|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Cloud Logical System Architecture Review (C-LSAR) Submission** | | | | |
| * Agency: Please complete and return this form to [SAR@tech.nj.gov](mailto:SAR@tech.nj.gov) when ready to request a C-LSAR. * We will respond to your request regarding next steps as soon as your request has been reviewed. * If you have any questions, we are here to help. Please contact: [SAR@tech.nj.gov](mailto:SAR@tech.nj.gov) * If a Technology Initiation Proposal (TIP) review was held: Please update the project’s RECAP Excel spreadsheet that was sent with the TIP meeting notes, indicating status of each action item and include it with your C-LSAR submission. * If a Technology Initiation Proposal (TIP) review was **not** held: Please submit a completed Asset Classification form (provided by the SAR team) along with this C-LSAR. All SAR forms are available on OIT’s website at: <https://nj.gov/it/whatwedo/sar/> | | | | |
| **Contact Information** | | | | |
| **Agency** | *<Agency Name>* | **Date of Request** | *<MM/DD/YYYY>* |
| **Agency CIO** | *<Agency CIO Name>* |  |  |
| **Agency CISO** | *<Agency Chief Information Security Officer Name>* |  |  |
| **Agency Point of Contact** | *<Name/E-Mail/Phone>* |  |  |
| **Vendor Point of Contact** | *<Name/E-Mail/Phone or N/A>* |  |  |
| **Project Information** | | | | |
| **Project Name** | *<Name as indicated on Tactical Plan>* | **Tactical Plan #** | *<999x999999>* |
| **Project Description** | Describe the general purpose and scope of the project: | | | |
| 1. Describe what has happened since the Technology Initiation Proposal (TIP) review meeting: | | | | |
| 2. Status of Action Items from the TIP review (Please update the action items in the project’s RECAP Excel spreadsheet and attach or note updates here): | | | | |
| 3. What is the estimated completion date? | | | | |
| 4. What is the estimated cost for this project, by Fiscal Year (FY)?  Current FY: $  Current FY +1: $  Current FY +2: $ | | | | |
| **System Information** | | | | |
| 5. List all of the cloud providers and services that will be used for this solution:    *NOTE: Include Cloud hosting service, hosting instance, as well as inter-cloud or any identified middleware components or APIs incorporated into the solution/system (e.g. “AWS GovCloud hosted cloud provider that employs Oracle cloud services for authentication, access and data transfer”).* | | | | |
| 6. Select the shared NJ Enterprise Services that will be used by this solution:  Active Directory  e-Payment  Enterprise Data Transfer  Data Warehousing  myNJ Portal  Web Services  Web Service Security  Geographic Info Systems (GIS) | | | | |
| 7. Describe any interfaces with systems hosted on State infrastructure: | | | | |
| 8. Describe and classify any data that is sent to the new solution, or that the new solution will send to an existing State system (e.g. does the solution need to *get data from* or *push data to* any State hosted resource, such as a data warehouse?):    *NOTE: the solution must be secured according to the highest level of data classification.* | | | | |
| 9. Describe how your Agency will ensure that the records/informational content will be accessible and useable throughout their required retention periods:    *NOTE: all cloud providers are contractually obligated to provide all externally hosted state data to be transmitted back to the sponsoring agency in a usable format based on the pre-determined frequency that satisfies the business operational objectives.* | | | | |
| 10. What assistance and/or services are you looking for from OIT for the new solution (e.g. technical design consultation, connectivity and access details/options, etc.)? | | | | |
| **Authentication and User Access** | | | | |
| 11. Who will be accessing this application and by what methods?  State Employees over State Internal Network and if checked, are:  Multiple Agencies involved  State Employees over Public Internet and if checked, are:  Multiple Agencies involved  Private Dedicated Connection to Service Provider (e.g. secure extranet, VPN)  Public Internet Users  Other, explain: | | | | |
| 12. Select the Authentication services needed by this solution:  myNJ Portal Authentication Services  myNJ – Single sign-on (SSO) solution utilizing SAML  myNJ – Premier e-Business Services (PBS) Integration  Directory Services (Specify Active Directory or other, and describe)    *NOTE: If data classification is identified as sensitive, multi-factor authentication must be enabled.* | | | | |
| 13. Will **new** user IDs or roles need to be created to support this solution?  NO  YES If YES**,** explain and identify if these are existing myNJ users: | | | | |
| 14. Describe the various user roles for the solution (e.g. admin vs. regular user): | | | | |
| 15. Describe how State employees and/or vendors will access the system to administer the software: | | | | |
| 16. Describe controls for limiting vendor access for State of NJ User Accounts: | | | | |
| 17. Describe the vendor’s audit trail capability that shows the actions performed by users and the date these actions were performed (e.g. logs that will be available to your agency, access, system, etc.):    *NOTE: Security monitoring in the cloud must be integrated with existing agency and/or NJCCIC security monitoring tools (e.g., API feeds to agency or enterprise SIEM).* | | | | |
| **System Access** | | | | |
| 18. Will this system connect to any outside agency or 3rd party systems?  NO  YES    19. Are new firewall rules needed (Agency/Campus or Enterprise) to allow conversation between servers in different locations?  NO  YES  If YES**,** are these connections within the Garden State Network (GSN)?  YES, please complete and submit the Firewall Request Form      NO, specify what type of connection is being used (Extranet, VPN, etc.):  Policy and required forms for dealing with business entities operating outside of the Garden State Network (click on links below to access forms):  [Business Entity/Extranet Policy](https://www.nj.gov/it/docs/ps/09-11-NJOIT_Business_Entity_IT_Services_andor_Extranet_Policy.pdf)  [Extranet Connection Form (formerly Appendix C)](https://www.nj.gov/it/docs/ps/0145_NJOIT_Extranet_Connection_Form.pdf)  *NOTE: Firewall requests should be initiated through ServiceNow by engaging our Enterprise Service Desk at* [*oit-esd@tech.nj.gov*](mailto:oit-esd@tech.nj.gov)*. Once the forms are completed, they should also be submitted as part of a ServiceNow request.* | | | | |
| 20. Describe how the solution controls access to and from the GSN:    *NOTE: All publicly facing websites shall be protected by web application firewalls (WAFs) that inspect all traffic flowing to the website for common web application attacks.* *OIT currently uses Imperva for the GSN’s standard WAF services. Agencies may use Imperva at no cost. Other WAF services may be used in place of Imperva, if they meet OHSP’s standards. Please contact* [*njccic-waf@cyber.nj.gov*](mailto:njccic-waf@cyber.nj.gov) *for more information*. | | | | |
| **Bandwidth Usage / Business Transaction Volume** | | | | |
| 21. For Cloud hosted solutions that **do** interface with the NJ Shared IT Infrastructure (NJSITI), estimate the average and peak business transaction volumes for this application. Describe the average number of transactions per month and any peak periods for this system (e.g. certain times of the week/month/year when transactions are exceptionally heavy):    22. Indicate the estimated bandwidth usage for this application:  LOW Limited data/usage (e.g. 1-5 users accessing application concurrently without any data transfer activity)  MED Moderate amount of data/usage (e.g. 5+ users accessing application concurrently with data transfer activity)  HIGH Large amount of data/usage (e.g. uploading/downloading large amounts of video and/or data warehouse files)  *NOTE: Agencies are responsible for transportation costs to/from the cloud (OIT is developing a chargeback algorithm)* | | | | |
| 23. Does your contract/agreement with the vendor include the ability to accommodate changes in demand, i.e. to scale the solution up or down?    *NOTE: It is* ***highly recommended*** *that you plan a Pilot Test to verify that the Network Bandwidth usage for your solution falls within acceptable ranges for the capacity of your existing internet connection PRIOR to production deployment.* | | | | |
| **Security** | | | | |
| The New Jersey Office of Homeland Security and Preparedness (OHSP) has implemented an Information Security Vulnerability Management Program into the System Architecture Review process, as part of the overall Agency and System Risk Review managed by OHSP/NJCCIC.  Departments and Agencies must plan and implement the Information Security Vulnerability Management Program into their System Development Life Cycle. Any questions please contact:[riskreview@cyber.nj.gov](mailto:riskreview@cyber.nj.gov)  *NOTE: For PCI (Payment Card Industry) Related Applications: A copy of the vendor’s Attestation of Compliance is required.* | | | | |
| 24. Confirm that your Agency Information Security Officer obtained a copy of your solution provider’s Security Plan and reviewed it:    Please submit a copy of your solution provider’s Security Plan to both OHSP and ISU (OIT’s Information Security Unit), respectively:  To OHSP: [riskreview@cyber.nj.gov](mailto:riskreview@cyber.nj.gov) and to ISU: [OIT.njinfosecure@tech.nj.gov](mailto:OIT.njinfosecure@tech.nj.gov) | | | | |
| 25. Please confirm that your Information Security Officer reviewed this project to ensure compliance with the [Statewide Information Security Manual (SISM)](https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf).    *NOTE: For required signoff form:* [*http://highpoint.state.nj.us/intranets/njccic/resources/2020-iso-sign-off-form.pdf*](http://highpoint.state.nj.us/intranets/njccic/resources/2020-iso-sign-off-form.pdf) | | | | |
| 26. Describe how the solution provider intends to notify you and the appropriate security personnel at the State of NJ (OIT ISU, OHSP) of any and all potential security issues with regards to your hosted solution, as part of normal support operation:    *NOTE: These may include (but are not limited to): DDos (Denial of Service) attacks, Violations of Compliance and Regulatory Norms, Compromised Credentials and Authentication Breaches, Threats to APIs deployed as part of the comprehensive solution, Hijacking of Accounts, Unauthorized or Suspicious Login activity.* | | | | |
| 27. Indicate the data encryption requirements for this application:  ***In Transport:***  Data requires no encryption while in transport  Data needs encryption while in transport over the Internet (SSL) (Browser to web server)  Data needs end-to-end transport encryption  ***In Storage:***  Data does not need to be encrypted in storage (normal database security applies)  Sensitive columns must be encrypted in storage  The entire system requires a secure, separate environment beyond encryption and database & network security | | | | |
| **Data Privacy** | | | | |
| **Please confer with your Agency Privacy Officer to fill in this section. Refer to the following sections in the** **Statewide Information Security Manual (SISM) for further information: (PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY (PT))** | | | | |
| 28. Has an Asset Classification and/or Data Inventory been completed?  YES  NO  If YES, please attach all documents. | | | | |
| 29. Has a Privacy Threshold Analysis (PTA) been performed?  YES  NO  If YES, please attach the PTA. | | | | |
| 30. Did the PTA show that a Privacy Impact Assessment (PIA) is warranted?  YES  NO  If YES, please attach all PIA documents for review by NJCCIC. | | | | |
| **Help Desk/Operational Support** | | | | |
| 31. Do you need Enterprise Service Desk (ESD) Help Desk support for this application?  YES  NO  Please describe any particular needs you have related to help desk support required for this project upon implementation:    **\*All applications require a Knowledge Event Guide (KEG) to ensure proper problem resolution.** Contact the OIT Service Level Management Group at: [OIT-KnowledgeMgmt@tech.nj.gov](mailto:OIT-KnowledgeMgmt@tech.nj.gov) for assistance with the development of the Knowledge Event Guide (KEG), formerly known as the Playbook. If the application does not require OIT monitoring, then a simple profile for the application should be placed on file at the OIT Help Desk. | | | | |
| 32. Describe any monitoring requirements needed to be performed by OIT: | | | | |
| **Disaster Recovery**  **NOTE:** For Cloud hosted solutions that do **not** interface with components currently within the NJ Shared IT Infrastructure (NJSITI), it is recommended that you obtain a copy of your vendor’s Disaster Recovery Solution and contact [OIT-DR@tech.nj.gov](mailto:OIT-DR@tech.nj.gov) to review and ensure that the solution meets your needs and is in accordance with FEMA/NIST standards. | | | | |
| 33. Does this Cloud hosted solution interface with the NJ Shared IT Infrastructure (NJSITI)?  YES  NO  If YES, is the Availability Essential or Critical?  YES  NO  If YES, a Business Impact Assessment (BIA) is required. BIA template can be found online in SimpliGov at:  <https://njoit.prod.simpligov.com/prod/portal/ShowWorkFlow/AnonymousEmbed/cef8ec36-58c3-4381-a881-39066d19e58e>  *NOTE: It is* ***recommended*** *you**contact* [*OIT-DR@tech.nj.gov*](mailto:OIT-DR@tech.nj.gov) *to discuss your Disaster Recovery requirements and build a recovery plan for your system/application. Submission of the BIA does* ***NOT*** *ensure system recovery.* | | | | |
| **Logical Infrastructure Diagram (Mandatory)** | | | | |
| 34. Include a logical infrastructure diagram for this project here, if it is not included in the attached Logical Design documents. Diagram should document all system components, indicating logical elements that currently exist and those proposed for implementation. The diagram should also depict any data that is shared between the cloud provider and the State, showing the direction(s) that the data travels (to and from the cloud provider and the State). For assistance in completing this diagram, your Vendor should provide you with a logical diagram that displays all of the logical components involved in your solution which are not hosted by the State of NJ.  For any questions regarding how the State of NJ infrastructure should be represented in the diagram, please contact the OIT Solutions Architecture team ([SA@tech.nj.gov](mailto:SA@tech.nj.gov)) for assistance. | | | | |
| [Insert your Logical Diagram by clicking in the center of the box below and a dialog box will show up. If you have difficulties inserting your diagram here, please attach a separate file with your submission. (Microsoft Visio Diagram is preferred)] | | | | |

|  |
| --- |
| **Acknowledgement of Risk Acceptance** |
| Understanding the relationships and interdependencies between the different cloud computing deployment models and service models is critical to understanding the operational and security risks involved in cloud computing. The differences in methods and responsibilities for securing different combinations of service and deployment models present a significant challenge for cloud Consumers.  For non NJOIT Enterprise Public Cloud services:  Please be aware that not all services currently provided by OIT will necessarily be duplicated by the cloud service provider once the solution is implemented.  As a consumer of a cloud-based service, it is important for you to ensure that your cloud Provider is compliant with State security and operational guidelines before requesting SAR review.  The Agency should obtain and review the vendor’s System Security and Privacy Plan that outlines the effective controls that either meet or exceed the baseline requirements listed in the **Statewide Information Security Manual (SISM)**.  <https://www.cyber.nj.gov/NJ-Statewide-Information-Security-Manual.pdf>  **Has your Agency's CISO/CIO approved the vendor’s (or NJOIT’s Enterprise Public Cloud) solution?      Yes  No** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Additional considerations as you prepare for this new solution** | | | | | |
| The State of New Jersey is committed to making information accessible to all, including individuals with disabilities. Information and communication technologies should meet or exceed the standards of the Web Content Accessibility Guidelines (WCAG) 2.0.  Follow the **Web Content and Accessibility Guidelines** (WCAG) below (click links to access information):  [W3C Web Content Accessibility Guidelines 2.0](http://www.w3.org/TR/WCAG20/)  [W3C Web Accessibility Initiative Resources](http://www.w3.org/WAI/Resources/#gl)  [Federal Information Technology Accessibility Initiative](http://www.section508.gov/)  Also, please review the NJ Web Presence Guidelines:  <https://www.tech.nj.gov/it/docs/NJ_Web_Presence_Guidelines.pdf> | | | | | |
| Follow the **Records Retention** policy as determined by the Division of Revenue and Enterprise Services (DORES).  Have you included the RMS Records Management Service Levels for Cloud Facilities, which can be found at the following link: <https://www.state.nj.us/treasury/revenue/rms/rms-cloud.shtml> into your agreement with the vendor?  **YES  NO**  If **NO** or for additional information, or for assistance with developing a records management plan, contact DORES RMS at [DorInfo@treas.nj.gov](mailto:DorInfo@treas.nj.gov). | | | | | |
| *NOTE: If a Feasibility Study by the Automated Records Management System Committee (ARMS) was required, please ensure that it was approved.* | | | | | |
| **Next Steps** | | | | | |
| **With regard to the SAR process, at the appropriate time in the process, next steps include:**   1. **Agency** provides information necessary for the Solutions Architecture group to perform a validated design of the solution.  Agency should contact the Solutions Architecture group at: [SA@tech.nj.gov](mailto:SA@tech.nj.gov) for assistance. 2. After the **Solutions Architecture** group has completed the validated design, they will inform the Agency to proceed with the next SAR step.    * the **Agency** is then responsible for:      + completing the Cloud Implementation Review (C-IR) document, including the validated design diagram (mandatory),      + updating the RECAP action item spreadsheet with status,      + accepting changes (revising as necessary) this marked up C-LSAR,      + submitting the preceding three documents to [SAR@tech.nj.gov](mailto:sar@tech.nj.gov) for C-IR review and scheduling.   On an **ongoing** basis, the Agency should:   * follow up on identified action items from all SAR review meetings * document the status/outcomes of action items in the RECAP action item spreadsheet * continue to have the detailed technical discussions that are required to keep the project moving forward toward deployment | | | | | |
| **Please do not write below this line. For OIT Use Only.** | | | | | |
|  | | | | | |
|  | | | | | |
| **Document Receipt and Initial Review:** | | | | | |
| **Received by** | | *<Receiver Name>* | **Date Received** | *<MM/DD/YYYY>* |
|  | |  | **Date Reviewed** | *<MM/DD/YYYY>* |
|  | Proceed to schedule | | | | |
|  | More information needed (return to submitter for resubmission with additional information)  *<Specific additional information being requested will be listed here…>* | | | | |
| **C-LSAR Review Meeting or eReview:** | | | | | |
| **Meeting Facilitator** | | *<Name / eReview - N/A>* | **Date of Review** | *<MM/DD/YYYY>* |
| **Meeting Location** | | *<Online MS Teams / eReview>* | **Time (if meeting)** | *<HH:MM AM>* |
| **Attachments[[1]](#footnote-1)** | | *<Attachments>* |  |  |

1. Attach any additional documents shared for review or reference. [↑](#footnote-ref-1)