

**Office of Information Technology**

**CONCEPTUAL**

**SYSTEM ARCHITECTURE REVIEW**

|  |  |
| --- | --- |
| **Group Name** |       |
| **Project Name** |       |
| **Tactical Planning#** |       |
| **Estimated Start Date** |       |
| **Estimated Completion Date** |       |
| **Document Creator** | Name:      Email:      Phone Number:       |
| **Project Originator** | Name:      Email:      Phone Number:       |
| **Project Manager** | Name:      Email:      Phone Number:       |
| **Date Submitted** |       |
| **CSAR held** |       |

|  |
| --- |
| **ABOUT THIS DOCUMENT** |
| The Conceptual System Architecture Review (CSAR) document is an opportunity for the Office of Information Technology (OIT) to assure that technology solutions for the State are conceived, designed, developed and deployed to maximize the benefits and functionality of the technology, while minimizing costs and risks. The SAR ensures compliance with cybersecurity, architecture standards and best practices, controlled introduction of new technologies, and appropriate reuse of existing technology, in order to increase returns on investment |
| **Purpose** | **Conceptual SAR (CSAR)**:* Allows the OIT business owner to enumerate, document and prioritize the business problem that the project is addressing.
* Ensures that State and/or Federal cybersecurity requirements are understood and classifies the digital assets to be managed in the proposed solution.
* Allows for discussion regarding new technologies and informs the business owner of existing State assets that could possibly be leveraged, as well as considering how the proposed solution might be leveraged by others
* Ensures awareness and support from all operational units and forms the baseline for subsequent reviews
* Ensures that the project aligns with relevant State enterprise IT infrastructure, processes and standards and how that infrastructure might be impacted
* Identifies, at a high level, whether the project might impact IT capacity so that proper planning can take place
* Identifies the costs and risks of certain decisions
 |
| **Important Note:** Before completing the CSAR document, please be sure to complete the Business Innovation Proposal (BIP) template required for OIT projects. The BIP template can be found at: <http://nj.gov/it/services/governance.shtml>The Conceptual SAR is not a “purchase approval” mechanism and no procurement can be made until the appropriate SAR reviews are held. The outcome of the Conceptual SAR is one factor in a purchase decision review. **When a CSAR is needed? Refer to:** <http://nj.gov/it/services/governance.shtml>This document must adhere to the following standard naming convention for the SAR document file.  “Agency Initials-Tactical Plan Number-Project Name-yyyymmdd-SAR Type”.Example: OIT-Project Name-20180120-CSAR |
| **Milestones** | **Conceptual SAR**:  Once the completed documents are received a CSAR meeting is scheduled.* Completion of Business Impact Analysis – if applicable
* Discuss Disaster Recovery requirements with OARS – if applicable
* Begin Certification and Accreditation Form

**Completion of Logical SAR** * Completion of Business Entity/IT Services/Firewall Rules -  Appendices A, B, C, or D – If applicable
* Physical design approval by Network and Information Security areas

**Completion of Physical SAR** * Schedule Vulnerability Assessment Scans
* Schedule and perform Stress Testing
* Completion of Vulnerability Assessment Scans
* Completion of Risk Management Remediation Form – If applicable
* Completion of Certification and Accreditation Form
* Completion of Exception Request Form – If applicable

**Completion of Implementation Review:** 2 weeks before deployment**Deploy to Production** |

1. **BASIC PROJECT INFORMATION**
2. Please provide a detailed description of the project including its purpose, scope and high level business requirements:

1. What problem(s) or untapped opportunity is this project addressing?

1. Is this project a result of legislative mandate?

[ ]  No

[ ]  Yes: [ ]  State Mandate [ ]  Federal Mandate [ ]  Regulatory or Audit Compliance

Please identify compliance requirement, legislative source and reference number:

1. How do you categorize this project:

[ ]  Refresh [ ]  New Build [ ]  Enhancement [ ]  Data Publishing

[ ]  Other:

1. What approaches are you considering for the development of this solution?

(Please check all that apply)

[ ]  Cloud-hosted, (XaaS) X as-a-Service Solution

[ ]  COTS/Packaged Solution

[ ]  COTS/Packaged Solution with Customization

[ ]  Custom, Vendor-developed, Purpose-built Solution

[ ]  Custom, Internally Developed, Purpose-built Solution

[ ]  Extension/Enhancement of Existing Solution

[ ]  Unknown at this time

[ ]  Other

1. What criteria will determine that the project implementation has been successful?

1. Please indicate the possible solutions that have been reviewed and estimated costs for each:

(supporting documentation should be available at review)

|  |  |
| --- | --- |
| **Solution (vendor)** | **Estimated cost.****Indicate out year licensing if known** |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |

1. Identify potential groups involved with development or ongoing support of this project:

|  |  |  |
| --- | --- | --- |
| **Group** | **Development** | **Ongoing support** |
| Application Development (All) | [ ]  | [ ]  |
| Administrative Services | [ ]  | [ ]  |
| Business and Community | [ ]  | [ ]  |
| Health and Social Services | [ ]  | [ ]  |
| Public Safety | [ ]  | [ ]  |
| Workforce Enhancement | [ ]  | [ ]  |
| Architecture | [ ]  | [ ]  |
| Enterprise Data Services | [ ]  | [ ]  |
| GIS | [ ]  | [ ]  |
| Infrastructure |  |  |
| Disaster Recovery | [ ]  | [ ]  |
| Enterprise Services | [ ]  | [ ]  |
| Mainframe | [ ]  | [ ]  |
| Network | [ ]  | [ ]  |
| Storage | [ ]  | [ ]  |
| PMO | [ ]  | [ ]  |
| Security | [ ]  | [ ]  |
| Other:       | [ ]  | [ ]  |

1. **RISK**
2. Is your funding at risk:

 [ ]  No, funding is in place

 [ ]  In Jeopardy Explain:

 [ ]  Not currently funded Explain:

1. Are there licensing, funding, mandates or other constraints that cause the start or end date to be inflexible?

 [ ]  No

 [ ]  Yes Explain:

1. Is your procurement available via a current contract:\

 [ ]  Yes

 [ ]  No Explain:

1. Are your Implementation (human) Resources:

 [ ]  Fully Identified and available

 [ ]  Partially Identified and available

 [ ]  Unknown

1. Is there designated, ongoing financial support for this project:

 [ ]  Yes

 [ ]  Partially

 [ ]  No

1. Is there designated, ongoing human support for this project:

 [ ]  Yes

 [ ]  Partially

 [ ]  No

1. **BUSINESS AND BENEFIT IMPACT**
2. What is the impact if this project is not completed on schedule?

a. How critical is it that this be implemented at this time?
 [ ]  Low [ ]  Medium [ ]  High

b. Is there a financial penalty
 [ ]  No [ ]  Yes, explain:

c. Is an alternate process path available if the schedule is not met?
 [ ]  No [ ]  Yes, explain:

1. Will other Agencies or Departments benefit from this project in any way?

[ ]  No

[ ]  The system has the potential to be scaled for additional users

[ ]  The system will be built to scale for additional known users

1. Time and Cost increase or decrease of this project:
2. Will this project save time; for example, will a former manual task now be automated?
[ ]  Unknown at this time

[ ]  No

[ ]  Yes, how much time will be saved?

How will this time savings be used to benefit the State?

1. Will this project reduce the number of staff/man hours required to support the current solution?

[ ]  Unknown at this time

[ ]  No

[ ]  Yes, how much time will be saved?

1. Will this project reduce current costs?

[ ]  Unknown at this time

[ ]  Yes, What is the current cost for doing these tasks?

What is the anticipated future cost for doing these tasks?

[ ]  No Will this project result in an increase in costs?

[ ]  No

[ ]  Yes What is the anticipated cost increase?

Why is this cost unavoidable?

**Potential for Revenue generation**:

1. Will this project generate any increased revenues for the State, County, Municipality or Local Government after accounting for estimated IT costs?

[ ]  No

[ ]  Unknown at this time

[ ]  Yes How much potential revenue will it generate and for whom?

How was this figure calculated?

|  |
| --- |
| 1. **FUNDING and PROCUREMENTS**
 |

1. Do you have funding for this project? [ ]  No [ ]  Yes

If yes, what is the funding source? [ ]  State [ ]  Federal [ ]  Grant Funding

 [ ]  Other, explain:

If yes, has the funding been allocated? [ ]  Yes [ ]  No

If yes, is the funding source shared, or dedicated? [ ]  Shared [ ]  Dedicated

1. Who is the funding Stakeholder?
2. Are there other funding streams being married to/supporting this project?
3. What is the estimated cost for this project (if known)?

[ ]  0-300,000 [ ]  300,000-1 Million [ ]  1-9 million [ ]  10 million +

Additional comments:

**Identify any anticipated procurements necessary for the project:**

[ ]  **To Be Determined** Explain:

***NOTE:*** *If* ***To Be Determined*** *is selected, this BCR Plan must be updated before the submission of the procurement package.* ***No hardware or software can be procured until a Logical SAR has been held.***

[ ]  **Hardware, or Infrastructure as a Service**

Estimated Hardware Cost: $0.00

PCs: Estimated Quantity:

Servers: Estimated Quantity:

Describe any additional anticipated hardware needs:

Where is the expected hardware installation site?

[ ]  **Software, OR Software as a Service**

Estimated Software Cost: $0.00

Describe anticipated software needs:

Are there annual subscription costs?

[ ]  **Training**

Estimated Training Cost: $0.00

Describe anticipated training needs:

[ ]  **Consulting**

Estimated Consulting Cost: $0.00

Describe anticipated consulting needs:

[ ]  **Other**

Estimated Cost: $0.00

Describe anticipated needs:

1. Has this venture ever been purchased with your operating expenses?

[ ]  No [ ]  Yes, explain:

1. Is Grant Funding being used? [ ]  No [ ]  Yes

How many years out does the grant funding cover?

1. If the identified funding source is removed, are there other funding sources for out-year expenses?

|  |
| --- |
| 1. **INFORMATION SECURITY PLANNING**
 |
| 1. **Asset Classification -** *Classification of the system is used to determine the necessary security safeguards.*
 |
| **Public** | Information that is authorized for release to the public. | **[ ]**  |
| **Secure** | Information that is available to business units and used for official purposes and would not be released to the public unless specifically requested and authorized | **[ ]**  |
| **Sensitive** | Information that is available only to designated personnel and would not be released to the public.Indicate data types:Criminal Investigation **[ ]** Homeland Security **[ ]** FEIN **[ ]** Personal Financial **[ ]**  Personal Medical **[ ]** Social Security # **[ ]** Personally Identifiable **[ ]** Business **[ ]** Other **[ ]**       |
| 1. User Access Controls
 |
|  (a) How do you expect users to access the system? (check all that apply) Public Internet **[ ]** State Intranet **[ ]** Partner Extranet **[ ]**  (b) Will users view or edit sensitive data? No Sensitive Data shown [ ]  View [ ]  Edit [ ]  |
| 1. **Potential Loss Impact:** *For each category below, select the level of impact to that best identifies the protection needed from unauthorized alteration or access to the data, or loss of system access. (*FIPS PUB 199)
 |
| **Security Objective** | **LOW** | **MODERATE** | **HIGH** |
| *Confidentiality*Preserving authorized restrictions on **information access and disclosure**, including means for protecting personal privacy and proprietary information.[44 U.S.C., SEC. 3542] | The unauthorized disclosure of information could be expected to have a **limited adverse** effect on organizational operations, organizational assets, or individuals.  | **[ ]**  | The unauthorized disclosure of information could be expected to have **a serious adverse** effect on organizational operations, organizational assets, or individuals.  | **[ ]**  | The unauthorized disclosure of information could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets, or individuals.  | **[ ]**  |
| *Integrity*Guarding against improper information **modification or destruction**, and includes ensuring information non-repudiation and authenticity.[44 U.S.C., SEC. 3542] | The unauthorized modification or destruction of information could be expected to have a **limited adverse** effecton organizational operations, organizational assets, or individuals.  | **[ ]**  | The unauthorized modification or destruction of information could be expected to have a **serious adverse** effect on organizational operations, organizational assets, or individuals.  | **[ ]**  | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets, or individuals.  | **[ ]**  |
| *Availability*Ensuring **timely and reliable access** to and use of information.[44 U.S.C., SEC. 3542] | The disruption of access to or use of information or an information system could be expected to have a **limited adverse** effect on organizational operations, organizational assets, or individuals.  | **[ ]**  | The disruption of access to or use of information or an information system could be expected to have a **serious adverse** effect on organizational operations, organizational assets, or individuals | **[ ]**  | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets, or individuals.  | **[ ]**  |

**NOTE:** See [130 – Information Asset Classification and Control Standard](http://nj.gov/it/ps/08-04-S1-NJOIT_130-01_Asset_Classification_Control_Standard.pdf) for information on State of New Jersey & Federal Government Information Asset Classification.

1. Is your Availability either Moderate or High? [ ]  No [ ]  Yes

If YES - You **must** complete a Business Impact Analysis.

Once the Business Impact Analysis is completed, please submit the signed form to OIT-DR@tech.nj.gov for review.

*The template for the BIA can be found at* [*http://www.nj.gov/it/services/governance.shtml*](http://www.nj.gov/it/services/governance.shtml)

*In addition, you are required to contact* *OIT-DR@tech.nj.gov* *to discuss your Disaster Recovery requirements and build a recovery plan if your system/application is hosted within an OIT infrastructure.* Submission of the BIA does **NOT** ensure system recovery.

1. **DECLARATION OF ADHERENCE**

## Business Architecture

This project will be consistent with the OIT Business Strategy.

[ ]  **Yes.** A copy of the business plan is attached.

[ ]  **To Be Determined** –be prepared to discuss at the review.

[ ]  **No** Explain:

This project will leverage existing systems/solutions implemented within the State of NJ:

[ ]  **Yes.** Systems exist and we will be taking advantage of them.

[ ]  **To Be Determined** –be prepared to discuss at the review.

[ ]  **No** Explain:

## Technology Architecture

The Project team has reviewed the current New Jersey Shared IT Architecture (<http://www.nj.gov/it/ps/Shared_IT_Architecture.pdf>) documents and will leverage existing solutions:

[ ]  **Yes**

[ ]  **No** Describe the anticipated technology in detail, and provide a justification that includes functionality, cost, and ongoing support comparisons:

Are you avoiding costs by leveraging available shared services?

[ ]  **Yes**

[ ]  **No** Explain:

## Security Architecture

The project team e has reviewed the minimum security requirements policies and standards:
 <http://www.nj.gov/it/ps/14-01-NJOIT_171_Minimum_System_Security_Requirements.pdf>

 <http://www.nj.gov/it/ps/14-13-NJOIT_205_Certification_and_Accreditation.pdf>

[ ]  **Yes**

[ ]  **No** Explain:

|  |  |
| --- | --- |
| stop | Please submit your completed CSAR request to:sar@tech.nj.gov |

The sections following will be completed **during the CSAR meeting** based upon the discussion of the information contained within this document.

**Appendix 1: Authentication Requirements Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potential Impact Categories for Authentication Errors**  | **1**  | **2**  | **3**  | **4**  |
| Inconvenience, distress or damage to standing or reputation where :Low: At worst, limited short-term inconvenience, distress, or embarrassment to any partyModerate: At worst, serious short term or limited long-term inconvenience, distress, or damage to the standing or reputation of any partyHigh: Severe or serious long term inconvenience, distress or damage to the standing or reputation of any party | Low[ ]  | Low-Mod[ ]  | High-Mod[ ]  | High[ ]  |
| Financial loss or agency liability where:Low: At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.Moderate: At worst, a serious unrecoverable financial loss to any party, or a serious agency liability.High: Severe or catastrophic unrecoverable financial loss to any party; or sever or catastrophic agency liability | Low[ ]  | Low-Mod[ ]  | High-Mod[ ]  | High[ ]  |
| Harm to agency programs or public interests where:Low: At worst, a limited adverse effect on organizational operations or assets, or public interests. Example: Mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *noticeably* reduced effectivenessModerate: At worst, a serious adverse effect on organizational operations or assets, or public interests. Example: Significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *significantly* reduced effectivenessHigh: A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Example: Severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions | N/A[ ]  | Low [ ]  | Mod[ ]  | High[ ]  |
| Unauthorized release of sensitive information where:Low: at worst, a limited release of personal, U.S. government sensitive, or commercial sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199Moderate: at worst, a release of personal, U.S. government sensitive, or commercial sensitive information to unauthorized parties resulting in a loss of confidentiality with a moderate impact as defined in FIPS PUB 199High: a release of personal, U.S. government sensitive, or commercial sensitive information to unauthorized parties resulting in a loss of confidentiality with a high impact as defined in FIPS PUB 199 | N/A[ ]  | Low [ ]  | Mod[ ]  | High[ ]  |
| Personal Safety where:Low: at worst, minor injury not requiring medical treatmentModerate: at worst, moderate risk of minor injury or limited risk of injury requiring medical treatmentHigh – a risk of serious injury or death | N/A[ ]  | N/A[ ]  | Low[ ]  | Mod orHigh[ ]  |
| Civil or criminal violations where:Low: At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement effortsModerate: At worst, a risk of civil or criminal violations that may be subject to enforcement effortsHigh: A risk of civil or criminal violations that are of specific importance to enforcement programs. | N/A[ ]  | Low [ ]  | Mod[ ]  | High[ ]  |

Based on the determinations above, the level of assurance needed for user access and authentication is determined to be:

|  |  |
| --- | --- |
| [ ]  | **Level 1**: No identity proofing – Little or no confidence exists in the asserted identity. |
| [ ]  | **Level 2**: Identity Information is collected. On balance, confidence exists that the asserted identity is accurate. |
| [ ]  | **Level 3**: Identity information is collected and verified. Appropriate for transactions needing high confidence in the asserted identity’s accuracy. |
| [ ]  | **Level 4**: Identity information is collected in person and verified. Appropriate for transactions needing very high confidence in the asserted identity’s accuracy. |



**Signature of Project Team reviewers:**

|  |  |
| --- | --- |
| CIO |       |
| DCIO |       |
| COO |       |
| COS |       |
| DCTO |       |
|       |       |
|       |       |
|       |       |
|       |       |