njoit

SAR FAQs

Last Update August 11, 2016

What is the purpose, and more importantly the value of the Architecture Review Process?

The System Architecture Review, or SAR, is intended 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.

Participation in the SAR process informs:

- Cybersecurity and privacy requirements
- Cross-Agency interoperability of systems
- Data sharing and reuse
- Opportunities to leverage economies of scale and/or existing solutions
- Impact on existing technology infrastructure and operations
- Prioritization of resources staff levels
- Disaster recovery & business continuity requirements

When is a SAR needed?

A SAR is needed if:

1. A new solution is being developed. Solutions include:
   - Custom development software applications
   - Procurement of a Commercial off the Shelf (COTS) Package
   - An "As A Service" solution will be utilized, including, but not limited to, Software (SaaS), Platform (PaaS) or Infrastructure (IaaS)
   - New hardware that will integrate with the Garden State Network
   - New hardware to be installed at any of the State Enterprise Data Centers
2. A significant enhancement or modification is being made to an existing solution. Enhancements/Modification examples include, but are not limited to:
   - Addition, modification or removal of enterprise functionality such as e-mail, e-payment, myNJ Portal, or reporting functionality
   - Addition, modification or removal of application specific functionality such as adding/removing a server call, adding/removing web service call
   - Extranet or firewall changes
   - Database platform changes
3. A system has been previously reviewed by the SAR group, but post-review changes have been made to the application design
4. A vendor solicitation (e.g., Requests for Proposal, Quotation, Information) with an Infrastructure Technology requirement is generated
5. When in doubt, fill it out. SAR surveys are reviewed before a meeting is scheduled. Based on your responses it may be decided that you don't need to appear at a normally scheduled meeting, but rather have a smaller meeting, an e-mail or phone discussion.

At what point in my development process should I fill out a SAR survey?

The SAR is a multi-phase Integration Planning Process consisting of 4 distinct review points that are held at various stages of the project lifecycle. Templates exist for each of the review points and must be submitted for each of the review points to occur. These templates will help capture the information needed within each phase.

1. **Conceptual**: Held before an RFP or RFQ has been generated, before a vendor or product has been finalized, and after the department or agency has internally approved its business case for moving forward. The Conceptual review:
   a. Allows the business owner to enumerate, document and prioritize the business problem that the project is addressing.
   b. Ensures that State and/or Federal cybersecurity requirements are understood and classifies the digital assets to be managed in the proposed solution.
   c. 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
   d. Ensures awareness and support from all operational units and forms the baseline for subsequent reviews
   e. Ensures that the project aligns with relevant State enterprise IT infrastructure, processes and standards and how that infrastructure might be impacted
   f. Identifies, at a high level, whether the project might impact IT capacity so that proper planning can take place
   g. Identifies the costs and risks of certain decisions**.**

   This review will be attended by:
   - Agency business owner/sponsor
   - Agency CIO
   - OIT Deputy CTO, Affinity Group aligned to the agency
   - OIT Deputy CTO, Architecture
   - OIT Chief Data Officer
   - OIT Information Security Officer
   - OIT Project Management Office
   - OHSP Statewide Office of Information Security

2. **Logical**: Held before any hardware or software has been procured or installed; after an RFP or RFQ has been awarded, and before any coding is begun. The Logical review:
   a. Ensures that capacity, resources, hardware and software needs are identified
   b. Ensures that infrastructure requirements are defined
   c. Reaffirms that cybersecurity requirements are defined
   d. Identifies, at the technical level, any existing systems that are impacted and may require change
   e. Identifies, at the technical level, the costs and risks of certain decisions and any remediation required

   This review will be attended by:
   - Agency business owner/sponsor
   - Project Manager
   - Deputy CTO, Affinity Group aligned to the agency or affiliated OIT manager
   - OIT Project Management Office
   - OIT Architecture
   - Subject Matter Expert(s) as needed and determined by the OIT Deputy CTO, Architecture

3. **Physical**: Held once a validated production architecture design has been produced. The Physical review:
   a. Ensures that the capacity, resources, hardware and software required for production deployment, including backup and disaster recovery, have been identified and approved

b. Ensures that cybersecurity requirements have been followed

This review will be attended by:

- Agency business owner/sponsor
- Project Manager
- Deputy CTO, Affinity Group aligned to the agency or affiliated OIT manager
- OIT Project Management Office
- OIT Architecture
- Subject Matter Expert(s) as needed and determined by the OIT Deputy CTO, Architecture

4. **Implementation**: Held no less than two weeks before go-live of any phase
   a. Determines whether the project is ready for deployment – all outstanding action items must be resolved or remediated
   b. Assures that all cybersecurity requirements have been successfully concluded
   c. Assures that the date for deployment, impact on other systems and related deployment activities have been assigned and agreed to

This review will be distributed to:

- Agency business owner/sponsor
- Project Manager
- Deputy CTO, Affinity Group aligned to the agency or affiliated OIT manager
- OIT Project Management Office
- OIT Architecture
- Subject Matter Expert(s) as needed and determined by the OIT Deputy CTO, Architecture

Where do I find blank documents?

The current Conceptual, Logical, Physical SAR and Implementation Review Templates can be found on the NJ IT website at https://www.nj.gov/it/whatwedo/sar/.

Where do I send the completed SAR?

Completed documents (in Microsoft Word format) should be submitted to OIT-Sarlist@tech.nj.gov for scheduling. Any update submitted should identify the reason(s) for resubmission. Unless requested by the OIT Affinity Group Deputy CTO, or the OIT Deputy CTO, Architecture, only one phase of SAR (Conceptual, Logical, Physical, Implementation) should be submitted at a time. The OIT-Sarlist@tech.nj.gov e-mail address can also be used for any questions regarding completion of the document.

What happens next?

Conceptual SARs are held on Monday afternoons. Logical and Physical SAR meetings are held on the 2nd and 4th Thursdays of each month. Your submitted SAR documents will be processed and you will be notified when and where the next meeting is held. The Implementation Review document must be submitted at least 2 weeks prior to the anticipated deployment date. An **ON-LINE** review will be completed within one week of that submission and a "Can Go" notice will be sent to the Project Leader after the submission has been determined to be complete.

Reference for CSAR section General Project Technology

Information Asset Classification

State of New Jersey – IT Circular 130 – Information Asset Classification Control Policy requires all departments and agencies take responsibility to protect the confidentiality, integrity, and availability of information generated, accessed, modified, transmitted, stored or used by the Executive Branch of New Jersey State Government, irrespective of the electronic or digital medium on which the information resides and regardless of format. All departments and agencies must be aware of, determine classification of, and maintain an inventory of all information assets of which they are either Owners or Stewards according to the Information Asset Classification and Control standard and procedures.

Federal Government – the Federal Information Processing Standard (FIPS) 199 requires that information assets be classified as High-Impact, Moderate-Impact or Low-Impact in terms of the risk to their confidentiality, availability and integrity. Your assessment of these dimensions will be used to develop recommendations for the appropriate technical solution.

In General, a higher Confidentiality, Integrity or Availability designation increases the cost to build the application, increases the cost of the infrastructure to host the application, increases the cost to maintain the application and reduces the performance of the application.