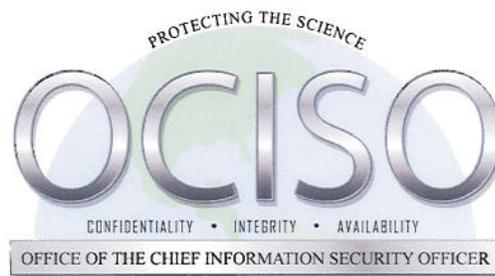


**U.S. Department of Health and Human Services
Centers for Disease Control and Prevention**

**OCISO Standard for the
Bridge Accreditation Approach, Version 3.0**



Submitted to Tom Madden, CISO
DHHS/CDC/CIO/OCISO
4770 Buford Highway K-81
Atlanta, GA 30329

Approved: 
6/29/07

Version Control

Date	Author	Versions	Notes
02/13/2006	NCPHI	1.0 – 2.3	
06/29/2007	OCISO Policy and Planning Team	3.0	Reformatted as the bridge accreditation approach

Contents

Bridge Accreditation Process Summary	4
1. Determine Required Changes	4
2. Create Bridge Plan	5
3. Implement Bridge Plan	7
4. Retire Old System and Complete Full or Modified C&A	8
Appendix A: Bridge Accreditation Process Steps.....	9
Appendix B: Bridge Accreditation Process Flow.....	10
Appendix C: Frequently Asked Questions (FAQs).....	11

Bridge Accreditation Process Summary

At the discretion of the CDC CISO, the bridge accreditation process may allow program owners to transition systems from one operating state or environment to another without losing their accreditation and without denying service for clients that are currently using the original system. This process is only permitted under rare and compelling conditions, and is generally used for transitioning a currently-accredited system into a new operating state or a new logical or physical environment. *The bridge process is an exception to the normal C&A procedure and its use is limited to cases that match its specific criteria. Once a system is approved for the bridge process, the process must be strictly followed.*

During the bridge process, the existing, currently-accredited system is being transitioned and does not change, except at the disposal phase.

The use of the bridge plan must be justified and must have CISO approval. OCISO reserves the right to audit any changes implemented in the course of the bridge accreditation. This may include, but is not limited to:

- Requests for production of documentation created to fulfill certification requirements in the course of risk mitigation (such as a Business Continuity Plan, an Incident Response Plan, or a Rules of Behavior document)
- Performance of a security test and evaluation (ST&E) to analyze the effects of implementing any bridge change
- Post-implementation review of change risk assessments by an OCISO analyst

Application of the OCISO bridge accreditation process may allow a system or application to temporarily operate absent full implementation of normally required conditions necessary for adequate protection of the system and information interests supported. In such a case four distinct phases must be strictly followed to transition the applicable system or application into a fully protected system or application as follows:

1. Determine the required changes from the current information system and the drivers that support both the change and the need for a bridge accreditation rather than a normal C&A.
2. Create a bridge plan that includes the following artifacts:
 - a. Statement of business need and drivers for bridge accreditation
 - b. Transition plan to fully protected state or environment
 - c. Project schedule for transition
 - d. Estimated security risk for transition and for each incremental change
3. Implement the bridge plan by defining each change as a series of incremental changes or steps, performing risk assessments to ensure that the security impact of the changes are known and within the original level of acceptable risk, and documenting the changes as they occur.
4. Complete a full Certification & Accreditation.

The information contained in this document and the flow chart (attached as Appendix B) explain the steps in each phase and the decision points at which it is possible to leave the bridge accreditation process in favor of a full Certification and Accreditation or a Change Risk Assessment (CRA).

It should be noted that the CDC National Center for Public Health Informatics (NCPHI) authored the initial versions of the *Bridge Accreditation Approach*.

1. Determining Required Changes

a. State drivers for the change

Drivers can be expressed as a requirement to which the system must conform.

System changes may have up to three types of drivers: technical, business, and security. Some example drivers might be: *current application cannot process data from new feed; 24x7 support is necessary to meet new SLAs; upcoming release of client software cannot process current authentication parameters; current location does not meet required physical security controls.*

b. Describe the current system state

The current system state is the documented technical, business, and security posture of the system, and is static in nature.

c. Describe the future system state

Desired system criteria are expressed in terms of requirements that the system should meet, including the desired future technical, business, and security posture of the system.

d. Determine delta between current state and future state

The delta is expressed as the difference between what the current system can provide and the requirements to meet the identified system drivers. Significant changes, such as overall system security rating change based on the information categorization, must be stated explicitly.

e. Determine that the system's future state requires bridge accreditation

A bridge accreditation is designed to allow an information system to continue in an active state while a new system is being built to meet its future state in support of expanded or new business goals. The bridge accreditation exists while the two systems run simultaneously, or until all services provided by the original system are provided by the new system and the old system is retired.

The bridge accreditation is specific to systems that cannot make required changes in the normal change risk assessment process. Examples of historical justifications for bridge accreditation include:

- i. The change requires old and new systems to be in production simultaneously
- ii. The change cannot be performed in an alternative fashion:

1. Change invalidates ATO
2. Not possible in current environment
3. Scope of related/dependant changes too broad for CRA
4. Changes take place over an extended period of time (not to exceed one year)
5. The change requires more resources (worker hours, time, money) to perform in another fashion

2. Create Bridge Plan

Once a determination is made that a bridge accreditation is necessary, the requesting system personnel shall document a plan to build the new system and to transition from the old system to the new system. This plan must detail measures in the new system to satisfy the drivers for change.

a. Determine steps in the implementation of the change

State the changes in broad steps that show how each change satisfies the system drivers. Technical detail should be omitted, except where necessary to explain the change's relationship to the drivers. (For example: a business driver does not need to be expressed in technical detail. A technical or security driver, on the other hand, may need to be expressed in technical detail.)

b. Order steps based on dependencies and timeframe

Once necessary changes are determined, they should be ordered or modified to include dependencies for their implementation. This includes both dependant and supporting information systems for the one undergoing bridge accreditation. These dependencies will impact the schedule and timeframe for the planned change.

The bridge accreditation period is determined by the ISSO and CISO, based upon the project schedule outlined in the bridge accreditation plan. This period includes: availability of system's new state in production, the necessary time to move processing services from the old system to the new system, and proper completion of C&A activities. In no case will this period be longer than one year.

If the original ATO period would normally end during the transition, this must be explicitly included in the bridge accreditation plan. The bridge accreditation should not be seen as a work-around for an expiring ATO.

c. Estimate security risk for each step and overall change

Examples of control changes that can incur additional security risks can include, but are not limited to: changes to communication ports, applications, untested hot site, removal of tape backup schedule, etc.

d. Create documentation to justify and describe a bridge plan to the ISSO and to the CISO

A bridge plan should contain the following elements:

- i. Information about current system state
 - a. Current ATO expiration date
 - b. Open POA&M items, including milestone dates and whether the future system will reduce or eliminate the open items (See Appendix C, FAQ #3)
- ii. Statement of business need and drivers for bridge accreditation
- iii. Information about future system state
- iv. Transition plan to new state
- v. Project schedule for transition (Schedule must include milestones, with dates and details)
- vi. Estimated security risk for transition and for each incremental change
- vii. Description of disposal phase of original system
- viii. Bridge plan approval signatures (DAA/Business, Technical and Security Stewards sign off on the plan before the plan is negotiated between the ISSO and CA)

e. Negotiate Bridge Plan with OCISO

Once the ISSO is satisfied with the bridge plan, he or she should set up an appointment with the CISO to discuss a plan for a bridge accreditation. The program's goals in that interview are to:

- i. Gain approval for use of bridge process
The bridge accreditation is available solely at the discretion of the CDC's CISO.
- ii. Negotiate check-in points for the process:
 1. Time-based - For example: every 60 days, the business steward will update OCISO on progress and changes, and the project plan timeline will be reviewed for adherence to the scheduled milestone dates
 2. Risk-based - For example, if any change has a security risk that is moderate or higher, the ISSO will obtain approval from the CISO before the change takes place. The acceptable level of risk is the "high water mark" to which this document refers

3. Security Tests & Evaluation – The CISO may also require the inclusion of a schedule for ST&Es in the bridge accreditation plan
- iii. Determine actions to be taken when milestones are not met due to driver issues (Technical, Security, or Business). A standard procedure for this would be:
 - a. Identify when a milestone date is not going to be met
 - b. Declare the reasons and remedies along with an amended date

The approved bridge accreditation plan should be incorporated into the SDLC and/or existing change management process. Delays causing the bridge accreditation schedule to extend beyond the one-year Bridge Accreditation ATO period are to be avoided. If the Bridge Accreditation lapses, neither system will have a valid ATO and the system will undergo immediate steps for C&A recertification as currently deployed. Changes to the system will be frozen until recertification is achieved. After system recertification, a new bridge plan will have to be submitted and negotiated.

3. Implement Bridge Plan

a. Define parameters for each incremental change

The incremental changes or steps should be defined in technical and business terms. The parameters you define should describe the hardware, software, application changes, environment changes, and data changes that will take place to meet the drivers for the change.

b. Write change risk assessment (CRA) for each incremental change

- i. Determine weaknesses introduced by each change. Risk analysis should include a review of the system requirements in FIPS 199, NIST SP 800-53 Revision 1, and NIST SP 800-63, but it is not limited to only those risks. Other common factors such as software vulnerabilities, server processing power, firewall and virus protection, and software compatibility should also be included in the evaluation
- ii. Suggest mitigations appropriate to the system security requirements based upon FIPS 199, NIST SP 800-53 Revision 1, and NIST SP 800-63, as well as good security practices
- iii. Document any deviations this change or related mitigations cause from the original bridge plan

c. Submit CRA for incremental change

The CRA should be submitted to the Business Steward and Technical Steward as normal. After approval, the CRA should go to the ISSO. If the change is at

or under the pre-negotiated risk level, the change does not need further approval, but the CISO must be informed that the change has taken place. If the change is above the pre-negotiated risk level, the CRA must be approved by the CISO and the Designated Approval Authority (DAA).

d. Determine aggregate risk for all changes so far

Aggregate risk is determined by ensuring that no changes together incur higher risk than each separately. This should be a rare occurrence, as each CRA takes into account the preceding risk assessments. In the case that the security steward or ISSO determines a higher level of aggregate risk based on a combination of changes:

- i. If risk is higher than the accepted risk level from the C&A process, the program must determine and implement additional mitigations
- ii. If risk is not above the high water mark, the program may continue without additional mitigations or implement additional mitigations

An ST&E may be conducted at the discretion of the Certifying Authority to ensure that the estimate of aggregate risk is accurate

e. Execute incremental changes

After risk has been explained and accepted, the incremental changes can be made. These changes should be handled with the care of any other production changes, and they should be documented for inclusion in new security documents.

f. Document deviations from the change plan made during execution

Any changes from the implementation plan must be noted so that any resulting documentation and subsequent changes do not introduce unexpected vulnerabilities.

4. Retire Old System and Complete Full or Modified C&A

Once the bridge accreditation period is complete and the system is fully migrated to the future state, the old system must be retired and the new system must complete a C&A.

Appendix A: Bridge Accreditation Process Steps

1. Determine Required Changes

- a. State drivers for the change
- b. Describe the current system state
- c. Describe the future system state
- d. Determine delta between current state and future state
- e. Determine that the system's future state requires bridge accreditation
 - i. The change requires old and new systems to be in production simultaneously
 - ii. The change cannot be performed in an alternative fashion:
 1. Change invalidates ATO
 2. Not possible in current environment
 3. Scope of related/dependant changes too broad for CRA
 4. Changes take place over an extended period of time
 5. The change costs more resources (worker hours, time, money) to perform in another fashion

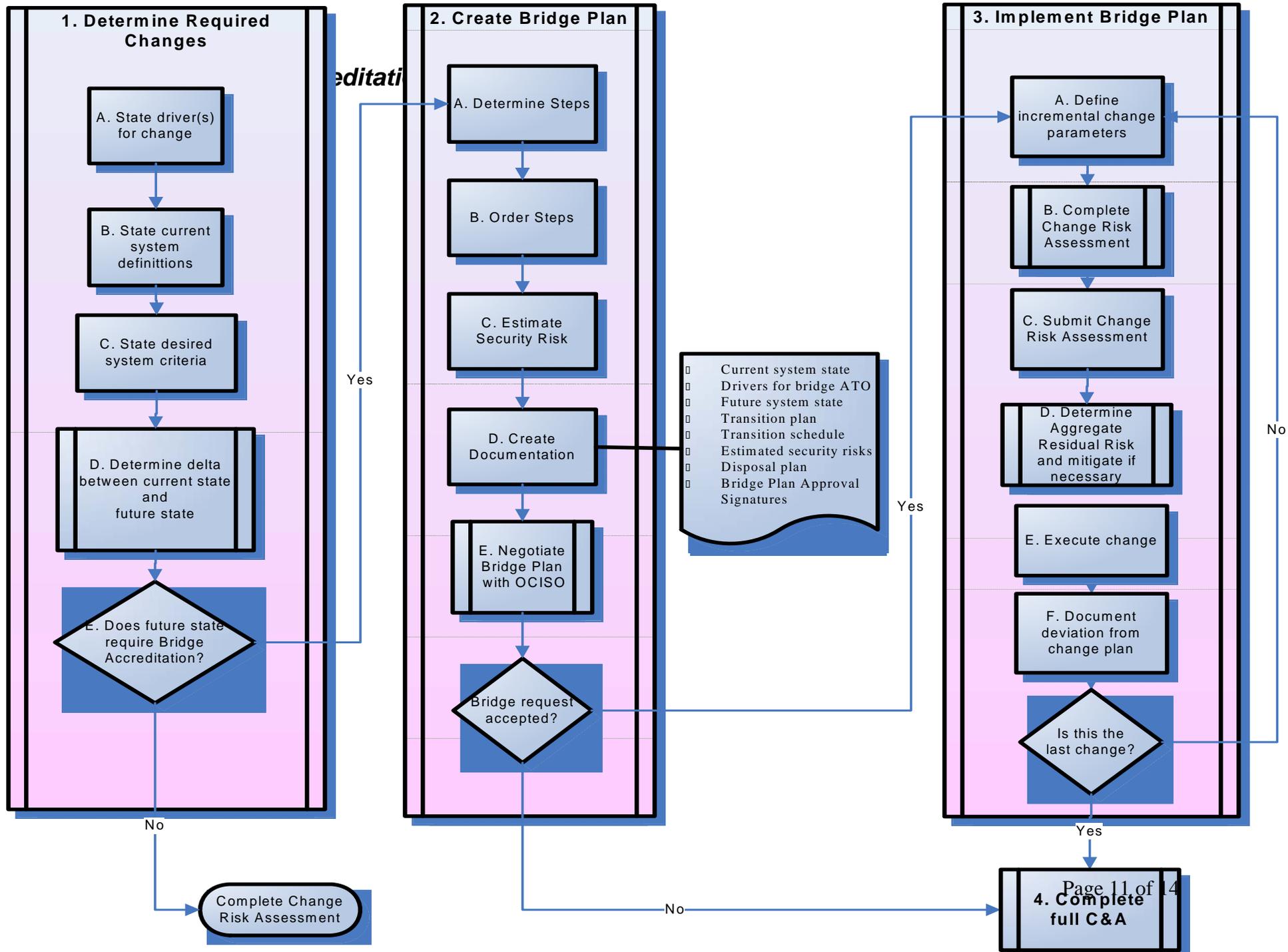
2. Create Bridge Plan

- a. Determine steps in the implementation of the change
- b. Order steps based on dependencies and timeframe
- c. Estimate security risk for each step and overall change
- d. Create documentation to justify and describe plan to ISSO & CISO
 - i. Information about current system state:
 1. Current ATO expiration date
 2. Open POA&M items, including milestone dates and whether the future system will reduce or eliminate the open items
 - ii. Statement of business need and drivers for bridge accreditation
 - iii. Information about future system state
 - iv. Transition plan to new state
 - v. Project schedule for transition (The plan must include milestones, with dates and details.)
 - vi. Estimated security risk for transition and for each incremental change
 - vii. Description disposal phase of original system
 - viii. Bridge plan approval signatures (Technical/Security/Business/DAA sign off on the plan before the plan is negotiated with the CA.)
- e. Negotiate Bridge Plan with OCISO
 - i. Gain approval for use of bridge process
 - ii. Negotiate check-in points for the process:
 1. Time-based
 2. Risk-based
 3. ST&E schedule
 - iii. Determine actions to be taken when milestones are not met due to driver issues:
 1. Identify when a milestone date is not going to be met.
 2. Declare the reasons and remedies along with an amended date

3. Implement Bridge Plan

- a. Define parameters for each incremental change
- b. Write change risk assessment (CRA) for each incremental change
 - i. Determine weaknesses introduced by each change
 - ii. Suggest mitigations appropriate to the system security requirements based upon FIPS 199, NIST SP 800-53 Revision 1, NIST SP 800-63, and other security requirements.
 - iii. Document any deviations this change or related mitigations cause from the original bridge plan
- c. Submit CRA for incremental change
- d. Determine aggregate risk for all changes so far
 - i. If risk is above the high water mark, determine additional mitigations
 - ii. If risk is not above the high water mark, continue without additional mitigations
 - iii. Conduct ST&E (at OCISO's discretion)
- e. Execute incremental changes
- f. Document deviations from change plan made during execution

4. Retire Old System and Complete Full or Modified C&A



Appendix C: Frequently Asked Questions (FAQs)

1. What is the role of the center's Information Systems Security Officer (ISSO) in Bridge Accreditation?
 2. What is aggregate risk?
 3. What happens to my active Plan of Action & Milestones during Bridge Accreditation?
-

1. What is the role of the center's Information Systems Security Officer (ISSO) in Bridge Accreditation?

The center's ISSO plays a central role in the planning, development, acceptance, and execution of the bridge accreditation plan. The responsibilities of the ISSO include, but are not limited to:

- Working with the program to ensure that the system is a viable candidate for bridge accreditation
- Assessing security risk associated with incremental changes and the bridge transition plan
- Reviewing associated documentation and milestones to ensure that the plan is complete
- Presenting the bridge accreditation plan to the CISO. In this meeting, the ISSO will answer questions about the plan and negotiate changes to the plan on behalf of, or in concert with, the system stewards
- Reviewing and/or performing incremental change requests and suggesting appropriate mitigations for risks above the acceptable level
- Approving change risk assessments at or below the approved level of risk and requesting approval for risks that will not be mitigated to the approved level of risk
- Assessing change requests for aggregate risk
- Scheduling and attending progress meetings with the CISO
- Reviewing deviations for the original plan with the CISO

2. What is aggregate risk?

Aggregate risk occurs when multiple actions taken together create more risk than each taken separately. A simplistic example would be in-place hardware maintenance of a server located next to a datacenter window and a scheduled pressure-washing of the windows on that floor:

- Open-case server maintenance may be a low or moderate risk
- Pressure-washing windows for a data center is low risk
- Pressure-washing a window near an open server creates a high-risk scenario: The integrity of the window glazing is all that protects the server from water that might leak into the building around the window

If the two tasks were scheduled separately, there is no reason to rate either a high risk scenario. When the server maintenance and pressure-washing take place at the same time, however, it becomes clear that extra precautions must be taken, such as moving the server to another location for maintenance or covering the window's interior with a plastic tarp.

A more complex and realistic example can be illustrated with software packages in use at CDC:

- The installation of MySQL is usually a low or moderate risk if the servers are appropriately patched and correctly configured
- The installation of Rhapsody Orion, a data brokering software, could also be rated a low or moderate risk, assuming appropriate controls
- The risk of using these products together is "HIGH"; the Rhapsody product can become unstable if its backend is MySQL

If the project plan contains both of these items but the project team has no knowledge that there is a performance issue with the combination of MySQL and Rhapsody, the planners would rate each change low or moderate risk. That lower risk would be reflected in the bridge accreditation plan that was approved by the ISSO and CISO. However, the above example shows that the lower risk originally projected is no longer accurate, and new mitigations (such as a move to MS SQL) should be implemented to reduce risk to the original acceptable level.

3. What happens to my active Plan of Action & Milestones during Bridge Accreditation?

Many systems have an active Plan of Action & Milestones (POA&M). Tasks assigned within POA&Ms must be accounted for when creating plans for Bridge Accreditation. Depending on the plan for old & new systems, there are several approaches to meet POA&M obligations. The path taken would require agreement between OCISO, the center ISSO, and the system stewards. Scenarios 1 & 2 are examples of cooperative, productive approaches for different situations.

Scenario 1:

New and old systems run concurrently for a year.

- New system: The bridge accreditation plan should articulate milestones that obviate or demonstrate mitigation of the POA&M items
- Old system: POA&M items should be mitigated as the program had previously committed to do. If the old system is to be decommissioned prior to the negotiated remediation date, then the decommissioning should be an appropriate mitigator

Scenario 2:

The new system will take the place of the old system, and no concurrent processing occurs. In this scenario, unresolved POA&M items should be applied to the new system, since the old system will be shut down.

- New system: The bridge accreditation plan should articulate milestones that obviate or demonstrate mitigation of the POA&M items
- Old system: Immediate decommissioning of the old system is an appropriate mitigator for any open POA&M items

If POA&M mitigation return on investment is significantly lowered by the bridge accreditation, then it should explicitly be revisited during the presentation of the bridge plan. For example, the return on a low risk's mitigation which requires hundreds of thousands of dollars and six months to implement would be significantly lowered if the old system were to be decommissioned in eight months. In this case, all involved parties might choose to accept the risk for the eight months that the system would still run.

Although these examples demonstrate appropriate methods of handling live POA&M items, any agreement between OCISO, the center ISSO, and the system stewards would be equally acceptable.