**Instructions:** All Proposers must respond to the following questions by restating the identifying number of each question (for example, 7A.01), restating each question or statement, and providing a detailed written response. The Proposal, at a minimum, must address the items listed below, and be organized in the order indicated below. Include all documents requested in Appendix 7A and label the document provided with the number it replies to. Do not include cost/pricing information in this section of the Proposal. Costs must only be in Appendix 13 – Cost Proposal.

|  |  |
| --- | --- |
| 7A.01 | Provide a full technical architectural overview and system documentation, in both written and visual form (where applicable), of the underlying infrastructure your solution runs on. |
| 7A.02 | Describe how your hosting options support the requirement to host solutions in the continental United States, and whether and how the options can support multiple dispersed locations for business continuity and disaster recovery purposes. |
| 7A.03 | Describe how the solution is designed for High Availability and High Reliability. |
| 7A.04 | Describe the solution's scalability and performance capabilities including how your solution can scale by either increasing or decreasing capacity and resources to maintain consistent performance (including for interfaces), how performance will be measured and reported and how live performance issues are managed. Please also include average/max load times for the user Interface. |
| 7A.05 | Describe how network performance is monitored and how latency and bandwidth issues are resolved to avoid system performance issues with end users, between components of the solution, or with other systems. Indicate how bandwidth is scaled to accommodate application usage growth. |
| 7A.06 | Describe your processes for performing:   Performance modeling. Describe how performance modeling is used to estimate the realistic mix of batch, interact, data integration, application interaction, and other processing types to design a performance test suite that models a representative test suite.   Use of performance testing. Describe how performance testing is not only used to ensure the code in development meets the performance requirements, but also how you leverage the performance information to improve your capacity planning activities.  Describe how proactive capacity planning that is performed before there are predicted changes in usage patterns, such as seasonal variations, product updates, cyclical work, or regulatory changes, is used. |
| 7A.07 | Business Continuity and Disaster Recovery Plans (BCP / DR).   Make available a copy of Proposer’s business continuity plan and redundancy architecture and describe how ETF's system availability goals are supported. This should include a schedule of the review and updating frequency of the proposer’s Business Continuity Plan.  Address the availability of Proposer’s service and its capabilities for data backup, disaster recovery within the organization’s contingency, continuity plan to ensure the recovery and restoration of disrupted cloud services and operations, using alternate services, equipment, and locations, if required. This should also include documentation of the proposer’s notification process, as part of an emergency communications plan, to communicate service level disruptions and recovery expectations to clients.  Describe in detail the disaster recovery capabilities for the solution, recovery plans and the roles played by the vendor and ETF in your plans. |
| 7A.08 | Describe the BCP / DR testing cycle, process, and resulting evidence including how often is it reviewed and tested. |
| 7A.09 | Provide details of your post implementation support approach. When do you usually start working/finalizing the post implementation support plan? |
| 7A.10 | Share details of the Risk Management Reporting Methodology used during implementation and support projects. |
| 7A.11 | Share details of your requirements management methodology during implementation, including how newly discovered requirements and changes to requirements during the project are managed. |
| 7A.12 | Describe Proposer’s ability to provide, manage, and maintain multiple and separate environments (for testing, training, development, etc.). Include details regarding how data is controlled, synchronized (when appropriate), and populated into the various environments. Also include details for code management that impact any external integrations. |
| 7A.13 | Describe the SDLC methodology that is leveraged by your organization to develop the solution and during the implementation for the client. Additionally, please address following:  - Your DevOps practices and how they are integrated into SDLC, including DevOps tools used.  - Details regarding roles ETF staff will have in your methodology. |
| 7A.14 | Describe and provide a copy of the security frameworks, best practices, audit standards, and standardized controls that are a part of the solution. Provide an independent third-party auditors report describing the operational effectiveness of your controls. Where applicable, cite the specification that the solution adheres to and maintains, and the ability of the vendor to provide attestation to the following standards or frameworks.  a. Independent Service Auditor Report [e.g., (SOC) 2] or, Third-Party Audit Assurance Report relevant to the Trust Principles of security, availability, processing integrity, and privacy. b. Health Insurance Portability & Accountability Act c. Federal Risk and Authorization Management Program (FedRAMP) d. Federal Information Processing Standard (FIPS) 140-2 e. Federal Information Security Management Act (FISMA) f. National Institute of Standards and Technology (NIST) 800-53 |
| 7A.15 | Provide the Personally Identifiable Information (PII) and Protected Health Information (PHI) Processing and Transparency Policy, including any related items, that your organization has developed, documented, and disseminated. Specifically, the policy should address:  a. Purpose, scope, roles, responsibilities, management commitment, and compliance  b. Consistency with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines  c. Procedures to facilitate the implementation of the PII processing and transparency policy and the associated controls |
| 7A.16 | How often and under what circumstances do you provide SOC2 type 2 audit reports? ETF expects annually, or upon change in subservice organizations, that vendors submit one of the following to the Department that demonstrates your organization’s oversight of the subservice organizations involved in the delivery of Services under the Contract:  a. Policy and procedure regarding monitoring the compliance of Subservice Organizations handling of Department data; b. Document(s) showing oversight of Contractor’s Subservice Organizations' security posture through annual reviews of Contractor’s vendors’ (e.g., SOC 2, Type 2 audit reports; corrective action plans; annual reviews of information technology controls; or c. Letter of attestation assuming your organization’s full liability for its Subservice Organizations. |
| 7A.17 | Provide a summary of the results of your organization’s most recent independent third-party internal, external and applications vulnerability test. If applicable, provide your corrective action plan to address identified vulnerabilities. |
| 7A.18 | Provide a summary of the results of your organization’s most recent independent third-party penetration test. If applicable, provide your corrective action plan to address identified vulnerabilities. |
| 7A.19 | Provide confirmation that your organization conducts an annual independent security review that assesses the suitability, adequacy, and operational effectiveness of your controls; measuring compliance, risks, identifying mitigating controls, and opportunities for improvement. |
| 7A.20 | Describe what software applications and supporting platform your organization (both in-house and third-party) will use to secure Department and member/participant related records and data. Provide information on how information is secured in transit and at rest. |
| 7A.21 | Describe how two-factor authentication will be employed for accessing confidential information including details of using MFA. Please also describe how you use secondary credentials and MFA before system administrative actions can be taken (i.e. Software installs and product environment access). |
| 7A.22 | Describe the system capability to integrate with ETF’s use of single sign on (SSO) for ETF staff (Microsoft Active Directory), Employers (Microsoft Entra), and Members (Okta). |
| 7A.23 | Describe the security controls that are in place within the system to manage user access. What is the process used to monitor and control access to the system? |
| 7A.24 | Describe the system’s ability to comply with, manage, and maintain industry standard security protocols. Include details regarding how the system handles unauthorized data access or security breaches, locked accounts and the related recovery, encryption protocols, data masking, file imports/exports, etc. |
| 7A.25 | Describe if there have been data related security incidents including the scope of the incident and data loss, how and when it was communicated to clients, measures taken to remediate and prevention in the short term and long term. |
| 7A.26 | Describe the security model of the solution for ensuring customer data security and integrity. Include a description of the security model from the following perspectives: a. Authentication b. Authorization c. Networking d. Data Storage |
| 7A.27 | Describe Proposer’s implementation strategy for segregating sensitive and non-sensitive data including: 1. If distinct infrastructure is used for each how does the Proposer ensures different levels of protection mechanisms and security controls based on the System Data Classification scheme and how updated or new security controls specified by ETF are integrated into the solution. 2. Data Disposition and Removal. Explain how the provider reliably deletes ETF System data upon request or under the terms of the contractual agreement. Describe the evidence that is available after data has been successfully deleted (e.g., CoD). 3. Encryption in Transit. Explain how strong encryption using a robust algorithm with keys of required strength are used for encryption in transmission and in processing per requirements identified in National Institute of Standards and Technology (NIST) 800-53v5. 4. Encryption for Data at Rest. Describe how strong data encryption is applied to all data at rest and in all storage locations. |
| 7A.28 | Describe in detail, how access controls are used to manage various types of users including but not limited to: a. Privileged users b. Administrators c. Standard users d. Researchers e. Non-ETF System users f. Service accounts For non-ETF users ( where “ETF users” are defined as ETF staff, employers, and members), include details regarding who, how often, data and components that are accessed, and frequency. |
| 7A.29 | Describe how user security roles are administered, configured, modified, and  managed for the solution, whether based on role, screen, business unit, etc. |
| 7A.30 | Describe the Secure SDLC (SecOps) principles that are part of the solution's design. |
| 7A.31 | Describe how the solution is tested for application security vulnerabilities that can be found in the Common Weakness Enumeration (CWE) list that may not be easily identified by vulnerability scanners. |
| 7A.32 | Describe how the solutions security model is designed with the ability to facilitate the principal of least-privilege. |
| 7A.33 | Describe your process to:   - Ensure third-party dependencies are maintained and up-to-date, with security relevant updates applied in line with your application patching schedule  - Prioritize efforts upon becoming aware of a Known Exploited Vulnerability affecting a third-party dependency  - Where not possible, how are equivalent mitigations implemented for all components of the application stack |
| 7A.34 | Describe how you support security in your development processes and application lifecycles. Include how you train your developers, implement development guidelines, and leverage modern, maintained and industry-standard frameworks, template languages, tools or libraries to meet your security goals. At a minimum address the following potential vulnerabilities: - Sanitizing and validating input and escaping or encoding outputs of libraries, components, and systems - Authorization bypass — Example: Accessing other customers' data or admin features from a regular account - Insecure session management — Examples: Guessable token; a token stored in an insecure location (e.g. cookie without Secure and Http Only flags set) - Injections — Examples: (No)SQL injection, LLM / Prompt injection, XXE, OS command injection - Cross-site scripting — Examples: Calling insecure JavaScript functions, performing insecure DOM manipulations, echoing back user input into HTML without escaping - Cross-site request forgery — Example: Accepting requests with an Origin header from a different domain - Handling untrusted data — Example: Reusing data supplied by users within sensitive application contexts |
| 7A.35 | Describe the current AI capabilities integrated into your PAS solution. Highlight specific functionalities such as predictive analytics, machine learning algorithms, natural language processing, and automation features. Provide examples of how these capabilities are being utilized in existing implementations. |
| 7A.36 | Outline your roadmap and vision for the future integration of AI technologies into your PAS solution. Discuss planned enhancements, new AI-driven features, and how you foresee AI evolving in your product over the next 3-5 years. |
| 7A.37 | Describe your approach to manage, monitor, and improve data quality over time which includes standardization, validation, metrics, monitoring, cleansing, and reporting. Also include any industry standards that you follow for data formatting and your approach to ensuring data quality during data migration. |
| 7A.38 | Assuming that ETF will provide the data for migration, describe your approach for migrating data with consideration for the SDLC. Please use examples from the Appendix 7D - Data Migration catalog for current state with the understanding that there may be some flexibility in the new pension system with some of the applications listed. |
| 7A.39 | Please describe your system's capabilities to integrate with third-party data cataloging tools. What specific tools do you support for data cataloging, and how does your system facilitate seamless integration? |
| 7A.40 | Provide details of any specific tools and methods your system uses for data validation & cleansing, including third-party integrations (e.g. address validation) and built-in data validations. Include capabilities for the ability for users to configure validation rules and standard set of rules for UI vs. batch validation. |
| 7A.41 | Please describe the high-level reporting architecture, any third-party tools or vendors involved, and any limitations with including large amounts of data in queries or reports. Also include the ability for a user to easily run parameter-based reporting, schedule reports, and run ad hoc queries without specialized technical skills. |
| 7A.42 | What metrics and reporting are available out of the box? What options are there for customization, either by the user or vendor? Please describe the process associated with any custom reports including options for custom reporting needs pre- and post-implementation. Put cost information ONLY in Appendix 13 - Cost Proposal. Tell us the number of reports included in the base PAS cost under Cost Proposal Tab 3, Table 1A. Put cost information about custom reports under Cost Proposal Tab 12 - Rate Schedules in the table titled Extras Rate Schedule. |
| 7A.43 | Can the system deliver full and incremental data feeds to ETF and various partners based on various frequencies (e.g. daily, weekly, monthly) and what data is included (e.g pension, reference/code tables, etc)? Does a standard interface exist with defined levels of aggregation, or would these be custom jobs for ETF? |
| 7A.44 | Describe how your platform/application and internal IT systems have changed/improved over the last 3 to 5 years (response should demonstrate how agile and flexible your organization is with regard to staying current with technology and IT best practices). |
| 7A.45 | Describe your approach for integrating with ETF and external systems through real-time and batch including any standards used, consideration for the SDLC process, and environments available for integrations. Include details regarding API technologies used, any requirements and/or limitations on data that can be shared between systems, the import/export process, timing of interfaces (real-time vs. batch) and any system functionality and actions that can be triggered, accessed, or initiated because of imported data. Please use examples from the Interface Catalog for current state with the understanding that there may be some flexibility in the new pension system with some of the interfaces listed. |
| 7A.46 | Discuss how does your solution architecture facilitates integration with cloud solutions and on-premises solutions to exchange information. |
| 7A.47 | Describe any processing activities in the solution that do not occur in real time, and how these activities are processed, e.g., batch processing, etc., Please include the approach to sharing file transfer interface documentation and to developing data quality agreements for data included in the file. |
| 7A.48 | Describe how the solution co-exists with Master Data Management (MDM) solutions to author and maintain master data (e.g. customer), including any integration with an internal or external CRM. Include the high-level steps needed to implement each integration, the type of integration supported (API, batch), and which system is considered the source of truth. |
| 7A.49 | Describe the Vendor’s security standards related to interfaces. |
| 7A.50 | Describe any requirements and/or limitations regarding data formats and changes to interface file parameters. |
| 7A.51 | Describe the Vendor’s process to ensure and resolve data synchronization issues between PAS and other interfaced systems. |
| 7A.52 | What tools and metrics are available to clients for tracking and reporting application and interface performance monitoring? |
| 7A.53 | Describe how you support resilience in your APIs and across any integration chains or workflows. How do you mitigate data loss when a downstream API is unavailable? How do you manage workflows when a required integration for a step is unavailable? What processes do you have to avoid cascading errors when one part of an integration chain is unavailable but the rest are available? Include how you manage resilience for both synchronous and asynchronous integrations. This question is focused on active, real-time mitigations when one system is up but others (external or not) are unavailable; as such do not include DR/HA strategies. |
| 7A.54 | Describe how you manage security between software components, services, and APIs that must integrate with each other directly. How do you handle machine-to-machine authentication and authorization when there is no specific user/human intervention? " |
| 7A.55 | Describe the system’s ability to enter, track, manage, respond to, resolve and report on customer questions and issues (both usage and technical) through multiple means. Include information (including knowledge base/documents) regarding incident tracking, creation and routing of potential workflows, resolution process, etc. from initial report through to resolution. Please describe the incident and problem management models you support. Also, describe the methodology to triage problem criticality and impact, including resolution procedures and escalation process for each classification of problems and issues.   What flexibility does your system provide for ETF staff, designated third parties and Employers to participate in incident management processes and procedures including, submitting/viewing/tracking incident tickets. Please detail the tools and processes used, including any metrics or KPIs that will be reported to ETF. |
| 7A.56 | How frequently does the system receive upgrade/updates? What is your process for implementing system updates including the versioning strategy and how you deliver major, minor, and patch updates, as well as your expectations of customers as part of the process for items like validation and testing? Include information around the timing and frequency of maintenance updates and product upgrades for the past 3-5 years, along with projected updates/upgrades for the next 3 to 4 years. If several Proposer’ products are used in an integrated solution (such as a PAS, a database, and a CRM product), describe your methods for ensuring the solution will continue to be stable given the update schedules of the various products. |
| 7A.57 | What is the standard turnaround time ETF should expect for the following to implement or resolve: - change requests - standard bug fixes - emergency fixes |
| 7A.58 | Describe the roles and responsibilities that the vendor and the client share in the overall infrastructure and operational security of the solution. Identify the roles that fall solely with the vendor and the roles that fall solely with the client. |
| 7A.59 | Describe the support/maintenance model including the role for both vendor and client for the solution post implementation. If there is a model you provide that works best for most of your clients please indicate why. |
| 7A.60 | Please discuss your pricing methodology for maintenance and support. For example, do you charge by the hour? Does the client purchase blocks of support time? Are upgrades included? DO NOT include any costs in your response to this question. All pricing must ONLY be included in the Cost Proposal. |
| 7A.61 | Describe how product change requests are managed. What is the process for requesting changes to your solution including how it is approved by the vendor and customer? |
| 7A.62 | Indicate and describe the service level agreements (SLAs) associated with the solution. |
| 7A.63 | What is your general approach to warranty and how does your model work? If you typically use a Service Level Agreement (SLA) for warranty please indicate how you do so in your response. |
| 7A.64 | Describe the procedures used when clients transition to other providers when their contracts expire. In the past 12 months, how many customers have terminated this solution or service? How long does it take, on average, for a customer to fully extract data from your solution?  What reporting abilities remain once a customer has terminated the contracts with the vendor? |
| 7A.65 | Can the Proposer guarantee that ETF will receive primary customer support from a staff member thoroughly trained in ETF’s system? Will this staff member be assigned to the PAS project at least three months prior to go-live? Will the Proposer guarantee that this staff member remains ETF’s primary support for at least 18 months after go-live? |
| 7A.66 | Describe the system’s ability to provide internal control functions. Include details regarding available built-in internal controls, such as segregation of duties and transactions that need interim review or approval steps. |
| 7A.67 | Describe the solution's monitoring and auditing capabilities, in terms of business data changes, user activity, history, and exception events including whether both changes to records and read only activities are included in the audit log. Be sure to include the type of information, field or property that would be included in the audit trail. Include details regarding how the integrity of the audit trail data is protected and any limitations on trackable data, sources, time frames, etc. |
| 7A.68 | Describe how and when software audits are conducted and by whom. |
| 7A.69 | Describe Proposer’s overall system architecture. |
| 7A.70 | Describe how your system can be configured to enable business capabilities without the need for custom development. |
| 7A.71 | Describe how you allow customization, configuration, or integration in ways that do not limit the ability to upgrade your solution. |
| 7A.72 | Describe the system’s ability to accommodate user defined fields (UDFs). Include details regarding any limitations or controls on UDFs. |
| 7A.73 | Explain how Proposer handles client requests for product enhancements and how they fit with your overall product roadmap or feature backlog. Talk about Proposer’s system’s customizability vs. configurability related to enhancements. |
| 7A.74 | Describe Proposer’s corporate / business partner strategy for moving new technologies into Proposer’s overall platform. How does the proposer evaluate and decide upon the need for external technologies to provide functional capabilities? |
| 7A.75 | Provide a roadmap for all platform / application enhancements that are planned for the next three years. |
| 7A.76 | Provide any guidelines or documentation that exists for customization of the solution by your customers. |
| 7A.77 | Describe how Proposer’s system optimizes the use of current up-to-date technology. Include details regarding any use of real-time processing, provisional and in-process save features, easily configurable/changeable data field parameters, dashboards, utility and other mass update capabilities, wizard-style guidance for entry screens, performance monitoring protocols, robust search and retrieval functionality, and context sensitive and other types of on-line help resources. |
| 7A.78 | Describe Proposer’s ability to produce, track, and manage on-demand standard correspondence (letters, invoices, enrollment confirmation notices, forms, brochures, other documentation, etc.). Include details regarding tracking and maintaining versioning and multi-lingual content. |
| 7A.79 | Describe system ability to support compliance with ADA/Section 508 of the U.S. Rehabilitation Act and compliance with WCAG AA standards stated in Nondiscrimination on the Basis of Disability; Accessibility of Web Information and Services of State and Local Government Entities (28 CFR Part 35). |
| 7A.80 | Describe the system’s ability to support mail processing and distribution. Include details regarding the types of distribution methods available for individual and mass mailings, compliance with USPS standards for hard-copy mailings, protocol for email and other electronic distribution, etc. |
| 7A.81 | Describe Proposer’s ability to create, update, and manage correspondence content with items such as templates, free form text input fields, auto-population of key account data, signatures, capturing and validating digital signatures to ensure compliance with federal and state laws, and tools and functionality to generate and display content to show estimates, “what-if” scenarios, comparison and other analysis data, etc. |
| 7A.82 | Describe the system’s ability to archive, manage, and retrieve all correspondence and related details. Include details regarding any capabilities to share data with an external document management system or data warehouse. |
| 7A.83 | Explain how your system archives communications at the time of generation and the user steps involved. |
| 7A.84 | Describe Proposer’s ability to electronically generate, manage, and distribute communications related to PAS activities and events. Include details regarding any requirements or limitations related to producing customer-specific on-demand communication in real time; system capabilities to initiate such communication via multiple sources - customer requests, processing or other key activities, events, milestones, etc.; available methods and options for distribution and delivery, etc. |
| 7A.85 | Describe the Proposer’s ability to manage and administer records retention Include details regarding tracking and maintaining record types; applying, updating, and expiring retention periods; flagging and managing exceptions, archiving and/or destroying records with appropriate follow-up/confirmation, etc. |
| 7A.86 | Describe the Proposer’s ability to capture, maintain, and manage a knowledge management-type repository of resources that can be accessed by system users. Include details regarding search and related features and any requirements and/or limitations on the type of resources that can be maintained. |
| 7A.87 | Describe Proposer’s ability to provide context sensitive and other types of on-line help resources. |
| 7A.88 | Explain your approach to ensuring that existing Legacy documents stored in OnBase are accessible to users via the new PAS system under respective business entities (Members/Employers). How will you handle data migration, document indexing, and retrieval to ensure seamless access to historical legacy documents? |
| 7A.89 | Explain the process and technology used for storing and managing documents in PAS. |
| 7A.90 | Describe Proposer’s user interface, including mobile capabilities. Include details regarding differences in user interface capabilities and functionality for different user types (employers, members, administrative users, TPAs, etc.), and the nature of any mobile capability in terms of native vs. hybrid mobile applications, online vs. offline requirements, and mobile responsiveness of web interfaces. |
| 7A.91 | Describe how the user interface enables all interaction techniques and input to be discoverable and chosen from a browse-able, hierarchical structure, arranged in order of the functions the user needs to perform. |
| 7A.92 | Describe how you incorporate UX first design principle as part of your solution, including how intuitive the system is. Also, describe any general population testing conducted against your system and provide major findings from the testing, how remediations were incorporated into the system based on feedback. |
| 7A.93 | Does your PAS include built-in CRM capabilities? If so, please describe the key features and functionalities of the CRM module including various options for viewing/accessing that data. If CRM capabilities are not built-in, what CRM solutions do you support for integration? Please provide details on compatible CRM platforms. |
| 7A.94 | What AI capabilities does your CRM solution offer to enhance customer interactions and operational efficiency? How does the CRM use AI to analyze customer data & interactions and provide actionable insights? |
| 7A.95 | Describe Proposer’s process for business rule collection and confirmation. |
| 7A.96 | Describe the system’s ability to track, manage, and apply multiple classes and versions of business rules. |
| 7A.97 | Describe Proposer’s process for business rule configuration. Include details regarding whether code changes are required, any special skills or expertise needed to configure business rules, etc. |
| 7A.98 | Describe Proposer’s process for managing and deploying business rules, processes, and workflows across multiple environments to ensure consistency and synchronization across all environments. |
| 7A.99 | Describe the system’s ability to conduct business rule-related analyses (e.g., analyze impact across the system of a business rule change; how many and which processes, calculations or eligibility determinations are tied to a given business rule; etc.). |
| 7A.100 | Describe if the proposed system utilizes an industry standard such as the Decision Modeling Notation (DMN) or a structured format (e.g., JSON or XML) to enable export and import of business rules. Describe the solution’s business rules modeling and notation. |
| 7A.101 | Describe how the system enables business rules to retrieve PAS data in a manner that doesn’t degrade system performance. Describe how the data is managed to keep the business rules atomic and independent yet reduces or eliminates the need to repeatedly querying the data. |
| 7A.102 | Described support for developing new business rules (authoring, sandbox, test execution, validation, best practices) and enabling/disabling categories of business rules. |
| 7A.103 | Describe the cloud service models that the proposed solution leverages. |
| 7A.104 | Does the solution have a presence or offering in GovCloud or alternatively is it able to meet the security needs based on controls in place? Describe the controls in place. |
| 7A.105 | Describe the cloud deployment model(s) (Private, Public, Hybrid cloud) that are being proposed for the solution. Describe your ability to integrate with ETF's data lake either on-prem or in the cloud. |
| 7A.106 | If the solution proposed is an IaaS solution, describe the model in which customers control both how they architect and secure their applications as well as securing the data they put on the infrastructure. |
| 7A.107 | If the platform is a multi-tenant environment, describe how customer environments are segregated including the data. If there is a choice between a single and multitenant model, describe the differences between the models. |
| 7A.108 | Describe depth of expertise and experience in offering secure, scalable Cloud services. |
| 7A.109 | As the consumer of your service, we foresee the need to move data into and out from your cloud solution. Describe the portability tools you use and how you provide access to those tools to enable customers to move data on and off their cloud infrastructure if needed. |
| 7A.110 | Describe commercial cloud industry standards and best practices including industry-recognized accreditations and certifications that are employed as part of the offering. |
| 7A.111 | Describe the types of cyber-security insurance you purchase on your own behalf. |
| 7A.112 | Outline the process that enables customers to request deletion of data. This might be done prior to the end of the contract – or at the time the contract expires. |
| 7A.113 | Describe how you enable customers to analyze cloud usage. How does this allow customers to determine how much they are spending? How can alarms, alerts or notifications inform customers that they’re nearing or passing pre-determined cost thresholds? Does your service provide a near-real time dashboard showing utilization and costs? |