

Year 2000 Certification

Air Force Tenets to Success

Thomas V. Ashton

U.S. Air Force Year 2000 Program Management Office

Certification of your systems is key to surviving year 2000 problems but cannot guarantee success. Certification by definition can add additional liability problems that can plague an organization after the year 2000. The Air Force has created a certification process with seven tenets that if practiced will help guarantee success in the year 2000.

Success in terms of your year 2000 (Y2K) project means not failing in your Y2K fixes. This means they must be done on time—this deadline will not slip. Timing *is* everything, and the time for certification is now.

Why certify? Do you have the time to work for the percent assurance that Jeffrey Voas calls a “utopian pipe dream”? [1] Or would you prefer a confidence based on sound process? Some will do neither and fall prey to the “I hope” syndrome, where no certification is performed and managers rely on normal testing to avoid failing. But the Y2K issue is an addition of a magnitude to the normal software challenge. Peter de Jager points out that we as software managers are late 50 percent of the time [2]. If your system has interfaces, you not only have your concerns but also your suppliers’ and users’ concerns as well. With all the renovation being done, each change creates another magnitude of problems that require regression testing. These factors, along with the additional Y2K burden, make certification a must.

The Air Force Certification process is built on two Air Force-recognized standards: The Air Force five-phased approach to the Y2K and the Year 2000 Compliance Checklist. These two form a solid foundation for certification. The five-phased approach is further described in the Air Force Year 2000 Implementation Plan (formerly known as the Guidance Package) and was adopted not only by the Air Force but also by the Department of Defense (DoD) and other federal agencies in early 1996. The Compliance Checklist is well known throughout the DoD and is also being accepted by other agencies.

On top of this foundation, forming the structure, is a set of seven basic tenets that bring a higher level of confidence to the certification process from the bottom, where the technical development is performed to the top levels of management:

- Consistency Within the Process.
- Working as a Team.
- Documentation, Documentation, and Documentation.
- Due Diligence.
- Responsibility and Accountability Within the Signatures.
- Independent Verification and Validation (IV&V).
- Using the Right Tools.

The roof is supplied by Air Force top-level support and management support. Many times, our management has stepped in to provide visible encouragement and support. To those in the field, this support is key to alleviating their concerns over the great amount of extra but necessary work this effort creates. Our corporate approach to Y2K provides the glue that holds it all together. We encourage and expect organizations to go beyond the continuing higher-level guidance and to make it work at their locations. Much of the guidance is in the process of being created, which demands creativity from our organizations. The guidance can be tailored, and suggestions for such are provided within each step, allowing precious flexibility for organizations to choose the way to make certification work for them.

Consistency Within the Process

This tenet starts with the selection of your certifier. The certifier is the most important person within the process and is therefore located at the center of this activity. The relationship between the certifier and the other roles within the

certification process is displayed in Figure 1. Certifiers need to be carefully selected to be able to fulfill the many demands placed upon them. The section “Certifier Qualifications” provides guidance to help select certifiers.

Organizations are also encouraged to remove all conflicts of interest that can be realized, e.g., if the individual’s job responsibility is directly within the same chain of command as the system. The systems programmer, system owner, system tester, and point of contact are all examples of individuals who have stakes in the system and therefore represent conflicts of interest.

A standard set of tasks has been developed for certifiers for each of the five phases in which they will be involved. This enables the same process to be followed each time with predictable results. Standard documentation has also been identified and issued with templates or guidance to be used to simplify the certifier’s job. Often, document content varies. By making documents standard, certifiers can maintain more control of the outcome when interacting with the others. Standard roles and relationships for individuals involved in the process create an accommodating atmosphere.

Next, a standard, required training process is used to train the certifiers so they will be aware of documentation, tools, and how to implement them consistently. Finally, if the certifier meets the requirements and is trained, the process used to certify systems should not vary across the Air Force. Therefore, consistency in the process means getting the right type of person as your certifier, providing standard training to increase the consistency across all certifiers, and performing checks to verify the process.

Working as a Team

This tenet is based on the five standard roles and relationships illustrated in Figure 1 and defined below. As specified in the previous tenet, these important roles place certifiers in the center, but even though certifiers have undoubtedly the most important role due to the collection of various experiences and knowledge they must have, they are only one part of the whole. They need to build relationships with the other players to be successful. Following are the titles of the other individuals as shown in Figure 1 and their relationship with the certifier.

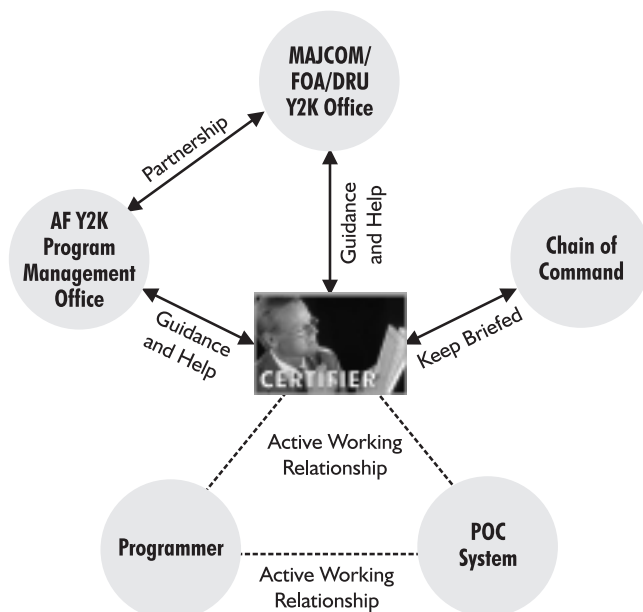
Year 2000 Program Management Office (Y2KPMO)

The relationship between the Y2KPMO and the certifier is one of support and reporting within already established major command (MAJCOM) Y2KPMO guidelines. It is never the intent to circumvent the established link between the certifier and the MAJCOM Y2KPMO. The Y2KPMO-certifier relationship should merely be an enabler toward certification. Since the Y2KPMO is responsible to assign certification control numbers (CCN) for systems, certifiers need to understand the reporting requirements to obtain them. The CCN is the control that identifies that the standard certification process has been applied to a system.

The MAJCOM PMO

This is the policy-making part of the organization. This group will determine the purview of all documentation, how the systems will be certified, who the certifiers are, what systems they are responsible for, and the extent of the Program Management Plan (PMP) for the organization (one overall broad PMP or several PMPs that represent separate business segments). The PMP must determine if all mission-critical and mission-essential systems receive independent test-type certification.

Figure 1. Roles and responsibilities. The certifier is the "center" of certification activities.



The Chain of Command

The certifier may be required to report to two chains of command. There will be the normal chain that involves the certifier's supervisor and the new addition of the systems chain of command. This relationship needs to be defined early to determine the needs of each party. Certifiers must feel confident with this chain of command because there may be times when they need their command's immediate attention to address a potential Y2K failure or symptom. The chain of command will need confidence that the certifier will only bring items tantamount to the success of the system to their attention. Therefore, this relationship is one of reporting and action. Care must be given to avoid unnecessary reporting to the chain of command, which can bog down the certification process.

The Programmer or Point of Contact (POC)

The programmer or POC is a generic representation of the person responsible for system development. In smaller organizations, the certifier may deal directly with the programmer. In larger organizations, it may be the system manager or POC. Depending on the software background of the certifier, this relationship may include formal and informal meetings. If certifiers have little software background, they may need to attend early meetings to determine responsibilities and types of reporting. Some of the other activities within this relationship are Y2K monitoring, assembling documentation (anticipating tenets four and five), and creating mutual Certification Tracking Document and Certification Level agreements. The more that is agreed upon in the Certification Tracking Document, the less that will be in contention later.

People in all roles need to work together as a team. If a single relationship is out of step, the potential for failure increases exponentially. For example, if certifiers find that actions taken by the development team are not consistent with the original plan, they must immediately bring this to the attention of the chain of command. It takes considerably longer to apply a fix once a system is in validation and has had a fixed window fix applied to it when the original strategy was for a four-digit year data fix. The same situation occurs if the chain of command does not speedily react. Fixes, if accomplished when discovered in the earlier phases, can be more easily applied.

Documentation, Documentation, and Documentation

Most of the documentation in question already exists in most organizations; therefore, providing documentation becomes as simple as creating the Y2K connections and additions to each piece. Just as documentation adds consistency to the process, the lack of documentation can cause disorder and increase the risk of failure and lead to interfaces that need rework or do not have anything to do with each other.

Taking the time to establish documentation early in the process will save time in the long run and reduce errors. Care must be taken to gather and organize the proper written communication that will maintain proper tracking through-

out the systems development or renovation. Along with providing a record of what was done, proper documentation helps all involved in the project better understand their roles and their relationship to others on the team. Maintaining documentation will not reduce all errors; however, when there are errors, the documentation will make it easier to track them down. The section "A Review of Required Documentation" lists all the required documentation and gives example content.

Due Diligence

Due Diligence will probably be the most important tenet after the dust settles. If your mission-critical or mission-essential system should fail due to a Y2K problem, you may find yourself testifying in court. Without evidence of due diligence, those involved could be held liable for the damage created by system failures—this is the case in the Air Force because the certifier must sign documentation to certify the system is Y2K compliant.

Recent news articles and comments by Air Force management have increased concern in this area, most notably through questions received during Air Force Certification training. Further, no one is "bullet proof," and the facts will determine how a case will be handled. In most instances, however, people who have been adequately trained, act responsibly, are competent in their job, put forth their best effort, and identify shortfalls that are beyond their control are at little risk. On the other hand, people who are incompetent, dishonest, or deceitful are at a higher level of risk. In the final analysis, there may always be some level of tension when managers try to allocate scarce resources and action officers try to apply these insufficient resources to complete the required tasks with due diligence.

We have defined due diligence as the necessary and earnest effort to accomplish a task. What does this mean? The definition is relative to the task being performed. Let us take it from the certifiers' perspective. First, certifiers must determine how their background fits in with the developers and the testers with whom they will be working. Some certi-

fiers may not have the background necessary to understand everything a developer or a tester does. In this case, we recommend that during Air Force Certification training, certifiers accompany the developers and the testers to their routine meetings to better understand these jobs. We also recommend that the certifier and the developer together complete the Compliance Checklist and determine the level of compliance the organization has chosen for certification of each system.

Additionally, there are seven forms of documentation required for certification: Certification Tracking Document (CTD), PMP, Contingency Plan, Memorandum of Agreement/Interface Control Documents (MOA/ICD), Test Plan, Configuration Management Plan (CMP), and Program Implementation Plan (PIP). Because they are an integral part of the IV&V portion of the certification process, these forms must be developed for each system, and the certifier needs to not only be aware of them but also understand how each is set up and how they are integrated.

The CTD is the most important tool the certifier has, and if necessary, it is designed to be his best defense in a future courtroom. As the title suggests, the CTD is the official tracker for the system. When a Y2K problem occurs, if the CTD is completely filled out, the document should point to the area where the problem occurred. The CTD helps expose areas of risk, uncover areas left undone, identify potential problems, and identify what is left to be done.

The concur and nonconcur blocks are the most important part of the CTD. Each block allows the certifier to raise a red flag if things are not proceeding as expected or desired. Additionally, and often overlooked, the remarks section of each block is a large area reserved for the certifier's comments about what is being done. Although there may not be enough evidence to nonconcur, certifiers have the opportunity to express any risks that may be evident that could lead to failure. Therefore, filling out the remarks section with pertinent information becomes due diligence. It shows that certifiers are doing their jobs as the key players in the process. Without this

information, it is suspect whether certifiers were involved in the process.

Some certifiers have allowed others to fill out the CTD for them, reasoning that the developer does the work and therefore can better answer the questions. This action or inaction can, in the worst case, lead to conflicts of interest—instances where the proper amount of time was not allotted to complete the document and other undesirable effects when the action of documentation gets in the way of development (from the certifiers' or programmers' perspective).

We included the job of the certifier in the process precisely to avoid this type of conflict. The certifier provides an objective look at the process. Developers and testers are too close to their work to effectively perform the certifier responsibilities contained in the CTD. Therefore, if this job is not done by the certifier—even though it does not lead to Y2K failure—it can be evidence that due diligence was *not* performed.

Since evidence can be used to defend oneself in court, it is important that the certifier maintain a folder for immediate and future perusal. This folder should contain copies of all required documentation as described above and any documentation deemed important to that system. For example, an IV&V performed by the Y2K PMO, audits by Air Force or DoD, and action plans to resolve deficiencies exposed by audits.

Responsibility and Accountability Within the Signatures

I have already discussed the importance of the CTD and what makes it an important document. However, all the information and data is meaningless unless accompanied by signatures of people in key roles. These signatures represent confidence in the work done and knowledge that everything possible was done to make the system Y2K compliant. Therefore, the responsibility goes back to all who were involved:

- The programmer or POC, lead developer, and systems manager (or however they are designated) will sign the CTD for every developer who worked on the system. They must know that their efforts and work were

complete and the total combination of effort will be Y2K compliant. Their signatures indicate that all the technical functioning and documentation is correct and complete. They must rely on most of the prior tenets to ensure their organizations are ready to document compliance.

- Certifiers are our center of activity; our coordinators, our unbiased view. Their signature attests that all bases were touched, everything went according to existing plans, and everyone who had a part played the part. The certifiers' eyes link all the players in the coordinated pattern represented by the documentation gathered.
- Users know what the system is supposed to do for them and the way the information should look. Their responsibility is to withhold their signatures unless their system is also proven to work to their specifications. This means that the documentation that is important to them (MOAs/ICDs) will be taken care of near the beginning to ensure direct compliance. Users are responsible for part of the certification work. It is essential that they are involved throughout the process to make sure things proceed along as they specified.

Systems accountability is provided by the signatures. If the system fails, the certifier, developer, and the user will share the fault and must work the fix together. Accountability works as a tool to enforce due diligence. The threat of the courtroom keeps all parties interested in the final outcome and ensures they do what it takes to get to Y2K compatibility.

Follow-Up Is the Key to IV&V

IV&V is the sixth tenet to certification and has been developed as a two-stage process. The first stage ensures that all tools gathered from the Certification training are in place, the Air Force Y2K Database (or Air Force Automated System Inventory) is cleaned up, and that further support is provided to the organization to get the certification process properly started. Discussions are initiated to develop the Certification Plan, the formal listing of certifiers and the systems they will certify, and to employ the proper initial documentation including the CTD. In this vein, follow-up provides a secure foothold that the original training initiated.

The second stage of IV&V is the actual verification and validation that certification has properly been done. In this stage, the database is analyzed for correctness, the systems are analyzed, and certifiers are interviewed to confirm consistent and standard application of the certification process. The organization then performs follow-up by taking all the findings from the second stage IV&V and developing an action plan to resolve any deficiencies or problems.

Using the Right Tools

Using the Right Tools and using them correctly is led by the CTD. All the required documentation is in the section "A Review of Required Documentation." There is no doubt these are the right documentation tools. The question is, "Were they used correctly?" Following are several of the tools and potential questions that can be asked.

CTD

- Did the certifier fill out all the blocks and initial all the activities?
- Did the certifier get management involved when the certifier was forced to nonconcur with an action?
- Were all nonconcurs resolved?

The Compliance Checklist

- Was the certifier present when the Compliance Checklist was completed?
- Did the developer complete the checklist during testing or after the tests were performed?
- Were there any comments as part of the checklist?

Contingency Plan

- Is a plan in place for all cases in which one is required?
- Are all Y2K considerations covered?
- Are system and operational items covered?

Test Plan

- Does the test plan include adequate Y2K testing?
- Does the regression testing include all the Y2K changes?

Certifier Qualifications

This section describes the characteristics and experience of the "perfect" certifier. We realize that individuals who fit this description realistically do not exist or are extremely hard to find. To find the best certifier for your systems, it is in your best interest to find a close match to the perfect certifier description. A certifier is designated by the commander and given proper authority and responsibility to meet the organization's and the Air Force's Y2K objectives. Selection criteria may differ depending on the functional area, mission requirements, and other circumstances determined by the commander. This document is a guideline that may be used by commanders to select a certifier.

Organizational Knowledge and Experience

- Knowledgeable of all key players, internal organizational, external functional, and command elements involved with systems of interest.
- Sufficient knowledge, skill level, and ability in the functional area of interest to allow effective and timely assessments and evaluations.
- Familiar with and displays an understanding of the complexities of the mission environment, systems, and applications they must certify.

Technical Knowledge and Experience

- Possess the technical and operational expertise to extract pertinent information during the certification process.
- Possess the ability to conduct a methodical and extensive lifecycle analysis of data, information, procedures, and processes related to the functional area assigned.
- To meet the technical criteria, a certifier should have some background in
 - the Capability Maturity Model for Software.

- quality assurance or IV&V.
- testing (planning or execution).
- software engineering.

Authority and Commitment

- Must serve in a level or position commensurate with the responsibility, possess the necessary authority to execute required actions, and have access to relevant databases and cognizant command authorities.
- Primary or "lead" certifiers must have sufficient time remaining in the assignment and position to perform the duties required until 2001 to ensure continuity.

A Review of Required Documentation

CTD

The CTD tracks the progress of certification for each system and reduces the risk of Y2K failure. This tracking provides management with greater assurance of success by the early identification and resolution of Y2K-related problems.

PMP

The PMP ensures that everyone, including people in your chain of command and any subordinate organizations, understands their roles and responsibilities in relation to solving the DoD and Air Force Y2K problem. The typical PMP contains

- information on the background of Y2K at the organization.
- a goal or purpose for the organization.
- direction or program strategy.
- objectives and management approach.
- responsibilities and resources.
- baseline milestones and tasks and schedule.
- annexes and support documentation.

Contingency Plan

The contingency plan maintains the continued success of the system by addressing every known or possible instance of failure and indicating alternative resolutions. Contingency plans address all possible known future occurrences of mission interruption—whole or partial. The plan identifies interim

and permanent remedies and associated implementation timelines. Contingency plans also inform system users of possible work-arounds. Air Force Contingency Plans consist of system and of operational contingency plans. The System Contingency Plan is developed by the programming system manager, and the Operational Contingency Plan is formulated at the unit level.

Test Plan

The test plan establishes standard and consistent plans and scenarios for all Y2K testing for the development team to follow. Test reports document the results of the testing. The test plan typically includes

- scope.
- system and interface identification.
- referenced documents.
- test environment.
- software transition.
- test site.
- test items.
- personnel.
- test levels and classes.
- test conditions.
- test schedules.

CMP

The CMP establishes and maintains integrity of automated information systems (AIS) throughout the AIS lifecycle. The CMP institutes specific procedures to manage changes to AISs. The configuration of the AIS is analyzed at given points in time. Configuration changes are systematically controlled, and there is traceability of the configuration at each step.

MOA/ICD

The MOA/ICD provides complete agreement between all interface users of a system. Many ways to solve the Y2K problem have been identified. Some of these solutions do not work well with each other. The MOA/ICD forces communication and agreement on the chosen Y2K resolution method. This is handled during the assessment phase in the renovation strategy. In addition, costs for translators, etc., must be addressed and agreed upon within the MOA/ICD.

PIP

The PIP documents when, how, and who will field the Y2K-compliant system. A typical PIP contains

- introduction.
- purpose and scope.
- authority references.
- action agencies.
- actions required.
- milestones.
- resourcing.
- command and control.

In addition, appendixes usually cover

- time-phased actions.
- contingency management.
- automated information systems.
- sources of information.
- points of contact.

Conclusion

Certification adds to the confidence of Y2K compliance by measuring the process and adding the assurance of unbiased checking. This assurance is accomplished throughout the five-phased process in a checklist, or ordered, fashion. Organizations must start now before it is too late. The seven basic tenets are keys that can make previous guidance more understandable and attainable and serve as a measuring stick and a helping hand. Remember, our corporate approach to Y2K is the glue that keeps everything together and allows flexibility. This approach allows organizations to work where they feel more comfortable. The Air Force Certification process is designed to bring management's expectations in line with Y2K compatibility assurance. ♦

About the Author



Thomas V. Ashton is a software specialist and one of the pioneers of the Air Force Y2K problem resolution. In the Program Management Office, he leads

the certification effort and was one of the key developers of the Certification Training Program, Certification Tracking Document, and Independent Verification and Validation Program. He co-wrote the "Year 2000 Air Force Challenges" and presented it at several conferences in 1996

See Y2K on page 29



Partnership Process for Electronic Warfare Acquisition

Maj. Art Huber and Lt. Col. Jay G. Santee
Office of the Assistant Secretary of the Air Force for Acquisition

The complete version of this article can be found on the *CROSSTALK*
Web site at <http://www.stsc.hill.af.mil/CrossTalk/crostalk.html>.

The Partnership Process is an acquisition reform initiative that has emerged from the electronic warfare (EW) community. The new process draws on lessons learned from world-class companies to re-engineer EW acquisition. These companies are customer-driven, so the lesson for Air Force acquisition is to respond to the voice of the war fighter by using military worth as the procurement criterion. Top companies maintain open dialog with their suppliers so the Partnership Process emphasizes new ways to foster commu-

nication with industry. The best organizations achieve their results through continuous optimization, so we must adopt methods to converge on best solutions.

The new acquisition process can be summarized by six activities (see Table 1) that consistently put superior solutions into the hands of our war fighters as quickly and inexpensively as possible.

These results were achieved through a series of intensive integrated process team meetings that included broad representation from Air Force organizations

and the contractor community. Our new process is described in a comprehensive report now available on our Web home page (<http://ewio.wpafb.af.mil>) and on a CD-ROM available free while supplies last. Currently, our focus is on laying the groundwork for process implementation through a war fighter-led pilot program, the development of an Internet-based training course, and the release of a quick-turn, PC-based decision aid known as the Measures of Effectiveness Tool. The pilot program will demonstrate the application of partnership principles in an area of interest designated by a major command requirements office. The training course will be developed with both government and industry audiences in mind and include the latest reform initiatives (such as the Lightning Bolts) within the holistic view of the partnership. ♦

Maj. Art Huber
Voice: 703-588-6515 DSN 425-588-6515
Fax: 703-588-1225 DSN 425-588-1225
E-mail: HuberA@af.pentagon.mil

Table 1. *Measuring military worth forms the foundation for our reformed acquisition process.*

Activity	Innovative Theme
Quantify mission deficiencies.	Base deficiency analysis on war fighter strategy-to-task.
Establish requirements.	Frame the requirement in terms of airspace bought back.
Convey requirements.	Structure Request for Proposal to ask for military worth, not specifications.
Select the source.	Incentivize the contractor to reach beyond thresholds.
Develop the solution.	Continuously optimize the trades to converge to a solution.
Evaluate the result.	Link test and evaluation directly to war fighter needs.

Y2K from page 10

including the Institute of Electrical and Electronics Engineers conference in St. Louis, Mo. and the DoD Database Colloquium in San Diego. He has also worked other software efforts within the Air Force such as software process improvement. He has a master's degree in business administration from Southern Illinois University and a bachelor's degree in computer science from the University of St. Thomas.

AFCA/ITYO
203 W. Losey Street, Room 1065
Scott Air Force Base, IL 62225-5224
Voice: 618-256-5697
E-mail: thomas.ashton@scott.af.mil

References

1. Voas, Jeffrey, "Certifying Year 2000 'Fixes,'" *CROSSTALK*, Software Technology Support Center, Hill Air Force Base, Utah, January 1998.
2. De Jager, Peter, "Throwing Down the Year 2000 Gauntlet," *CROSSTALK*, Software Technology Support Center, Hill Air Force Base, Utah, January 1998.