments, funding for Government-system integrations, or other financial support. Please also clarify which costs are expected to be recovered by the supplier, the intended treatment of change requests and expansion to additional use cases, and whether an affordability envelope or indicative budget will be provided at the subsequent procurement stage.
Answer 139:	Please refer to the response to Questions 14 and 62

Question 140:	In written answers published on 23 October 2026, the Ministry said the Government has not selected a particular technical standard, credential format, trust framework or digital wallet model, and that a future model would need to distinguish between the individual's identity, the credential used to represent or verify that identity, the underlying government records, and the technology through which the credential is provided. Please confirm by addendum that responses may describe more than one workable approach, including a single-provider identity platform and wallet, and an open credential model in which government issues credentials and wallets are offered by multiple providers to published standards.

Answer 140:	The Government has not prescribed a specific technical standard, credential format, trust framework, digital wallet model, or implementation architecture. Respondents may propose solutions that meet the requirements and objectives set out in the RFSQ, and these will be evaluated in accordance with the published evaluation criteria.

Question 141:	For the immigration use case, may a response describe verification of the documents already used today, a passport, a work permit, a marriage certificate, and related credentials, in the combination the case requires, and also describe a wider platform, so that government can compare those levels of scope before choosing?
Answer 141:	Please refer to the responses to Questions 59, 80, 89 and 136

Question 142:	The particulars ask for a gap assessment against the UK Digital Identity and Attributes Trust Framework. Is that framework a reference for comparison, so that a response may also describe a Bermuda approach based on how documents are issued and certified today, including authorised private issuers and interoperable private wallets?
Answer 142:	Yes. The UK Digital Identity and Attributes Trust Framework is intended to serve as a reference point for assessment and gap analysis purposes and should not be interpreted as prescribing a single implementation model. Please also refer to the responses to Questions 50, 60 and 126.

Question 143:	Will material that keeps the architecture open be retained on the file and available when government decides whether and how to proceed?
Answer 143:	Yes. Information provided by respondents regarding alternative approaches, future-state architectures, open standards, credential models, identity ecosystems, wallet models, interoperability options, and related considerations will form part of the respondent's submission and may be

	considered by the Government as part of its evaluation and future decision-making.

Question 144:	May a respondent submit as an individual with a stated intent to form a Bermuda entity before any second stage or contract award? If so, may that respondent meet the experience, reference, and production-system requirements through the documented experience of its principals and key personnel, or of named subcontractors or consortium members?
Answer 144:	For the purposes of the RFSQ, respondents should clearly identify the legal entity submitting the response and the parties that will contribute to the delivery of the solution. Where experience, references, production deployments, specialist capabilities, or key personnel from subcontractors, consortium members, affiliates, or proposed future entities are relied upon, respondents should clearly describe those relationships and the role each party will perform. The Government will assess responses based on the information submitted and the respondent's demonstrated ability to deliver the requirements of the RFSQ.

Question 145:	May the ISO/IEC 27001 (or equivalent) requirement be met by a subcontractor or hosting partner that will operate the relevant systems, or by a commitment to obtain certification before any contract award?
Answer 145:	Please refer to the response to Question 1 and 8.

Question 146:	For the requirement of a production digital identity or high-assurance credential system within the last five years, does a system qualify if it was in production during that period, even if it began earlier or is no longer operating?
Answer 146:	Yes. For the purposes of demonstrating relevant experience, a production Digital Identity or high-assurance credential system may qualify if it was

	operational in a production environment at any time within the preceding five years, even if the system was originally deployed earlier. Where a solution is no longer in operation, respondents should clearly identify the period during which the system was in production, the scope of the deployment, the respondent's role, and the relevance of the experience to the requirements of the RFSQ. Respondents should provide sufficient information to enable the Government to assess the scale, complexity, operational maturity, and relevance of the referenced deployment against the requirements of the RFSQ.

Question 147:	The Ministry has said that no final commercial model has been selected. May a response describe, as one possible first phase, making documents the Government already issues verifiable, in the way Bermuda's vaccination certificates were, built by a provider at its own cost? The Government would pay only for use, by transaction or subscription, with no upfront payment and no obligation to adopt it. A wider platform would remain a later decision.
Answer 147:	Respondents may describe alternative implementation and commercial approaches that meet the objectives of the RFSQ.

Question 148:	Section 1.4.1 specifies a submission deadline of 27 November 2026 at 10:00 a.m. Bermuda local time, whereas Section 1.5.3 refers to the opening of submissions on 20 November 2026 at 10:00 a.m. We would be grateful if the Procurement Authority could confirm the applicable submission deadline and opening date.
Answer 148:	Please refer to the responses to Questions 30 and 34.

Question 149:	Pending completion of the Government-led information classification assessment, could the Procurement Authority please clarify which baseline security controls respondents should address at the qualification stage and what supporting evidence is required to demonstrate their ability to meet the forthcoming classification-dependent requirements?

Answer 149:	At the RFSQ stage, respondents are not required to demonstrate compliance with a specific Government information-classification control baseline. Respondents should instead describe their security, privacy, governance, and operational capabilities, and provide relevant certifications, attestations, or other evidence demonstrating their ability to support security requirements appropriate to Government-defined classification levels. Detailed classification-dependent requirements and control standards will be confirmed at a later stage of the procurement process.

Question 150:	Could the Procurement Authority please confirm whether the Government has a preferred or prescribed hosting model for the platform, namely commercial public cloud, Government-hosted infrastructure or a hybrid deployment?
Answer 150:	Please refer to the responses to Questions 5, and 77.

Question 151:	Could the Procurement Authority please confirm whether personal information, including biometric data, must be stored and processed exclusively in Bermuda? If overseas storage or processing is permitted, we would appreciate clarification of the acceptable countries or regions for primary processing and storage, disaster recovery and backup, together with the applicable cross-border transfer safeguards and Transfer Impact Assessment requirements.
Answer 151:	Please refer to the response to Question 5.

Question 152:	Could the Procurement Authority please confirm whether remote support and administration from outside Bermuda are permitted and, if so, clarify the conditions applicable to such access?
Answer 152:	Remote support and administration from outside Bermuda are not prohibited under the RFSQ. Remote access to personal information from outside Bermuda may constitute a transfer to an overseas third party under section 15 of the Personal Information Protection Act 2016 (PIPA) (see the response

	to Question 136), and no such arrangement is approved by this response. Respondents may propose remote support and administration arrangements disclosing each location from which access would occur (Annex B (Privacy), Q1.2); Respondents may propose remote support and administration arrangements; however, any such arrangements must comply with the Government's final security, privacy, data residency, and cross-border data transfer requirements, which will be confirmed during a later stage of the procurement process.

Question 153:	With reference to Annex B, Security Q1.1, could the Procurement Authority please clarify whether a respondent proposing on-island or Government-hosted infrastructure and answering "No" to the cloud-hosted service question would be considered non-compliant with the mandatory technical requirements, or whether an equivalent non-cloud deployment may satisfy the requirement?
Answer 153:	A response proposing on-island, Government-hosted, or other non-cloud infrastructure will not be considered non-compliant solely because it answers "No" to Annex B, Security Q1.1. Respondents may propose an equivalent deployment model, provided they demonstrate how the proposed solution meets the functional, security, operational, and technical requirements set out in the RFSQ.

Question 154:	With reference to Annex B, Security Q1.7, could the Procurement Authority please confirm whether the Government is required to operate its own hardware security module (HSM) or key management service, or whether customer-managed keys within the supplier's cloud tenancy, under Government administrative control, would satisfy the requirement? We would also appreciate clarification of the required allocation of authority for key creation, rotation, disablement and recovery, together with the approval and audit requirements for emergency ("break-glass") access.
Answer 154:	The RFSQ does not prescribe a specific hardware security module (HSM) ownership or key management model. Respondents may propose either Government-operated key management services or customer-managed keys under Government administrative control, provided the proposed approach meets the security, audit, governance, and operational requirements of the solution.

Question 155:	With reference to Annex B, Biometric Q1.1, could the Procurement Authority please clarify whether the template-only requirement extends to a credential portrait retained for identity proofing and credential issuance, or applies solely to biometrics used for authentication and liveness verification?
Answer 155:	Please refer to the responses to Questions 47, 48 and 59

Question 156:	Data storage model. The Government's recent public responses note that a future model would need to distinguish between the individual's identity, the credential, the underlying Government records and the technology. To help respondents frame their proposals, does the Government have a preference between a model in which the operator holds a central record of identity data and one in which credentials are held by the individual and verified against authoritative Government records, with minimal personal information retained by the operator?
Answer 156:	Please refer to the responses to Questions 5 and 47

Question 157:	Continuity for individuals. On exit or transition to another operator, is it the Government's intention that individuals should be able to continue using credentials already issued to them, without re-enrolment, and should respondents design for that outcome?
Answer 157:	The RFSQ does not specify exit, transition, or credential portability requirements. Respondents may describe how their proposed solution would support continuity of service, including the ability for individuals to continue using existing credentials without re-enrolment following a transition to another operator. Detailed requirements relating to portability, migration, and transition arrangements, if required, will be addressed in any potential subsequent stage of the procurement process.

Question 158:	Assurance levels. We note that no decision has yet been made on levels of assurance. Would the Government welcome respondents proposing an

	assurance framework mapped to recognised standards, for example NIST SP 800-63 or the UK Good Practice Guides, for the Government's consideration?
Answer 158:	Yes. As no assurance framework or assurance levels have been prescribed at this stage, respondents may propose assurance models aligned with recognised national or international standards, such as NIST SP 800-63, the UK Digital Identity and Attributes Trust Framework, or comparable frameworks. Respondents should clearly explain the proposed approach, its applicability to the Bermuda context, and how it could support a range of Government service assurance requirements.

Question 159:	Relying parties and recognition. Will the Government or the operator be responsible for setting the criteria for onboarding and approving private-sector relying parties, such as banks, insurers and healthcare providers? And does the Government intend to seek recognition of Bermuda credentials under overseas frameworks, to support use by financial institutions in line with the Bermuda Monetary Authority's work on reliance on digital identity for customer due diligence?
Answer 159:	The RFSQ does not specify the governance model for onboarding or approving private-sector relying parties, nor does it identify whether these responsibilities will rest with the Government or the future operator. Respondents may describe proposed approaches for relying-party governance, onboarding, and trust management as part of their solution. The Government has also not specified any requirement for recognition of Bermuda-issued credentials under overseas trust frameworks. However, respondents may describe how their proposed solution supports interoperability with recognised international standards and frameworks, and how it could facilitate future cross-jurisdictional recognition or reliance arrangements if required.

Question 160:	The cover page and timetable state that submissions are due on 27 November 2026 at 10:00 a.m. Bermuda time, but section 1.5.3 refers to opening on 20 November 2026 at 10:00 a.m. Please confirm the correct date and time.

Answer 160:	Please refer to the responses to Questions 30 and 34.

Question 161:	Is there a page limit for the response? What signature and proof-of-authority documents are required for Appendix A, Appendix C, and the response submission?
Answer 161:	The RFSQ does not prescribe a page limit for responses, other than any limits expressly stated in the procurement documents. Respondents should ensure submissions are clear, concise, and sufficiently detailed to address all evaluation requirements. Appendix A, Appendix C, and the response submission should be signed by an individual authorised to bind the respondent. The RFSQ does not specify additional proof-of-authority documentation; however, respondents should ensure that all certifications, declarations, and submissions are executed in accordance with their internal governance and authorisation requirements.

Question 162:	For a joint submission, which forms and supporting documents must be completed by the prime contractor and which must be completed by each consortium member?
Answer 162:	Please refer to the responses to Question 1, 8 and 41.

Question 163:	For the 30% Local Benefits evaluation, how will local benefits be assessed where the prime contractor is Bermudian and a delivery partner is overseas?
Answer 163:	Please refer to the responses to Questions 4 and 10.

Question 164:	Can the ISO/IEC 27001 or equivalent security certification be held by a consortium member or hosting provider? Would SOC 2 Type II be accepted as equivalent?
Answer 164:	Please refer to the responses to Questions 8 and 27.

Question 165:	Must Government data be hosted in Bermuda, or is overseas hosting permitted subject to a Transfer Impact Assessment and PIPA safeguards? Are there restrictions on the countries where data may be hosted or processed, including support access, backups, replication, and other on-island versus off-island activities?
Answer 165:	Please refer to the responses to Question 5.

Question 166:	For Annex B, which requirements are mandatory and which are desirable? Can a respondent indicate partial compliance or explain how a requirement will be met by go-live, and would any response of “No” or partial compliance result in disqualification?
Answer 166:	Unless expressly identified as mandatory in the RFSQ, Annex B requirements should be treated as solution requirements against which respondents will be evaluated. Respondents may indicate partial compliance and should clearly describe any planned future capability, implementation approach, or roadmap to achieve full compliance by go-live. A response of “No” or partial compliance will not automatically result in disqualification unless the requirement is specifically identified as mandatory. However, Annex B requirements that give effect to obligations under the Personal Information Protection Act 2016 (PIPA) cannot be varied by agreement (section 4(5)) and are mandatory: Annex B (Security), Q1.5 and Annex B (Privacy), Q1.1, Q1.2, Q1.3, Q1.4, Q1.5 and Q1.6. Respondents should provide sufficient information to enable the evaluation of any proposed alternative approach or implementation timeline.

Question 167:	Are facial matching and liveness checks mandatory, or are they optional? Would a solution that does not store biometric data be acceptable?
Answer 167:	Please refer to the responses to Questions 47 and 48.

Question 168:	Is a pricing or commercial model required at the RFSQ stage, or will pricing be requested at a later stage?
Answer 168:	Pricing and detailed commercial proposals are not required at the RFSQ stage unless specifically requested in the procurement documents. The purpose of the RFSQ is to assess respondents' qualifications, experience, capabilities, and suitability. Pricing, commercial arrangements, and contractual terms, if required, will be addressed in any potential subsequent stage of the procurement process.

Question 169:	For the production digital identity reference, what scale, recency, and sector are expected? Can the reference be for a solution delivered by a consortium member?
Answer 169:	The RFSQ does not prescribe minimum requirements for the scale, sector, or number of users associated with a production digital identity reference beyond the criteria stated in the procurement documents. Respondents should provide references that demonstrate relevant experience operating a production digital identity, identity assurance, or credentialing solution within the required timeframe. Where a response is submitted by a consortium or team of organisations, references from consortium members may be included, provided the respondent clearly identifies each party's role, responsibilities, and contribution to the referenced implementation and demonstrates how those capabilities will be available to the proposed delivery team.

Question 170:	Can the Government provide estimated user volumes, transaction volumes, and projected growth?

Answer 170:	Please refer to the responses to Questions 70 and 74.

Question 171:	Can information be shared during the qualification period with material third-party suppliers or consultants, in accordance with section 3.5.1, Confidential Information of Government?
Answer 171:	Subject to the requirements of Section 3.5.1, respondents may share Government confidential information with material subcontractors, consortium members, advisers, or consultants where necessary for the preparation of their response, provided that such parties are bound by appropriate confidentiality obligations and the information is used solely for the purposes of the procurement process. Respondents remain responsible for ensuring compliance with all confidentiality requirements set out in the RFSQ.

Question 172:	Could the Government clarify the digital wallet use case referred to in Appendix B?
Answer 172:	Please refer to the responses to Questions 58 and 69.

Question 173:	Which services and functions are expected to be federated? What identification platforms are currently in use, and what standards or mechanisms are used for MFA, tokenization, and related functions?
Answer 173:	Please refer to the response to Question 83.

Question 174:	Given the restricted PKI/encryption standards and current identity-provider information, will there be an opportunity to ask stakeholders questions or exchange information at a roundtable, panel, or meeting before submission?
Answer 174:	The RFSQ does not identify any planned roundtable sessions, workshops, stakeholder meetings, or pre-submission consultation forums. Any additional engagement activities, if considered necessary, will be communicated to all respondents through the formal procurement process.

Question 175:	Is Government seeking a high-level commercial model only, or should respondents also provide directional or budgetary pricing? Given that detailed requirements and solution design remain subject to further definition, would any pricing submitted at this stage be evaluated, and under which published criterion?
Answer 175:	Please refer to the response to Question 168.

Question 176:	If indicative pricing is expected, will Government provide common assumptions for the contract term, implementation phases, user and transaction volumes, and integration scope? Where these are not yet established, should respondents present cost ranges with explicit assumptions rather than a fixed project price?
Answer 176:	Please refer to the response to Question 168.

Question 177:	What level of technical design is expected in the RFSQ response beyond the requested capability evidence and high-level approach? Would a reference architecture, proposed delivery model and clearly identified dependencies be appropriate, with implementation-specific design developed during the subsequent procurement?

Answer 177:	Respondents should provide information appropriate to enable the Government to evaluate their response against the requirements of the RFSQ.

Question 178:	For a joint submission, may the mandatory production Digital Identity reference and comparable project references be provided by named consortium members responsible for the relevant services? Please clarify any experience requirements that the prime contractor must independently satisfy and the evidence needed to establish each member's contribution.
Answer 178:	Please refer to the responses to Questions 1, 3, 8 and 144.

Question 179:	Please clarify the relationship between the preconditions referenced in Section 2.5 and the requirement for an Interim Authority to Operate before contract award. Are shortlisted respondents expected to complete these assessments following prequalification, or only when progressing towards a contract award under the subsequent procurement? What assessment materials or environments are expected at each stage?
Answer 179:	The RFSQ does not specify when the preconditions referenced in Section 2.5 or any Interim Authority to Operate (ATO) activities must be completed. Respondents are not expected to undertake detailed security assessments, certification activities, or provide operational environments at the qualification stage unless expressly requested in the procurement documents. The RFSQ stage is intended to assess capability and capacity to satisfy such requirements. Any formal security assessment, ATO process, testing, evidence requirements, or provision of assessment environments would typically be addressed during any potential subsequent procurement phase and/or prior to contract award. Respondents should describe their experience supporting similar assurance, accreditation, or ATO processes and their ability to provide the necessary documentation, artefacts, and environments when required.

Question 180:	For a solution comprising multiple established components, what system boundary should the independent penetration-test evidence cover? Please clarify the evidence expected at RFSQ submission for the underlying platforms and for integration or configuration work specific to the eventual Bermuda deployment.
Answer 180:	The RFSQ does not prescribe a specific system boundary for independent penetration testing. For solutions comprising multiple components, respondents should provide evidence that is representative of the security assurance practices applied to the relevant platforms, services, and solution components within the proposed architecture. At the RFSQ stage, respondents may provide existing penetration test reports, security assessments, certifications, attestations, or equivalent evidence relating to the underlying platforms and products proposed. Deployment-specific penetration testing, security validation, and assurance activities for integrations, configurations, and the final Bermuda implementation would typically be undertaken during any potential subsequent design and implementation phases. Respondents should describe their approach to security testing and assurance throughout the solution lifecycle.

Question 181:	For the initial work-permit and residents' permit use case, what minimum service outcomes and user groups should respondents assume? In particular, how should the boundary between Digital Identity enablement and existing departmental application, approval and case-management processes be understood?
Answer 181:	Please refer to the responses to Questions, 53,70, 80 and 136.

Question 182:	What information will be made available regarding authoritative Government registers, available interfaces and data readiness? How should respondents allocate responsibility for source-system access, data correction and resolution of conflicting identity or status records when describing their delivery approach?
Answer 182:	For the purposes of the RFSQ, respondents should describe their proposed approach to integrating with authoritative data sources and managing identity

	data. Respondents should clearly identify any assumptions, dependencies, and responsibilities relating to source-system access, data quality, data correction, and the resolution of conflicting identity or status records. Final responsibility allocations and operating model arrangements will be determined during the detailed design and implementation phases.

Question 183:	The RFSQ requires a gap assessment against the UK Digital Identity and Attributes Trust Framework. Which version should respondents use, and how should this assessment relate to the BMA's published digital identity/eKYC consultation materials and subsequent stakeholder communications? Does Government expect the proposed solution to meet particular provisions from those BMA materials? Please identify any provisions that should be treated as mandatory requirements rather than reference guidance for this procurement.
Answer 183:	Please refer to the responses to Questions 60, 126 and 142. The RFSQ also does not prescribe specific requirements derived from the Bermuda Monetary Authority's digital identity, eKYC, or related consultation materials. Such materials should be treated as relevant contextual and reference information. Respondents may describe how their proposed solution aligns with, supports, or could facilitate compliance with any relevant regulatory or supervisory expectations. Unless expressly stated in the RFSQ, no specific provisions from the BMA consultation materials should be treated as mandatory requirements for the purposes of this procurement. Any mandatory legal, regulatory, policy, or trust framework requirements applicable to the solution will be confirmed by the Government through the procurement process.

Question 184:	Beyond the requirements already stated in Annex B, are any mandatory hosting jurisdictions, remote-access restrictions, availability targets or recovery objectives established at this stage? If these will follow the Government-led classification assessment, when will they be made available to respondents?
Answer 184:	Please refer to the response to Question 5.

Question 185:	Please clarify the intended control boundary for Government's administrative authority over the encryption-key lifecycle, including its application to cloud and specialist service providers. What evidence should demonstrate Government-authorised processing and support access while preventing access or decryption without Government authorisation?
Answer 185:	The RFSQ does not prescribe a detailed encryption key governance model or define the precise boundary of Government administrative authority over the key lifecycle. Respondents should describe their proposed approach to key generation, storage, rotation, revocation, recovery, and destruction, including how Government authorisation and oversight would be maintained across any cloud, managed service, or specialist service provider arrangements.

Question 186:	Does the immediate-disposal requirement apply to source identity-document images and their embedded photographs as well as separately captured biometric images or recordings? What verification evidence may be retained for audit, fraud investigation or dispute resolution without conflicting with these requirements?
Answer 186:	Annex B (Biometric Data), Q1.1 requires raw biometric captures to be discarded immediately after template generation. The RFSQ does not specify whether it applies differently to identity-document images or embedded photographs; respondents should note that “biometric information” under section 2 of the Personal Information Protection Act 2016 (PIPA) includes facial images that allow the unique identification of an individual and is sensitive personal information under section 7(1). Respondents should therefore describe their proposed approach to the collection, retention, protection, and disposal of such information, including how it aligns with privacy, security, audit, and fraud prevention requirements. Any retention proposed for audit, fraud investigation or dispute resolution must be identified in the response, with its purpose, duration and safeguards; no retention is approved in advance (see PIPA sections 10, 11, 12(2) and 13).

Question 187:	How should the biometric invalidation and rebinding requirement be evidenced where biometrics are used only for initial identity verification, rather than retained as a reusable authenticator? Please clarify the expected

	distinction between biometric-template compromise controls and recovery or reissuance of the resulting digital credential.
Answer 187:	The RFSQ does not prescribe how the biometric invalidation and rebinding requirement should be implemented where biometrics are used only for one-time identity verification and are not retained as an ongoing authenticator. Respondents should describe their proposed approach to managing biometric compromise scenarios, including any controls for revoking, re-verifying, or re-establishing trust in a user's identity and credentials.

Question 188:	Are specific accessibility standards and minimum assisted or non-biometric service channels prescribed for the initial deployment? What baseline should respondents use for people without a suitable smartphone, supported identity document or ability to complete the standard digital verification journey?
Answer 188:	The RFSQ does not prescribe specific accessibility standards, assisted-service channels, or non-biometric enrolment pathways for the initial deployment. Respondents should describe how their proposed solution supports accessibility, inclusivity, and equitable access for individuals who may be unable to complete a standard digital verification journey.

Question 189:	How should the intended single-provider PPP model be interpreted alongside Section 3.1.8's non-exclusive procurement provisions? Please clarify the intended boundary of the selected supplier's operating responsibility and any implications for the commercial-model assumptions respondents should present.
Answer 189:	The RFSQ does not prescribe a final operating model and does not define how any potential single-provider PPP arrangement would interact with the non-exclusive procurement provisions in Section 3.1.8. Respondents should not assume any exclusivity beyond that expressly stated in the procurement documents.

Question 190:	Please clarify whether the anticipated scope includes the supply, installation and ongoing maintenance of dedicated identity-verification or biometric

	equipment at Government offices or ports of entry, such as fingerprint readers, document readers or enrolment kiosks, or whether respondents should assume verification through standard mobile and web devices. Are any specific biometric methods mandated, and are airport or border-control use cases included in the initial deployment, contemplated for later phases, or outside this procurement? Where physical equipment is envisaged, please indicate whether suppliers would provide new equipment or integrate with existing Government devices, and when the relevant specifications, locations and quantities will be available.
Answer 190:	Please refer to the responses to Questions 47, 59 and 66

Question 191:	For a joint submission (s1.3), may the Digital Identity Production Experience case study (Section C) and the Proven Digital Identity Solution requirement (Section D) be met by a named consortium member or subcontractor, rather than the prime contractor itself?
Answer 191:	Please refer to the responses to Questions 1, 2, 3 and 8.

Question 192:	May the ISO/IEC 27001 requirement (Section D) be met by the consortium member whose certified ISMS covers hosting and operation of the platform? If the prime must hold it, is certification in progress acceptable at RFSQ stage?
Answer 192:	Please refer to the responses to Questions 1 and 8.

Question 193:	Will rated criterion 1 and the three required project references be evaluated on the combined experience of all named consortium members?
Answer 193:	Please refer to the responses in Questions 2 and 8.

Question 194:	For Annex C and rated criterion 7, will Local Benefits be assessed for the prime contractor only or for all consortium members? How is the 30% weighting broken down between its factors?
Answer 194:	Please refer to the responses to Questions 4 and 10.

Question 195:	What evidence is required to demonstrate Specified Business status, e.g. certification by the Bermuda Economic Development Corporation or a self-declaration?
Answer 195:	Evidence may include applicable registration, certification, or other supporting documentation demonstrating eligibility under the relevant Government procurement requirements.

Question 196:	In a joint submission, which documents must each member complete, and which the prime only? What equivalents are accepted from non-Bermuda members for the Certificate of Incumbency and the Social Insurance and Payroll Tax numbers?
Answer 196:	Please refer to the responses to Questions 8, 11, 17 and 26.

Question 197:	Would an exclusive teaming agreement between a prime contractor and a technology subcontractor breach Appendix C(b)? May a technology provider appear in more than one submission?
Answer 197:	Appendix C(b) applies to respondents submitting qualifications and should be read in accordance with the requirements set out in the RFSQ. The RFSQ does not prohibit respondents from using subcontractors or technology providers. A technology provider may participate in more than one submission, provided each submission is prepared and submitted independently and complies with all applicable RFSQ requirements regarding conflicts of interest, confidentiality, and collaboration. Exclusive teaming

	arrangements are a matter for the parties, provided they do not create a breach of the RFSQ requirements.

Question 198:	Section 1.5.1 provides for email submission, while 1.5.3 refers to hard copies and a sealed package opened on 20 November, before the 27 November deadline. Is one electronic copy by email sufficient, and what is the opening date?
Answer 198:	Please refer to the responses to Questions 30 and 34.

Question 199:	May a respondent that is a newly incorporated Bermuda company rely on the staff, experience and certifications of its shareholders? May a shortlisted respondent assign its position to a company it controls before the second stage?
Answer 199:	A respondent may present the experience, qualifications, certifications and resources of affiliated entities, shareholders, consortium members, subcontractors or key personnel where relevant to demonstrating the required capabilities, provided the relationship and proposed role are clearly described in the submission. Any assignment, transfer or substitution of a respondent, consortium member or key delivery entity following submission or shortlisting would be subject to the terms of the RFSQ and any approvals required by the Government. Respondents should identify the entity that will be contracting with the Government and disclose any proposed reliance on related entities in their submission.

Question 200:	For Annex B Biometric Q1.1, does immediate discard of raw captures apply to identity-document images and to liveness captures held for a limited, Government-approved period for fraud investigation?
Answer 200:	Annex B (Biometric Data), Q1.1 should be answered as written: it asks respondents to confirm that raw biometric captures are discarded immediately after template generation, with no retention window.

	Respondents should explain in the comments field any respect in which their solution differs. The RFSQ does not prescribe specific retention periods or exceptions for identity-document images, liveness captures, or fraud-investigation purposes. Respondents should clearly describe any retention, disposal, fraud-management, audit, or evidential arrangements within their response and identify any assumptions or dependencies requiring Government approval. No retention is approved in advance, and any retention must be consistent with sections 10, 11, 12(2) and 13 of the Personal Information Protection Act 2016 (PIPA).

Question 201:	For Annex B Security Q1.7, is a key-management design acceptable in which the Government holds key-administration roles in an HSM/KMS? Does it also apply to credential signing keys?
Answer 201:	Please refer to the responses to Questions 92 and 154.

Question 202:	Pending the classification assessment, should respondents assume hosting in Bermuda, or is hosting in another named jurisdiction, supported by a Transfer Impact Assessment, acceptable in principle?
Answer 202:	Please refer to the response to Question 5.

Question 203:	Where private-sector relying parties use the platform, is the Government expected to be sole controller of identity data, and may the supplier contract directly with those relying parties?
Answer 203:	The RFSQ does not prescribe the future operating, governance, contractual, or data-controller arrangements for private-sector relying parties. Respondents should note that the Personal Information Protection Act 2016 (PIPA) does not provide for a single controller of identity data: each organisation that uses personal information, including a private-sector relying party that receives it, is responsible for its own compliance with PIPA

	(sections 2 and 5), and the Government remains responsible for personal information used by the supplier on its behalf (section 5(3)). Respondents should not assume that the supplier may use identity data for its own purposes, or contract with relying parties on terms that give it independent rights to personal information held for the Government (see Annex B (Privacy), Q1.1). The allocation of responsibilities between the Government, the supplier, and any relying parties will be determined during any potential subsequent phases of the programme. Respondents may describe their proposed operating model, including arrangements for onboarding and supporting relying parties, but should identify any assumptions regarding contractual relationships, data governance, and commercial arrangements.

Question 204:	Given residents will not be charged, does the Government anticipate funding through Government payments, relying-party fees, or both? Is an indicative contract term available?
Answer 204:	Please refer to the response to Question 14.

Question 205:	Can the Government provide the anticipated number of resident users, business users, and government users expected during the initial implementation phase and projected growth over the next five years?
Answer 205:	Please refer to the responses to Questions 70 and 74..

Question 206:	What are the anticipated citizen enrolment and onboarding volumes during the first year of operation?
Answer 206:	Please refer to the responses to Questions 53 and 70.

Question 207:	Can the Government provide an indicative implementation timeline and expected rollout schedule for the Immigration use case?

Answer 207:	Please refer to the responses to Questions 53 and 55.

Question 208:	Will historical immigration and permit records require migration to the proposed solution? If yes, can estimated record volumes be provided?
Answer 208:	Please refer to the response to Question 72.

Question 209:	Can the Government identify the source systems from which identity, immigration, permit, and user data will be migrated and provide an estimate of record volumes per system?
Answer 209:	Please refer to the response to Question 72.

Question 210:	Will the supplier be responsible solely for data migration execution, or is the supplier also expected to perform data cleansing, data remediation, identity deduplication, and data quality improvement activities?
Answer 210:	Please refer to the response to Question 72.

Question 211:	Can the Government provide expected availability targets, Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO) for the platform?
Answer 211:	Please refer to the response Question 76.

Question 212:	What are the expected service level targets for platform availability, response time, and incident resolution?
Answer 212:	The RFSQ does not specify mandatory service level targets for platform availability, response times, incident response, or incident resolution. Respondents should describe their proposed service levels, operational support model, monitoring approach, and service-management capabilities as part of their response. Detailed service level requirements, if applicable, will be established in any potential subsequent procurement, negotiation, or contracting phases.

Question 213:	What is the anticipated contract duration, including implementation and managed-services periods, under the PPP model?
Answer 213:	Please refer to the responses to Questions 14, 62 and 189.

Question 214:	Can the Government provide additional details regarding the proposed PPP operating model, including governance structure, supplier responsibilities, service management obligations, performance expectations, and risk-sharing arrangements?
Answer 214:	Please refer to the responses to Questions 14, 62 and 189.

Question 215:	Can the Government provide additional details regarding the anticipated CNII classification and associated baseline security requirements?
Answer 215:	At this stage, the Government has not completed the information-classification assessment and has not specified the anticipated CNII classification or detailed baseline security requirements. Respondents should describe their security capabilities and proposed controls based on industry good practice and the requirements set out in the RFSQ, identifying any assumptions or dependencies.

Question 216:	Can the Government provide a list of systems, registries, and authoritative data sources that will be integrated with the Digital Identity Platform?
Answer 216:	Please refer to the responses to Questions 52, 67, 72, 77, 84 and 182

Question 217:	Are APIs currently available for the identified systems, or should suppliers assume API development and integration enablement activities?
Answer 217:	Please refer to the response to Questions 54 and 106.

Question 218:	Can the Government clarify the expected scope and deliverables associated with legislative gap analysis, regulatory enablement, and advisory activities under this programme?
Answer 218:	Please refer to the responses to Questions 78, 94, 129, 130, 132, and 133.

Question 219:	Are there mandatory Bermuda data residency requirements for identity, credential, biometric, and audit data?
Answer 219:	Please refer to the responses to Questions 5, 73 and 152.

Question 220:	Will hosting outside Bermuda be permitted if Transfer Impact Assessments and PIPA compliance requirements are satisfied?

Answer 220:	Please refer to the responses to Questions 5, 73 and 152.

Question 221:	Does the Government have an indicative roadmap for legislative and regulatory changes supporting the Digital Identity Programme?
Answer 221:	Please refer to the responses to Questions 55 and 132.

Question 222:	Can the Government provide a high-level inventory of authoritative systems including technology platforms, ownership, and available integration channels (API, ESB, database, file-based, etc.)?
Answer 222:	Please refer to the response to Question 77.

Question 223:	Are there existing digital identity, authentication, citizen portal, or identity proofing solutions currently in use that will require migration, coexistence, or integration during the transition period?
Answer 223:	Please refer to the response to Question 77.

Question 224:	Can the Government provide a high-level overview of the current OSS architecture, including IAM components, authentication and federation standards, user volume estimates, and expected integration requirements between the OSS platform and the proposed National Digital Identity Platform?
Answer 224:	At the RFSQ stage the Government is not providing detailed information regarding the current OSS architecture, IAM components, authentication standards or user volumes. Further information may be provided during any potential subsequent procurement stage.

Question 225:	What are the expected annual transaction volumes for Work Permit and Resident Permit services during the initial implementation phase?
Answer 225:	Please refer to the responses to Questions 53 and 135.

Question 226:	What identity and access management technologies are currently used within the OSS programme and broader Government ecosystem?
Answer 226:	At the RFSQ stage, the Government is not providing details of current IAM technologies, platforms or authentication services. Further information may be provided during any potential subsequent procurement stage.

Question 227:	Does the Government have a preferred technology stack or identity platform already shortlisted for the future procurement phase?
Answer 227:	No preferred technology stack or identity platform has been prescribed or shortlisted by the Government.

Question 228:	What credential types are expected to be issued during the initial implementation phase (e.g., Work Permit, Resident Permit, Identity Credential)?
Answer 228:	The Government has not prescribed the specific credential types to be issued during the initial implementation phase. Respondents may propose credential types and deployment approaches consistent with the objectives of the Digital Identity Programme. The scope and prioritisation of credentials to be issued will be determined by the Government during any potential subsequent project phases.

Question 229:	Is offline credential presentation and verification required for the Digital Wallet solution?
Answer 229:	Please refer to the responses to Questions 52 and 58.

Question 230:	Can the Government confirm that the National Digital Identity Platform is intended to serve as an enterprise-wide identity capability for multiple Government services, with Immigration (Work Permit and Resident Permit services) being the initial implementation use case in Phase 1?
Answer 230:	Please refer to the responses to Questions 74 and 83.

Question 231:	Are references from regulated industries such as banking, telecommunications, and healthcare considered equivalent to government-operated Digital Identity programmes for evaluation purposes?
Answer 231:	References from government and non-government sectors, including regulated industries such as banking, telecommunications, and healthcare, will be evaluated in accordance with the requirements and evaluation criteria set out in the RFSQ. Respondents should demonstrate experience that is relevant to the delivery and operation of digital identity and credential solutions of comparable complexity, scale, and assurance.

Question 232:	What identity assurance levels are expected for citizens, residents, businesses, and government users?
Answer 232:	The Government has not prescribed identity assurance levels for citizens, residents, businesses, or government users. Respondents may propose an assurance framework aligned to recognised standards and appropriate to the intended use cases. Final assurance requirements will be determined by the Government during any potential subsequent phases of the Digital Identity Programme.

Question 233:	Is biometric verification mandatory for all enrolments or only for specified high-assurance user journeys?
Answer 233:	Please refer to the responses to Questions 59 and 66.

Question 234:	What minimum user base, active user population, transaction volumes, service availability targets, and operational maturity criteria will be used to determine whether a deployment qualifies as a national-scale or equivalent Digital Identity implementation?
Answer 234:	The RFSQ does not define minimum user numbers, active-user populations, transaction volumes, service-availability targets, or operational-maturity thresholds for determining whether a deployment qualifies as a national-scale or equivalent digital identity implementation. Respondents should provide examples of relevant production deployments and sufficient information to demonstrate the scale, complexity, and operational maturity of the referenced implementation.

Question 235:	Will certifications such as ISO 27701, SOC 2 Type II, ISO 22301, and CSA STAR be considered additional strengths during evaluation?
Answer 235:	The Government has not identified any specific cybersecurity certifications or accreditations that will attract additional evaluation credit beyond the published qualification and evaluation criteria. Respondents should provide details of relevant certifications, assurance frameworks and security controls held by the organisation or proposed solution, which may be considered as part of the overall assessment of capability, experience and compliance with the Mandatory Technical Requirements - Cybersecurity Certification and Controls.

Question 236:	Can the Government provide the security and compliance framework, assessment methodology, and minimum control requirements that suppliers

	will be expected to satisfy as part of the security review and Authority-to-Operate approval process?
Answer 236:	The Government has not published the security and compliance framework, assessment methodology, or minimum control requirements that will apply to the security review and Authority-to-Operate process. Respondents should address the security requirements set out in the RFSQ and demonstrate their capability to satisfy applicable Government security, privacy, and compliance requirements. Further details will be provided during any potential subsequent procurement and implementation phases.

Question 237:	Will annual penetration testing, vulnerability assessments, security audits, and privacy compliance audits be mandatory throughout the contract term?
Answer 237:	The RFSQ does not specify whether annual penetration testing, vulnerability assessments, security audits, or privacy compliance audits will be mandatory throughout the contract term. Respondents should demonstrate their capability to support ongoing security assurance, testing, monitoring, and compliance activities consistent with Government security, privacy, and operational requirements. Any specific assurance obligations will be defined during any potential subsequent procurement and contracting phases.

Question 238:	Can the Government provide additional details regarding the Local Benefit scoring methodology and scoring bands?
Answer 238:	Please refer to the responses to Questions 10 and 25.

Question 239:	Will knowledge transfer, local skills development, certification programs, and Digital Identity capability-building initiatives be considered part of Local Benefit scoring?
Answer 239:	Please refer to the response to Question 24.

Question 240:	We request that the Government consider extending the RFSQ submission deadline by one week, to 4 December 2026, to allow respondents sufficient time to prepare and submit a comprehensive and fully compliant response. We would appreciate the Government's confirmation of whether this extension can be granted and, if approved, the corresponding amendment to the procurement timetable.
Answer 240:	At this time, the submission deadline remains unchanged. Any amendments to the RFSQ timetable will be communicated to all respondents by formal addendum.

Question 241:	Could the Government please confirm the date on which responses will be opened? Section 1.5.3 indicates that responses will not be opened until Friday November 20, 2026, while the Submission Deadline in Section 1.4.1 is Friday November 27, 2026.
Answer 241:	Please refer to the responses to Questions 30 and 34.

Question 242:	Could the Government please confirm the required submission format? Section 1.5.1 accepts submissions by email, while Section 1.5.3 refers to "0 signed original hard copies" and to a sealed package. Would a single electronic submission by email (PDF/Word, zipped if over 10 MB) fully satisfy the requirements, with no hard copy or sealed package required?
Answer 242:	Please refer to the response to Question 31 and 35.

Question 243:	Could the Government please clarify the expected key management model under Q1.7? In particular, would models in which the provider operates the platform while the Government retains administrative authority over the key lifecycle (e.g., Bring Your Own Key / Hold Your Own Key using Government-controlled HSM or key vault) be considered compliant?
Answer 243:	Please refer to the response to Question 154.

Question 244:	Q1.2 refers to AES-256 for data at rest and in transit. Could the Government please confirm that, for data in transit, the use of TLS 1.2 or higher (preferably TLS 1.3) with cipher suites based on AES-256 or equivalent strength would be considered compliant?
Answer 244:	Yes. For data in transit, the use of TLS 1.2 or higher, including TLS 1.3, with cipher suites providing AES-256 or equivalent cryptographic strength would be considered compliant, provided the overall solution meets the security requirements of the RFSQ and applicable Government security standards.

Question 245:	Could the Government please clarify the scope of Q1.8a (privacy or security breach in the last 3 years)? Should the response cover the responding legal entity only, the proposed platform/solution, or the wider group/network of which the respondent is a member? Could the Government also indicate any materiality threshold?
Answer 245:	For the purposes of Q1.8a, respondents should disclose any relevant privacy or security breaches relating to the responding legal entity and the proposed solution or services to be provided under the Contract. Where the respondent is part of a wider corporate group, any breach that may reasonably be considered material to the respondent's capability, security posture, or proposed solution should also be disclosed. The Government has not prescribed a specific materiality threshold. Respondents should exercise reasonable judgement and provide sufficient information to enable the Government to assess the relevance and impact of any disclosed incident.

Question 246:	"The Supplier shall provide all hardware, software, licences, subscriptions, tools, and supporting components necessary to deliver, operate, and maintain the Bermuda National Digital Identity Platform and associated Digital Wallet solution. This includes all infrastructure, identity management components, integration tools, monitoring solutions, and supporting technologies required for a fully functional production environment. Would the Supplier be required to factor the costs for hardware and software in the Commercials?"

Answer 246:	Please refer to the response to Question 168.

Question 247:	Can the Government provide clarification on whether the "Rectification Period" of 3 business days is intended for technical corrections or for addressing mandatory gaps identified during Stage I evaluation?
Answer 247:	The Rectification Period is intended to allow respondents to address deficiencies, errors, omissions, or non-material irregularities identified by the Government during the evaluation process.

Question 248:	The Government of Bermuda intends to procure a Digital Identity (DI) Platform through a single-provider Public-Private Partnership (PPP) model - will the Government provide a draft framework or template outlining the specific shared responsibilities for long-term risk allocation?
Answer 248:	The Government has not provided a draft PPP framework, risk-allocation model, or responsibility matrix as part of the RFSQ. Respondents should describe their proposed delivery and operating model, including governance, responsibilities, and risk allocation arrangements. Further details regarding contractual and risk-sharing arrangements may be provided during any potential subsequent procurement stages.

Question 249:	"Any contract will not be exclusive. The programme is described as a single-provider PPP. Please confirm whether the final contract will be exclusive, given that the programme is described as a single-provider PPP."
Answer 249:	No. The RFSQ states that any resulting contract will not be exclusive. While the Government currently intends to procure the Digital Identity Platform through a single-provider PPP model, the Government reserves the right to procure related goods and services from other suppliers in accordance with the RFSQ and applicable procurement requirements. The appointment of a single provider under this procurement does not imply exclusivity.

Question 250:	"Delivered through a single-provider PPP. Residents will not be charged for essential services. What payment structure is the Government considering, for example milestone payments, annual service fees, transaction fees or a mix? Is the supplier expected to fund the upfront build costs?"
Answer 250:	Please refer to the responses to Questions 14 and 62.

Question 251:	"The supplier must propose a commercial model that keeps the service sustainable over the long term. Has the Government set an indicative budget or funding envelope for the programme?"
Answer 251:	The Government has not disclosed an indicative budget, funding envelope, or programme value as part of the RFSQ. Respondents should propose a sustainable commercial model in accordance with the requirements of the RFSQ. Any budgetary or funding information that the Government elects to provide will be communicated through the procurement process.

Question 252:	"The contract will include data portability, knowledge transfer, transition support and exit management. What is the expected contract length? At the end of the contract, who will own the platform, software licences and data?"
Answer 252:	Please refer to the response to Question 71.

Question 253:	"The contract will include transition support and Government step-in rights.

	How long will the handover period be at the end of the contract, and will the supplier be paid for exit and transition support?"
Answer 253:	The RFSQ does not specify the duration of any end-of-contract transition or handover period, nor does it state whether transition and exit support will be separately compensated. Details of transition arrangements, supplier obligations, Government step-in rights, and any associated commercial provisions will be addressed in any potential subsequent procurement and contracting stages.

Question 254:	"The top 5 respondents will be shortlisted for a possible second-stage process. What is the expected timeline for the second stage and for contract award? Will shortlisted respondents receive detailed requirements before preparing final proposals?"
Answer 254:	The RFSQ states that up to five respondents may be shortlisted for a any potential subsequent procurement stage. The timeline for any potential second-stage process and contract award has not been specified. Shortlisted respondents will be provided with any further requirements, procurement documentation, and instructions applicable to the next stage of the procurement process.

Question 255:	"Legislative and regulatory changes may be needed. The supplier will assist with legislative gap analysis. If the required laws are delayed, will project timelines and payments be adjusted? Who will carry the risk of such delays?"
Answer 255:	The RFSQ does not specify the treatment of delays arising from legislative or regulatory changes, including any adjustment to project timelines, milestones, or payments. Respondents should identify relevant dependencies, assumptions, and risks within their proposed approach. The allocation of risks associated with legislative, regulatory, or Government approvals will be addressed during any potential subsequent procurement and contracting stages.

Question 256:	In the event of a joint submission, can the experience, references and certifications of all partners be counted, or only those of the prime contractor?
Answer 256:	Please refer to the response to Question 8.

Question 257:	Regarding the requirement for interoperability with "Verifiable Credentials" and "Decentralized Identifiers (DIDs)," does the Government have a preferred standard or ecosystem (e.g., W3C) that it intends to adopt?
Answer 257:	Please refer to the responses to Questions 49 and 106.

Question 258:	What is the expected level of integration with the "One Stop Shop (OSS)" programme?
Answer 258:	Please refer to the responses to Questions 77 and 83.

Question 259:	Will the "authoritative Government registers" (e.g., Immigration, Taxation) provide modern RESTful APIs, or should the solution account for legacy protocols (e.g., SOAP, file-based transfers)?
Answer 259:	Please refer to the response to Question 54. Initially, respondents may assume that integration will be through standard web service interfaces (REST or SOAP). The availability and scope of any Government data source, and the related data-sharing arrangements, will be determined by the Government having regard to PIPA (in particular sections 6, 10 and 11), and responsibility for exposing any interface will be confirmed at any potential subsequent stage.

Question 260:	Given the requirement for "data residency" and "cross-border data transfers," will the Government mandate that all PII (Personally Identifiable Information)

	be hosted on-island in Bermuda, or is a specific sovereign cloud region acceptable?
Answer 260:	Please refer to the responses to Questions 5 and 73.

Question 261:	Regarding "biometric and non-biometric options," does the Government require the storage of raw biometric templates, or is it preferred to use "match-on-device" or "match-on-server" architectures ?
Answer 261:	Please refer to the responses to Questions 47 and 200. The Government does not require the storage of raw biometric captures. Respondents are encouraged to favour match-on-device or encrypted, revocable template architectures that minimise the biometric data held by the supplier (see the response to Question 47).

Question 262:	For the "Digital Wallet" functionality, is the requirement for hardware-backed security (e.g., Secure Enclave/TEE on mobile devices) a mandatory technical specification for the user application?
Answer 262:	Please refer to the responses to Questions 58 and 140.

Question 263:	Will the "independent security assessments" require specific certifications beyond ISO/IEC 27001, such as SOC 2 Type II or specialized penetration testing reports?
Answer 263:	Please refer to the responses to Questions 27 and 87.

Question 264:	Will the "phased implementation approach" require the solution to be backward compatible with legacy identity methods used during the transition period?

Answer 264:	The RFSQ does not specifically require backward compatibility with legacy identity methods during the transition period. Respondents should describe how their proposed phased implementation approach will support migration, coexistence, and continuity of service where legacy systems or processes remain in use.

Question 265:	What are the minimum "service availability" (SLA) targets expected for the production environment,
Answer 265:	The RFSQ does not prescribe minimum service-availability targets for the production environment. Respondents should describe the availability levels, service commitments, resilience measures, and support arrangements associated with their proposed solution. Specific SLA requirements, if any, will be defined by the Government during any potential subsequent procurement and contracting stages.

Question 266:	The section heading refers to “Accessibility Requirements”, but no accessibility requirements are specified. Could the Government confirm the applicable accessibility standard (e.g. WCAG 2.1/2.2 AA) and any other accessibility obligations for the wallet, web portal and enrolment channels?
Answer 266:	The RFSQ does not specify a particular accessibility standard or detailed accessibility requirements for the digital wallet, web portal, or enrolment channels. Respondents should demonstrate how their proposed solution supports recognised accessibility standards and inclusive design principles. Any specific accessibility requirements will be defined by the Government during any potential subsequent procurement or implementation phases.

Question 267:	When will the Government-led information classification assessment be completed? Will its outcome (cryptographic standards, logging and monitoring, RTO/RPO, incident response obligations) be shared with shortlisted respondents before the second stage?

Answer 267:	The Government confirms that the outcome of the information-classification assessment, once completed, will be shared with shortlisted respondents in advance of the Stage 2 evaluation.

Question 268:	Could the Government provide indicative volumes: target enrolled users, annual authentication/verification transactions, number of relying parties per phase, and expected peak concurrency?
Answer 268:	Please refer to the response to Question 70.

Question 269:	Could the Government confirm the target user population? Is it residents only, or also work/resident permit holders, non-residents and legal entities (organisational/business identity)?
Answer 269:	Please refer to the responses to Questions 70, 103 and 234.

Question 270:	For the priority use case (work permits and resident permits), is the scope limited to identity proofing, credential issuance and authentication, or does it also include integration with or changes to the immigration permit application and case management systems?
Answer 270:	Please refer to the responses to Questions 53, 80 and 135

Question 271:	Could the Government share the indicative roadmap of public and private sector services and credentials planned after the immigration use case?
Answer 271:	Please refer to the responses to Questions 55 and 81.

Question 272:	Could the Government confirm the list of authoritative registers in scope per phase, and whether API specifications, data dictionaries and a data-quality assessment will be provided at the second stage? Who is responsible for developing and maintaining interfaces on the source-system side?
Answer 272:	The Government has not provided a definitive list of authoritative registers to be included in scope for each implementation phase. The sequencing and prioritisation of integrations will be determined by the Government as the programme progresses. The RFSQ does not confirm whether API specifications, data dictionaries, or data-quality assessments will be provided during any potential subsequent procurement stage. Any integration documentation made available by the Government will be provided to shortlisted respondents at the appropriate stage of the procurement process. Respondents should identify their assumptions regarding integration responsibilities in their submission. Specific responsibilities for the development, operation, and maintenance of source-system interfaces will be defined during any potential subsequent procurement and contracting stages.

Question 273:	Is any physical credential (ID card/token) or assisted-enrolment hardware (biometric capture devices, document readers, kiosks) in the supplier's scope? If so, how many enrolment locations are expected?
Answer 273:	The RFSQ does not specify whether physical credentials, identity cards, hardware tokens, biometric capture devices, document readers, kiosks, or other assisted-enrolment equipment are within scope. Respondents may identify any assumptions regarding enrolment models, credential formats, and supporting hardware within their submission. The Government has not specified the number or location of enrolment sites expected to participate in the programme. Any detailed enrolment, credential issuance, and deployment requirements will be defined during any potential subsequent procurement and implementation phases.

Question 274:	Must the 24/7 Security Operations Centre and operational support personnel be located in Bermuda, or may these services be delivered from offshore locations, subject to data residency requirements?

Answer 274:	Please see the response to Question 152.

Question 275:	For the UK Digital Identity and Attributes Trust Framework gap assessment, is a solution-level assessment expected, or also recommendations for a Bermuda trust framework (roles, certification, governance)? Is formal certification against the UK DIATF anticipated later?
Answer 275:	Please refer to the responses to Questions 50, 60, 126 and 142.

Question 276:	In general guidelines the request is: "Proponents may provide evidence to support their responses within the comments section or include evidence as appendices to their proposal". Could you please clarify what kind of evidence you would like to receive (e.g. Certain questions, such as Q1.2, appear to seek an explanation of our proposed approach to meeting the relevant requirements. We therefore consider that providing supporting evidence may not be applicable in such cases.) ?
Answer 276:	The Government has not prescribed specific evidence requirements for individual questions. Respondents should provide evidence where it is relevant and available to substantiate their responses, qualifications, certifications, experience, capabilities, references, or compliance claims. For questions that primarily seek a description of the respondent's proposed approach, methodology, or capability, supporting evidence is optional and may not be necessary where the response itself adequately addresses the requirement. Respondents should exercise reasonable judgement regarding the relevance and proportionality of any supporting documentation provided.

Question 277:	Thanks for providing the table which describes the Category and weighting evaluation. Could be possible to share the evaluation guide and principles?
Answer 277:	The Government has provided the evaluation categories and weightings applicable to this RFSQ. The Government has not published a separate

	evaluation guide, scoring methodology, or evaluation principles beyond the information contained within the RFSQ. Responses will be evaluated in accordance with the requirements, criteria, and process set out in the RFSQ. The Government reserves the right to apply its evaluation methodology and assessment procedures in accordance with applicable procurement requirements.

Question 278:	In a joint submission, must the Submission Form, Certificate of Confirmation of Non-Collusion, Certificate of Incorporation and Certificate of Incumbency be provided by the prime contractor only, or by each member?
Answer 278:	Please refer to the responses to Questions 1, 2 and 8.

Question 279:	How should a respondent without a Bermuda presence complete the Social Insurance Number and Payroll Tax Number fields? How will the Section E financial and Registrar of Companies checks apply to such a respondent, and is a Bermuda-registered entity required before contract award?
Answer 279:	Please refer to the response to Question 11.

Question 280:	May the production digital identity experience and ISO/IEC 27001 requirements be met by any member of a joint submission, or must the prime contractor meet them? Is SOC 2 Type II accepted as an equivalent certification?
Answer 280:	Please refer to the responses to Questions 1, 8 and 27.

Question 281:	For a joint submission, are "specified business" status and Bermudian employment assessed on the prime contractor alone or on the whole team, including subcontractors? Should each member complete Annex C?

Answer 281:	Please refer to the responses to Questions 4, 8 and 10.

Question 282:	Given paragraph (b) of Appendix C, may a firm be named as a member or subcontractor in more than one joint submission?
Answer 282:	Please refer to the response to Question 7.

Question 283:	Section 1.5.3 refers to hard copies, a sealed package and opening on 20 November 2026, before the 27 November 2026 Submission Deadline. Please confirm that an email submission alone is acceptable, and confirm the opening date.
Answer 283:	Please refer to the responses to Questions 30, 31, 32 and 35.

Question 284:	Which Government registers are expected to be available at launch for identity proofing and attribute validation, such as immigration, civil registration, passports and social insurance, and will access be by API, batch transfer or another method?
Answer 284:	Please refer to the responses to Questions 54,77,182 and 272.

Question 285:	Will the Government provide in-person or assisted enrolment locations and staff, or should respondents plan to deliver the full enrolment channel, including support for residents without suitable documents or devices?
Answer 285:	Please refer to the responses to Questions 67, 68 and 95.

Question 286:	Is the Government able to share indicative figures for enrolled users, relying parties and annual transaction volumes in the early phases, so that solutions can be sized appropriately?
Answer 286:	Please refer to the response to Question 70.

Question 287:	Which existing Government identity, authentication or access management systems would the platform replace or integrate with, including arrangements supporting the One Stop Shop programme?
Answer 287:	Please refer to the responses to Questions 77, 83 and 84.

Question 288:	We note that the Government will complete an information classification assessment before the next stage. In the meantime, should respondents plan on the Restricted tier indicated on Annex B, and is hosting in approved overseas cloud regions likely to be acceptable, or should on-island hosting be assumed? Relatedly, as Annex B, Security Q1.7 places authority over the encryption key lifecycle with the Government, will the Government operate its own key management or HSM service, or should respondents supply one under Government control?
Answer 288:	Please refer to the response to Question 5, 73, 153 and 154. Annex B is currently marked “Restricted”; see also the response to Question 82.

Question 289:	Since no decision has been taken on biometric identification, how should a respondent whose solution does not depend on biometrics complete the Biometric Data section of Annex B?
Answer 289:	The Government has not mandated the use of biometric identification as part of the proposed solution. Respondents whose solution does not rely on biometrics should complete the Biometric Data section of Annex B by describing their proposed approach and indicating where biometric functionality is not applicable to the solution.

Question 290:	For the purposes of Appendix B, Section D, would a professional or sector-specific credentialing system operated for a public regulator qualify as an “equivalent high-assurance digital credential solution for a regulated industry”?
Answer 290:	A professional or sector-specific credentialing system operated for a public regulator may be considered an equivalent high-assurance digital credential solution for a regulated industry where it demonstrates comparable identity assurance, credential issuance, security, governance, and operational characteristics to those sought under the RFSQ. Respondents should provide sufficient evidence describing the scale, assurance level, regulatory context, and operational performance of the referenced solution to enable the Government to assess its relevance and comparability.

Question 291:	Appendix B, Section B asks respondents to propose a commercial model under which residents are not charged for essential services. May that model include fees from public and private relying parties and optional value-added services, subject to Government approval?
Answer 291:	Please refer to the response to Question 137.

Question 292:	How will the factors within the 30% Local Benefits weighting be weighed against one another, in particular Bermudian ownership and management, the employment and training of Bermudians, the use of local specified businesses, and commitments made for the life of the contract?
Answer 292:	Please refer to the responses to Questions 10 and 25.

Question 293:	In a joint submission, may the prime contractor rely on the qualifications, certifications and references of other members to meet the Mandatory

	Technical Requirements, and will Local Benefits be assessed on the prime alone or on all members?
Answer 293:	Please refer to the responses to Questions 4 and 8.

Question 294:	Section 1.5.3 refers to “0 signed original hard copies” and gives an opening date of 20 November 2026, a week before the 27 November deadline. Could you confirm that one electronic copy sent to mcneale@gov.bm is sufficient, and confirm the correct opening date?
Answer 294:	Please refer to the responses to Questions 31, 32, 35 and 65.

Question 295:	Section 1.1 describes a single-provider partnership, while Section 3.1.8 says any agreement will be non-exclusive. Could you clarify the Government’s position on exclusivity, the expected contract term, and the timetable for the second stage?
Answer 295:	Please refer to the response to Question 249. The timetable for any second-stage process, including issuance of detailed requirements, bidder engagement activities, and contract award, will be communicated to shortlisted respondents following completion of the RFSQ evaluation process.

Question 296:	Does the RFSQ impose any requirements under the Computer Misuse Act 2024?
Answer 296:	Respondents should note that any security incident affecting the proposed solution may engage offences under the Computer Misuse Act 2024, including unauthorised access and unauthorised acts impairing or damaging computer systems. Respondents’ incident response arrangements must support offence recognition, evidence preservation, and timely referral to the National Cybersecurity Incident Response Team (NCIRT) and, where appropriate, the Bermuda Police Service Cybercrime Unit. Respondents

	should describe how their proposed incident response processes would accommodate these obligations.

End of Addenda No, 001