

10 Tips for Cutting Certification and Accreditation (C&A) Costs

Bruce M. Szabo
EADS NA Defense Security and Systems Solutions Inc.
28 March 2007

1. Ensure your staff is adequately trained.

Within most organizations, the personnel that conduct certification and accreditation activities and tasks have many other job related duties and responsibilities that they perform on a daily basis. Often, their involvement with C&A activities is one of their least frequently performed task areas. Tasks and deliverables associated with C&A are highly technical, prescribed by ever-evolving guidance and take considerable time and effort to successfully perform. Therefore, one of the best cost saving approaches is to ensure up front that the participating C&A team members have a solid understanding of the regulatory guidance and the prescribed C&A process.

It's important to determine if the team members have ever received formal training or if there may be a need for some form of refresher training prior to beginning the C&A project. Are there training resources within the organization that can provide effective C&A training or should consideration be given to training organizations that regularly conduct C&A activities? Is there a need to find a training provider offering certified curriculum that may be required to meet regulatory guidance? Is it more cost effective to send the C&A team to a training provider's location or bring the training to the organizational location?

Most organizations have incredibly talented personnel conducting C&A activities, but without ensuring they fully understand current guidance, tasks and deliverables, they will be unable to perform in the most efficient and cost effective manner. There are many C&A training providers with curriculum targeted towards compliance with a wide range of regulatory guidance and C&A processes. A little research will help you find a training provider that utilizes instructors who are also highly experienced in conducting C&A activities. The benefits of this will be readily apparent when your team has specific questions about current guidance, processes or tasks during their training. While Computer Based Training is a viable option for providing some types of training, it is not always the most effective when it comes to more technical matters and applications.

2. Assess your current workload.

Conducting any certification and accreditation process is not an inexpensive venture in terms of resource utilization. It typically involves several staff personnel, takes a significant amount of time to complete and comes with a suspense date that hovers somewhere between attainable and optimistic. An initial assessment of the current workload of the staff and the anticipated scope of the C&A effort will be beneficial in determining whether it can all be done in the prescribed time with existing resources.

In smaller organizations, the information assurance staff conducting the C&A activities and tasks are likely to be the same limited but talented IT staff that support a myriad of IT services including system administration, help desk support, incident response, etc. Can the staff continue to execute those critical and business sensitive support processes and still dedicate the resources to complete the C&A effort within the prescribed timeframe? What are the costs to the organization if supporting the normal day to day activities are cut back or response time is decreased? What is the impact if the C&A is not conducted within the allocated time? Will it be more cost effective to secure assistance outside the organization to conduct some of the C&A process?

In larger organizations, there may be a staff dedicated to C&A and other IT security support. In this case, the focus should be more on the number of systems that require C&A support over the near term and prioritizing the efforts. Can the staff complete all currently scheduled C&A projects in the allotted time? Can the schedules for some efforts be slipped without a significant impact?

3. Establish and utilize an effective C&A Team.

Completing the C&A process in a timely and cost effective manner requires the involvement of a team of personnel with a variety of organizational roles, responsibilities and skill sets. Meeting the C&A process requirements, eliminating or mitigating risk and ensuring you can successfully field the system requires commitment and participation by a multidisciplinary team regardless of whether the key personnel are organizational resources or are contracted to assist.

The team should include the functional program manager or members who possess the key information needed to adequately describe the functionality of the system. The team should also be able to identify the key financial data, identify interfaces and any memorandum of agreements, determine classification of the system and detailed system information that will be necessary in documenting the C&A process or in registration of the system if required. Key system administrators, database managers and other technical support staff will be required to address the elimination or mitigation of any vulnerabilities or risks identified during the risk assessment process.

Bringing the entire team together at the start of the project and involving them in the planning, scheduling and progress reviews will not only help get buy-in, but will also help with identifying any potential pitfalls or delays that may have a negative impact on the overall cost of the project. It will also educate the team in the C&A process and applicable security requirements and help reduce future C&A costs by ensuring the requisite security features are planned as an integral part of any new acquisitions or system upgrades.

4. Develop an executable schedule.

A detailed project plan provides scalable framework, highlights the big picture and identifies executable milestones, tasks and deliverables to assist you with keeping the

project on track. It should include key project information such as estimated costs, contract or project numbers, key personnel, milestones, specific tasks and deliverables, responsible individuals or offices for each task and deliverable as well as targeted and actual completion dates. The schedule will also provide insight into significant changes in resource allocation, periods which you may not be able to totally control timelines due to tasks such as documentation reviews by personnel or offices external to the day to day C&A effort, conduct of internal or external scans, or execution of fix or mitigation actions identified during the process.

The schedule will provide the most benefit if it's drafted in as much detail as possible during the very early stages of the project. This helps identify key participants and activity levels and may provide additional insight into the make-up of your C&A team. The schedule should then be reviewed by the C&A team and updated throughout the project as changes occur. The benefits beyond the obvious ones of monitoring progress and keeping things on track, is that a completed schedule can also serve as a reliable tool for forecasting the level of effort and costs for future C&A efforts.

5. Conduct monthly progress reviews.

Monthly progress reviews provide a valuable vehicle to document recent and overall progress, identify problems experienced or anticipated, identify the need for additional resources, make or recommend adjustments to the project schedule and provide yet another tool to assist with the planning or forecasting of future projects and costs. Monthly progress reviews may be conducted through meetings, documented by meeting minutes or simply be a written monthly progress report with input derived from the participating team members.

Documentation of the progress reviews provides an avenue for higher management level review and oversight without the need of their active participation in the project. The greatest benefit of team participation in the monthly progress reviews is that it brings a variety of experience and perspectives to the project and enhances the ability to identify potential project pitfalls and process improvement suggestions rather than relying solely on the guidance and oversight of a project manager. It is also an invaluable learning experience for team members as they more actively share in the experiences and perspectives of other team members. What they individually and collectively learn may be transferred to future projects and represent additional cost savings for the organization.

6. Keep abreast of changes in guidance.

Chances are, if you're following the same guidance you followed for previous certification and accreditation efforts, you're most likely following obsolete or significantly changed guidance. If your baseline requirements are driven by public law, NIST guidance, OMB circulars, etc. it is important to verify the currency of the respective guidance in the early stages of your C&A process. Failure to do that may have a significant negative impact on the validity and reliability of your assessment and may require much of the work to be re-accomplished. Obviously, those potential results come

with an additional cost in resources and may be exacerbated by the frustrations of personnel involved in the project or management personnel.

If you're conducting C&A activities within the DoD, you'll need to stay current in not only any changes to public law and NIST guidance but also in the current implementation guidance for DIACAP which has replaced DITSCAP as the C&A process. The DoD is continuing to refine their implementation guidance and the component service guidance is continually evolving and emerging as well. If you're not keeping current with the changes in guidance as well as the base-line and component-specific IA controls and validation methodologies, the months you spend completing the C&A process may prove far less than productive when you finally submit your package through the certifying authority to the DAA. The costs associated with any compliance shortfalls at this point not only relate to wasted resources on work accomplished to date, but also to the additional unplanned work and subsequent impact to other projects for which the C&A participants may be responsible.

7. Keep focused on satisfying requirements or validation of IA controls.

The accreditation determination will ultimately be based on compliance with the applicable IT security requirements or Information Assurance (IA) controls. Identification of the applicable requirements and controls will occur in the beginning stages of any C&A process and will be the focus of the security test and evaluation or validation tasks. There is often a significant lapse in time between the identification and testing/validation tasks, with a myriad of other information gathering and documentation related tasks occurring during that time period.

While all of the tasks and deliverables of the C&A process are important, satisfying the security requirements and controls will generally have the biggest impact on cost, particularly if they were not fully integrated into the system in the developmental stages and continuously maintained as the requirements and controls changed or new ones were introduced. The C&A team should continuously focus on ensuring the system meets security requirements and controls in order to ensure the timely identification of risk and vulnerabilities as well as any corrective or mitigation actions.

Assessment of the requirements and controls early in the process will provide the much needed lead time necessary to respond to any requirements or controls which are not currently being met before entering the final testing/validation activities. Failure to keep focused on satisfying the requirements and controls throughout the process can often lead to costly project delays and the need to utilize additional unplanned resources to ensure a positive outcome.

8. Assess the costs of fix versus mitigation actions.

In ideal situations, the prescribed or applicable security requirements and IA controls are integrated into the system during the planning and developmental stages. In fact, within some organizations (DoD in particular) there are IT acquisition guidelines that require

exactly that. Unfortunately and historically, this guidance has not always been followed and functional organizations often find themselves in situations where they have forecasted and executed significant system acquisition funds and later learn that the system contains unacceptable risk and vulnerabilities which adversely impact the ability to implement or field the system.

Structured C&A processes generally provide some latitude in determining whether a risk or vulnerability must be corrected or may be acceptably mitigated in some manner (often through policy). The choice to correct or mitigate often comes down to availability of funding and other resources, but the choice often affects the ultimate decision on whether to fully accredit the system or to recommend an interim approval of some sort. The first consideration in this regard should obviously be the residual risk to the system or enterprise as reducing that risk is the ultimate goal of performing C&A.

When making resource based decisions on whether to immediately correct or mitigate a particular risk or vulnerability, it is important to weigh immediate against long term costs. If you decide to move forward with a policy-related mitigation action, will personnel completely comply with the policy until a permanent corrective action can be implemented? What risks will be posed to the system if the policy is not followed? Will the costs associated with accepting an interim approval to utilize the system, developing and executing a Plan of Action and Milestones, re-testing and validation and documentation changes at some future point (when the cost of living may further increase the costs) outweigh the cost of correcting the risk or vulnerability now? These are important considerations that face a program manager or system owner and should be given their due.

9. Conduct a post project review.

One important aspect of C&A projects that is often overlooked is ensuring you make the time to conduct a post project review. One of the basic laws of learning often referred to as the Law of Recency, indicates that things most recently learned are best remembered. With this in mind, the review should ideally occur within a week of project completion while the project is still fresh in the minds of the project participants. When conducting the review, you should include the key project participants and utilize the project schedule or plan as a guideline for your review. This will assist you in ensuring all important aspects of the projects are reviewed. The lessons learned from such a review can be very beneficial in future project budgeting, including identification of resources and potential cost efficiencies.

According to *Bart Perkins at Leverage Partners, Inc.*, “Post project reviews enable organizations to acknowledge (and maximize) their strengths, address their weaknesses and brainstorm improvements. Properly conducted, PPRs leverage valuable project experience to enhance future IT delivery capability.”

10. Determine potential cost savings in contracting C&A support.

Large organizations will often have the resources available to satisfy their certification and accreditation needs, but often find themselves in situations where new system acquisitions or changes increase the workload beyond what they can reasonably handle in the time allowed. Smaller organizations with far fewer systems or networks often struggle the balancing act between conducting required certification and accreditation and the conduct of day to day IT security responsibilities. Vendors desiring to market their applications to organizations with regulatory guidance covering IT acquisitions often find themselves with a product that has great functionality and that they believe to be secure, yet are unable to make the sale without incurring or negotiating the costs associated with ensuring the application will stand up to the scrutiny of a formal C&A process.

In the aforementioned situations, it's important for an organization to carefully consider whether it has the existing resources with the necessary skills and experience to conduct the C&A activities and tasks or whether they should consider contracting the support services to an experienced provider. When deciding whether it's more cost efficient to secure external assistance, how do you cull through the vast numbers of companies offering C&A support services? How do you separate the companies that specialize in C&A support services from those that may perform other IT support tasks and simply hang an additional shingle for C&A support? Can you easily find a vendor that will provide ample evidence of extensive successful past performance and customer satisfaction? If your organization is located in a high cost area, is it more cost effective to utilize a local service provider or are there highly experience companies that can balance limited travel and conducting much of the work at their secure facilities at a significantly reduced cost? Can the C&A provider you select provide individualized or formal classroom instruction in the applicable C&A process (and that may require certified curriculum) to help educate your staff, increase efficiency and reduce costs for future C&A efforts?

Resource costs for conducting C&A are far from minimal, regardless of whether the C&A tasks and activities are conducted using internal or external resources. Considering the 10 areas should provide some assistance with helping to minimize your costs and in making your business case decisions.

EADS NA Defense Security and Systems Solutions Inc. does not find it in our best interest nor that of our customers to require contact information prior to allowing visitors to our website to download white papers or similar publications. We retain full rights to the contents of any white papers we produce and will gladly entertain requests for re-use of the material. Please feel free to contact us if you would like any additional information about the content of this or any other white paper on our site.