AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1 CONTRACT ID CODE	PAGE OF PAGE(S)
	1 | 3

2 AMENDMENT/MODIFICATION NO	3 EFFECTIVE DATE	4 REQUISITION/PURCHASE REQ. NO	5 PROJECT NO (If applicable)
1	SEP 16 1998		

6 ISSUED BY	7 ADMINISTERED BY (If other than Item 6)	CODE

9 NAME AND ADDRESS OF CONTRACTOR (No. Street, county, State and ZIP Code)

DynCorp Information & Engineering Technology, Inc.
Attn: Rober Toth
12750 Fair Lakes Circle
Fairfax, VA 22033

(✓)	9A. AMENDMENT OF SOLICITATION NO
	9B. DATED (SEE ITEM 11)
	10A. MODIFICATION OF CONTRACT/ORDER NO: NAS1-98091
	10B. DATED (SEE ITEM 13): April 30, 1998

CODE FACILITY CODE

☐ forth ☐ is extended, ☐ is not extended

(✓)

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

X Mutual Agreement

D. OTHER (Specify type of modification and authority)

E. **IMPORTANT:** Contractor **is required** to **sign this document and return** _1_ **copies** to **the** issuing office.

14 DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to delete clause H.8 entitled "Commercial Computer Software and Systems and make changes to Clause C.1 entitled "Statement of Work – Systems Engineering for Research Facility Integrated Systems (SERFIS)". Therefore, the following changes are made to the contract:

(Continued on Page 2)

(continued)

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Robert F. Toth Contracts Manager	CHARLOTTE T. HARDY, CONTRACTING OFFICER
15B. CONTRACTOR/OFFEROR: (Signature of person authorized to sign)	15C. DATE SIGNED: 9/15/98
16B. UNITED STATES OF AMERICA BY: (Signature of Contracting Officer)	16C. DATE SIGNED: 9/16/98

NSN 7540-01-152-8070
PREVIOUS EDITION UNUSABLE

30-105
Computer Generated

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA FAR (48 CFR) 53.243

FILE

A. Clause H. 8. Entitled "Commercial Computer Software and Systems" is deleted in its entirety.

B. Clause C.I. entitled " Statement of Work – Systems Engineering for Research Facility Integrated Systems **(SERFIS)"** is changed by adding the following paragraph:

'9.0 Year 2000 Compliance

9.1 Year 2000 compliant." as used herein. means that the information technology (hardware, software and firmware, including embedded systems or any other electro-mechanical or processor-based systems used in accordance with its associated documentation) accurately processes date and date-related **data** (including, but not limited to, calculating, comparing, and sequencing) from, into, **and** between the twentieth **and** twenty-first centuries, and the years 1999 and 2000 and **leap** year calculations, to the extent that other information technology, used in combination with the information technology being **acquired,** properly exchanges date and date-related data with it.

9.2 Any information technology provided. operated and/or maintained under this contract **must** be **Year** 2000 compliant. To ensure this result. the Contractor shall provide documentation describing how the IT items or services demonstrate Year 2009 compliance.

The Contractor shall test any information technology items that are provided. operated, and/or maintained under this contract in accordance with the document "**NASA** Year 2000 Agency Test and Certification Guidelines and Requirements" (Attachment 1 to this modification). Documentation and testing requirements for Year 2000 compliance are based on complexity of the information technology and the **risk** associated with the IT item Y2K non-compliance. The testing of the IT items shall be determined using **a** risk-based approach. Risk has been categorized into 3 categories: Low, Medium, and High. **A** phased testing approach will be used io identify and correct errors. The testing shall **be** consistent with Attachment 1. considering the risk level, type of system. and Year 2000 date dependency of the IT item. In order to document the Year 2000 testing and compliance, the "NASA Langley Research Center Y2K Compliance Verification Form" (Attachment 2 to *this* modification) shall be utilized.

Pursuant to subject contract Statement of Work. Paragraph 1.3 Facility Automation Systems, the fourth paragraph states that the Government will furnish EPICS (Experimental Physics and Industrial Control System) software to Contractors for delivery orders requiring its use. The Contractor is not required to make the EPICS development tools or the run-time environment tools Y2K compliant. However, the Contractor's software application that is required as part of a specific delivery order is required to be Y2K compliant.

9.3. Milestones for Renovation, Validation and Implementation: Any IT determined to be non-Year 2000 compliant shall be replaced. retired. or repaired in accordance with the following schedule:

. "Renovation" includes making and documenting software and hardware changes, developing replacement systems. and decommissioning systems to **be** retired. The Contractor must complete renovation of affected software, hardware and firmware by September 30, 1998.

. "Validation" includes unit. integration. system, and end-to-end testing for Year 2000 compliance. The Contractor must complete validation and testing of converted or replaced systems by January 31, 1999.

. "Implementation" includes acceptance testing and integration of converted and replaced systems into a production environment. The Contractor must complete implementation by March 31. 1999.

9.4. At a minimum, the Contractor shall provide documentation, including project plans and status reports, which demonstrate that the Contractor is meeting the milestones listed above."

9.5: The requirements of 9.2 above shall be implemented as follows. As part of any request for a Delivery Order proposal, NASA will identify to the Contractor any information technology items to be operated or maintained by the Contractor which are subject to the requirements of 9.2. Any items to be operated or maintained by the contractor which are not so identified, shall not be subject to the requirements of 9.2. However, all information technology provided by the Contractor shall be Year 2000 compliant in accordance with 9.2.

Note: (1) "NASA Year 2000 Agency Test and Certification Guidelines and Requirements" document referenced in the above section and attached was developed for NASA's use. This document is provided as a tool for the Contractor to establish the appropriate testing and documentation requirements for Year 2000 compliance.

(2) Attached for your information is the "NASA, Langley Research Center Y2K (Y2000) Compliance Verification Form which will be signed by the Contractor and the Contracting Officer's Technical Representative (COTR). The "Y2K Decision Tree for Documentation and Testing Requirements" form is also attached and can be used to determine the required documentation and testing.

A. All other terms and conditions remain unchanged

Attachments

NASA Year 2000 Agency Test and Certification Guidelines and Requirements

Volume 1

July 2,1998

National Aeronautics and
Space Administration

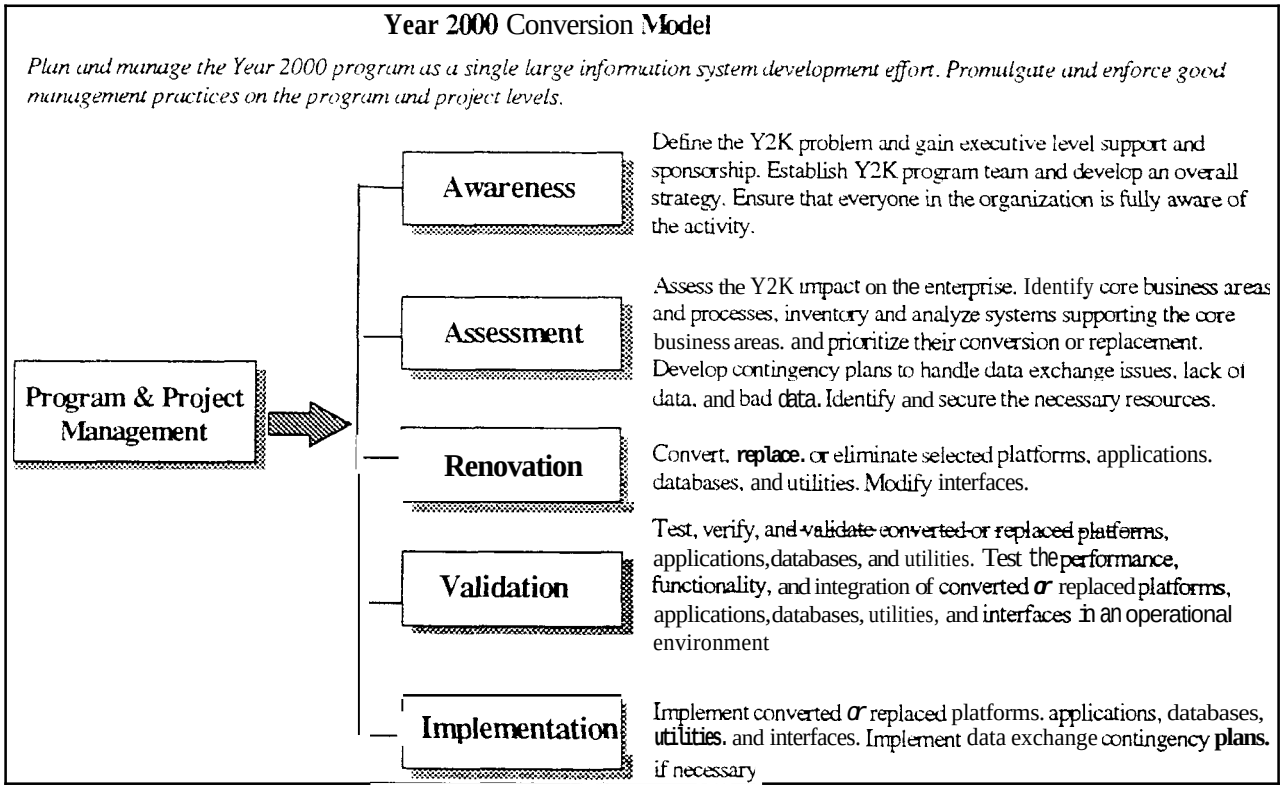
Contents

Tables

Section 1. Background

NASA initiated the Year 2000 (Y2K) program in August 1996 to address the challenges imposed on Agency software, hardware, and firmware systems by the new millennium. The Agency Y2K program is centrally managed by the NASA Chief Information Officer, with decentralized execution of program requirements at each of the nine NASA Centers, Headquarters, and the Jet Propulsion Laboratory. The Y2K Program Plan details the technical, schedule, and cost commitments, and it includes strategies for acquisition, risk management, and test and verification. Center Y2K Project Plans provide detailed requirements and plans that are consistent with the overall program management approach, guidance, and requirements.

In January 1997, the Office of Management and Budget (OMB) required all federal agencies to adopt the Government Accounting Office (GAO) five-phase model for implementing the Y2K program. The following exhibit graphically illustrates the five phase model NASA has adopted for the Y2K program.



NASA completed the Y2K assessment of its inventory of hardware, software, and firmware in August 1997. The scope of the assessment included applications developed in-house (in development or operations); Commercial-off-the Shelf (COTS) software, hardware, and firmware; and special support areas such as facilities and environmental control systems and other embedded uses of information technology (IT) products. Renovation of inventory items needing corrective action is to be completed by September 1998; validation by January 1999; and

implementation by March 1999. Objectives and approaches for completing renovation, validation, and implementation may be found in the NASA Y2K Program Plan.

The objectives of the validation phase are to uncover errors introduced during the renovation phase; and verify the operational readiness of inventory items. Government-wide requirements for validating renovated inventory items include unit-level, integration-level, and system-level testing. In April 1996, the Program provided general Y2K test guidance for Centers to consider when identifying their local Y2K test strategies and methods. In April 1998. we conducted a review of current Center practices and strategies for Y2K testing. Generally, Centers are adapting local systems management practices to meet Y2K validation and verification requirements. Examples are structured systems development methodologies that include formal testing and verification processes, use of independent testing organizations, such as a Center Software Product Assurance Office or an independent Y2K contractor, and the exceedingly formal Independent Verification and Validation (IV&V) associated with testing changes on systems affecting human space flight. The selected approach is highly dependent upon the inventory item function, criticality, and **risk.**

The objectives of this guidance are to:

(1) Provide general guidance and requirements for Y2K certification and testing.
(2) Establish required minimal Y2K test criteria and certification processes that will be consistently applied to NASA inventory items.

This document specifies minimal requirements (identified by terms "shall" and "must") and general guidance (identified by terms "should" and "may") for accomplishing Y2K certification and testing. Centers are encouraged to tailor guidance to meet local requirements. Centers should also refer to the GAO Guide, "Year 2000 Computing Crisis: **A** Testing Guide." for additional guidance on testing.

This document has four sections and Appendices A to I. Section 2 provides guidelines and requirements for Y2K certification. Section 3 provides guidelines and requirements for conducting Y2K tests. Section **4** provides guidance on Y2K compliance criteria. Appendices **A** to D provide sample certification forms and Y2K checklists. Volume 2 provides sample test plans used at **NASA** Centers.

Throughout this document the term, "NASA employee" includes employees of the Jet Propulsion Laboratory (JPL) for JPL inventory items.

Section 2. Y2K Certification Guidelines and Requirements

This section provides guidelines and requirements for completing Y2K certification of inventory items. Inventory items must be vendor certified or otherwise tested and certified by NASA. Section 3 provides requirements and guidance on test criteria and testing levels for inventory items that are tested by or for NXSA. Section 4 provides guidance and general criteria which should be satisfied for an inventory item to be considered compliant.

2.1 Inventory Item. Centers are responsible for determining what constitutes an inventory item to be assessed. corrected, validated. or certified compliam for Y2K purposes. A NASA inventory item may be an IT system, non-IT system (e.g. environmental, biomedical), application, hardware component, software component, firmware, or COTS product. An inventory item may be a combination of custom software, hardware, and COTS products, or any component item. Inventory items must be classified as either mission-critical or nonmission-critical (see Glossary, Appendix C).

Inventory items must be assigned one of the following statuses:

2.1.1 **Non-Compliant/Repair**—Non-compliant inventory item components will be manually or automatically modified, or both, to make them Y2K compliant.

2.1.2 **Non-Compliant/Replace or Upgrade**—The non-compliant inventory item will be replaced with a Y2K compliant system that provides comparable functionality. For COTS components. upgrades are classified as replace/upgrade.

2.1.3 **Non-Compliant/Retire or** Discontinue — The inventory item will leave the **NASA** inventory because of Y2K or other reasons. No replacement system is anticipated. For COTS components, the product will leave the NASA inventory, with no anticipated upgrade or replacement.

2.1.4 **Non-Compliant/No** Corrective Action ~~A~~ non-compliant Y2K inventory item that will be retained in the NASA inventory and not made compliant.

2.1.5 Not Date Affected - Inventory item does not process dates or date related data.

2.1.6 Date **Affected/Compliant** – Inventory item processes dates or date-related data and is Y2K compliant

2.2 **Certification of Inventory Items. NASA** inventory items must be certified as Y2K compliant by March 31, 1999.

- To be certified as Y2K compliant. an inventory item must fulfill one of the following requirements:
- Successfully complete testing conducted by or for **NASA**
- Demonstrate Y2K compliance by vendor certification
- The only exception to this requirement are the Non-Compliant/No Corrective Action inventory items.
- Inventory items classified as not calendar date affected must either be tested or documented as not date affected.
- The content and level of detail for certification may vary based on Center requirements and the nature of the inventory item.
- Inventory items that are tested must complete the system level test for certification. However, there is some flexibility for testing COTS products. Centers may elect to use integration testing or system level testing to certify COTS products, as appropriate.
- Certification forms must be signed by a NASA employee. (Sample forms are in Appendix **A.)** Centers may elect to require additional signatures, including contractors responsible for operations and maintenance of inventory items, as required.

Appendix C, Glossary of Terms, provides the NASA definition of "Y2K compliant" consistent with Federal guidance. Appendix **A** provides sample certification forms for vendor certified, NASA tested, and not date affected inventory items. The following paragraphs detail requirements.

2.2.1 **Vendor Certified:** The inventory item is a COTS product that is date affected and certified by the vendor or contractor as Y2K compliant. Documentation may include standard product literature, test reports, test procedures, or commercial certification statements. Documentation must be commensurate with the **risk** level of the inventory item. Appendix **A-1** provides a sample certification form for COTS products.

Three NASA Centers have been assigned responsibility for tracking and reporting test and certification results of COTS hardware and software products in five areas: workstation, mainframe, midrange, communications, and supercomputing . At a minimum, Centers must follow established certification and documentation procedures for COTS products in these areas. For COTS products that do not fall under these areas. Centers should establish similar certification and documentation procedures commensurate with the risk-level of their inventory items.

2.2.2 **Tested and Certified:** The inventory item is date affected and has been tested **and** certified by or for NASA against required tests and standard test criteria commensurate with the risk level of the inventory item (described in Section 3). If the inventory item is a COTS product that a Center decides to independently test, Centers must follow the appropriate test and documentation procedures established by the three COTS principal centers (MSFC, LeRC, and **ARC).**

Tested Inventory items must meet the documentation requirements specified in Table 3-7. Three levels of documentation are required: test plans and procedures, test results, and certification forms.

2.2.2.1 **Test Plans and Procedures** – Test plans and procedures must be prepared to address required levels of testing, test criteria, and Test procedures. Test plans and procedures may be written to address a specific inventory item (e.g., a specific mission-critical system) or a class or group of inventory items (e.g., desktop COTS products). The-content and level of detail of the *test* plan and procedures will vary based upon the complexity of the inventory item and the magnitude of the Y2K impact. Volume 2 provides examples of the following Y2K test plans for reference:

- MSFC LASER TPP
- LeRC COTS Test plan for workstations
- MSFC COTS Communications Test Plan
- JPL Year 2000 Compliance Requirements
- Year 2000 Test Plan for Langley Research Facilities
- Flight Dynamics Y2K Test Plan

2.2.2.2 **Test Results** – Test results must be documented in a test report or completed Y2K checklist for each inventory item tested. The content and level of detail of the test report will vary based upon the complexity of the inventory item and the magnitude of the Y2K impact. Sample Y2K checklists are provided in Appendix B. Y2K checklists should be tailored to meet Center requirements. The content of the checklist may vary based on the inventory item tested. Examples of Y2K checklist content include the following:

- The results of Y2K test cases for system functions
- A list of components comprising the inventory item, along with the component ID, component type (hardware (H/W), software (S/W), firmware (F/W), or COTS))
- The date the component was tested and the **NASA** responsible person
- **-A** list of all external interfaces, the date the interface was tested ,and the **NASA** responsible person for ensuring that the testing and documentation is accurate.

2.2.2.3 **Certification** – All tested inventory items must be certified by a NASA employee. Appendix A-2 provides sample certification forms. The content and level of detail for certification may vary based on Center requirements and the nature of the inventory. Centers may elect to require additional signatures, including contractors responsible for operations and maintenance of inventory items, as required.

2.2.3 **Documented and Certified As Not Date Affected.** The inventory item is not date affected and not tested. Documentation is required to certify that the inventory item is not date affected. Appendix D provides a sample checklist for verifying that an inventory item is not date affected.

2.3 **Non-Compliant/No Corrective Action Inventory Items.** Non-compliant items that will have no corrective action taken must be identified and documented. Documentation must include the name and description of t he non-compliant inventory item, the business or operational rationale for not taking corrective action (e.g., not upgrading), and a determination of the risks or potential impact to the Agency for not taking corrective action. Decisions and documentation for non-compliant Y2K inventory items must be approved by the Center Y2K Project Manager and the Center CIO Representative. Accounting of these actions must be sent to the **NASA** Y2K Program Manager.

2.4 **Independent Validation and Verification.** Test processes must include an independent validation and verification of test results for mission critical systems. Independent validation and verification may be performed by any individual(s) independent of the developer or certifying individual. Centers should use quality assurance groups or validation and verification agents where practical to ensure consistency and quality of test processes and results.

2.5 **Waivers.** Centers must establish a formal waiver process for any variance from the minimum requirements established in this document. Waivers may be issued to combine testing levels where the criteria are met in the combined test, or, in limited cases, where the degree of testing is reduced because the Y2K changes are cosmetic or the risks of Y2K impacts are low. At a minimum, waivers must be approved by the Center Y2K Project Manager and the Center CIO Representative. Accounting of these actions must be sent to the NASA Y2K Program Manager.

2.6 **Grandfather Clause:** Inventory items that completed testing prior to this guidance and that meet the following criteria are exempt from this guidance:

- The test approach for the inventory item meets the minimal test requirements and criteria established in this guidance, commensurate with the level of risk of the inventory item
- Processes followed for the inventory item meet the intent of this guidance through comparable test and certification processes.

The Center CIO Representative and Center Y2K Project Manager must approve Y2K inventory items that are exempted (i.e., grandfathered) from this guidance. Accounting of these actions must be sent to the NASA Y2K Program Manager.

Section 3. Y2K Testing Guidelines and Requirements

This section provides test guidelines and requirements for Inventory items being remediated and/or tested by or for NASA for the Certification process described in Section 2. The intent is to provide an Agency Y2K test approach yet permit enough flexibility to allow Centers to use their existing test processes to the extent practical, augmented by Y2K time-shift testing. Centers should also refer to the GAO Guide, "Year 2000 Computing Crisis: A Testing Guide," for additional guidance on testing.

3.1 **Purpose.** The purpose of Y2K testing is to verify the Y2K compliance of a date-affected inventory item and ensure that Y2K corrective actions have not adversely impacted the existing functionality of an inventory item. Test processes must provide sufficient assurance of diligence in testing documented by test plans and/or test procedures, test reports or compliance checklists, and certification signoff. Quality assurance staff or independent validation and verification agents shduld be used, where practical, to ensure that test requirements and guidance are met.

3.2 **Risk-Based Approach.** NASA is adopting a risk-based approach for the testing and certification of inventory items. Risk categories are low risk, medium risk, and high **risk** (see Glossary, Appendix C). At a minimum. NASA inventory items must meet the test requirements and test criteria established for low risk items or provide documentation that the inventory item is not date affected. Medium and high risk inventory items must meet the minimal test requirements and test criteria defined in Tables 3-1 through 3-6. By definition, NASA inventory items classified as "mission critical" would typically meet test requirements and test criteria specified for high risk items, but there is some flexibility for Centers to tailor risk levels assigned. Inventory items designated as mission critical may contain components that are medium or low risk; for example, a mission critical system may include auxiliary components that are low or medium risk, such as faxes or printers. Centers may selectively tailor test criteria to reduce the level of testing for those components. Table 3-7 summarizes the minimum test criteria for each risk level. Centers should establish test requirements and test criteria beyond the minimal where appropriate.

3.3 **Testing Approach.** The NASA Y2K testing approach applies time-shift testing to a renovated component through a series of test levels according to its assigned risk. The time shift test dates represent critical dates for Y2K compliancy. The test levels include unit testing, integration-testing, system testing, acceptance testing, and end-to-end testing. The testing should include regression, performance, stress, and window boundary testing, as appropriate for the test level. All Y2K certification testing must be accomplished in a Y2K compliant environment, where feasible.

The NASA-Y2K testing approach is based on demonstrating that existing functionality will operate normally on general days in 2000 and that rollovers for the dates specified in Table 3-1 do not generate anomalous behavior. The most cost-effective order for conducting Y2K testing is to first validate the operation for general days in 2000 and then to conduct

specific time-shift tests (e.g., rollover from 12/31/1999 to 01/01/2000) according to the level of risk (Appendix C) and available resources.

3.4 **Time-Shift Testing.** One test technique used to uncover Y2K problems is known as Time-Shift Testing. Time-shift testing is simply the process of altering system clocks so that a future date and time appears to be the current date and time. This time-shifting technique is applied to the test environment to establish the dates for Y2K compliance tests. Time-shifting can be accomplished by physically changing the system clocks or by installing date simulation software that intercepts calls to the system clock. Note that time-related or time-dependent data in databases and manual input data may also need to be adjusted to make the data consistent with system clocks each time the system is time-shifted.

3.4.1 **Time-Shift Test Precautions.** Time-shift testing should be performed on systems that are isolated from both development and operations. Before beginning such testing, the system should be completely backed up to external media; procedures should have been previously tested and documented that describe how to back up the data, change the dates at all layers of the system architecture, and restore the data. After completion of time-shift testing, the media must be erased, and all backup files must be restored. Failure to do sc risks the creation of anomalies arising from files and operating system services having dates in a future year.

3.4.2. **Required Test Dates.** Table 3-1 identifies the required dates that Centers must use, as a minimum, in testing low risk, medium risk, and high risk inventory items. Centers may select additional dates to test based on the complexity and risk level of the inventory item. These dates are listed as optional or recommended for each risk category.

3.4.3. **Rollover Exceptions.** There may be cases where low and medium risk inventory items opt to power down during the January 1, 2000 rollover. In these instances, inventory items do not necessarily have to be tested for the 12/31/1999>01/01/2000 date. These inventory items must, at a minimum, conduct time shift testing for random dates in the Year 2000 ensure general functionality is validated.

3.4.4. **Window Boundary (Backward Time) Testing. These tests are required only for window techniques used to interpret 2-digit year dates.** Testing shall ensure that the window boundaries (Appendix C) selected to resolve 2-digit year representations meet the following criteria:

- Do not exclude valid ranges in the data. Example: If the window boundary is set for 1930 for a personnel system, and if the current database contains information on an individual born prior to 1930, the information on this individual cannot be recognized as 20“ century data.
- Test dates around the window boundaries ensure that the software properly interprets the century. For example, if a window boundary is set at “70,” tests should ensure that “69” is interpreted as 2069, and 70 is interpreted as 1970.

3.4.5 **Julian Dates.** Table 3-1 defines February 29 and March 1 as leap year test dates. These test dates are valid for systems that carry the day, month, and year. For systems that carry the Julian date, December 31 (day 366) and January 1 (day 1) are the dates appropriate for leap year testing. Where both date formats occur within a system. both tests apply.

3.4.6 **Date Expirations.** Date expirations may occur as a result of time shifting the system dates. Test preparation needs to identify and protect against date expirations. Examples of date expirations that may occur are:

- License expirations
- File expiration dates that may delete files, data or programs, passwords and user IDs
- Archive and Retrieval functions
- Database delete functions
- Network Access
- Hierarchical storage functions.

3.5. **Levels of Testing. A** phased approach to testing reduces the cost and time to identify and correct errors and increases the probability that errors will be discovered. Unit and Integration testing uncover errors injected during Y2K code corrections. The cost and schedule for fixing errors at the unit and integration levels are significantly less than at the higher testing levels. System testing verifies the system performs its functions correctly and interfaces with other systems across and after the Y2K transition. Acceptance testing determines whether the system is ready for normal operation. End-to-end testing ensures that critical mission threads function correctly and will provide essential mission services across and after the Y2K transition.

3.5.1. Required Test Levels. Tables 3-1 through 3-8 in Section 3 of this document define the requirements Centers must follow in testing low, medium and high **risk** systems. For each level of **risk,** Tables 3.1 through 3-8 describe the test coverage, and entrance and exit criteria for completing the level of test specified. There is sufficient flexibility within the tables to allow the Centers to tailor these tests to their individual requirements. For example, Table 3-4 requires low **risk** systems to test basic system functions, but leaves it to the Centers to determine what constitutes the basic functions of the inventory item.

3.5.2 **Unit Level Test.** Unit testing focuses on identifying and correcting defects in modified or newly developed units before they are integrated with other units. Unit test criteria (Table 3-2) apply to the smallest defined renovated module, e.g., subprograms, subroutines, or procedures. Unit test does not apply to COTS. Table 3-2 contains unit test criteria, which are required for unit testing of renovated

modules other than COTS. For unit test, the same level of test applies to all risk levels.

Example: If a unit computes the position of the moon, and was renovated for Y2K, it would be tested to ensure it still correctly computes the position of the moon. Where possible, existing test cases would be used for this verification. For Y2K testing, additional tests would be designed and run to ensure that the position of the moon is computed correctly for the relevant dates described in Table 3-1.

3.5.3 **Integration Level Test.** Integration testing focuses on uncovering module interface errors introduced during renovation and verifying that the integrated components are Y2K compliant. Integration test focuses on the internal interfaces of the inventory item. Integration level test is based on the systems requirement specifications for the inventory item. Centers have the option to certify COTS inventory items at the integration level or system level.

Example: For an orbit determination system inventory item consisting of hardware, unchanged software, and renovated software such as the moon position module, integration tests would ensure that the inventory item still produced the same results using existing test cases. For Y2K testing, tests would also verify correct Y2K interfaces to the moon position module by ensuring that the orbit computed used the correct moon position and other data for the relevant dates described in Table 3-1.

Table 3-3 contains integration test criteria, which is required for integration-testing of renovated program modules other than COTS.

3.5.4. **System Level Test.** System testing involves testing all of the integrated components of an inventory item, including interfaces external to the inventory item, data. and operational procedures against their requirements specification. The risk level assigned to that inventory item, as Table 3-4 describes, determines the scope and depth of system testing. Specialized tests run either separately or in some combination in an actual or simulated operational environment are run to verify that entire system performs as intended. Tests may include

- Functional testing: The purpose of functional or "black box" testing is to verify that the system correctly performs specified functions. As such, the test team's ability to design the functional tests is limited by the completeness and precision of the functional specifications. Starting with these specified functions, the test team develops test cases using a range of valid input conditions and options as well as invalid or unexpected inputs. The test team then compares the test outputs to expected outputs.

- Performance testing: The purpose of performance testing is to assess how well a system meets specified performance requirements. Like functional testing, performance testing can only be as complete and precise as the system's defined performance requirements. Examples of performance requirements include specified system response times under normal workloads (e.g., defined

transaction volumes) and specified levels of system availability and mean times to repair.

- Repression testing: The purpose of regression testing is to demonstrate that newly added or modified system components (hardware or software) have not compromised system functionality and performance (i.e., have not introduced new errors).
- Stress testing: The purpose of stress testing is to analyze system behavior under increasingly heavy workloads (e.g., higher transaction rates) and severe operating conditions (e.g., high error rates, lower component availability rates), and, in particular, to identify points of system failure.

Example: For an orbit determination inventory item consisting of Flight Dynamics GOTS software, computer hardware and software, LAN connections to ground control systems and to White Sands Ground Terminal (WSGT): system level testing consists of verifying that the functions of each of these components operate correctly. Simulators are often used in testing external interfaces (e.g., the interface to WSGT). For systems that contain renovated code, the above tests are conducted using the current date, and results *are* compared against a known baseline. For Y2K testing, these tests are repeated for each of the relevant dates in Table 3-1. If the orbit determination inventory item is high risk, all system functionality and interfaces will be tested to the maximum extent possible, as described in Table 3-4.

For example, this may include testing orbit calculations for several moon positions. If the inventory item is medium risk. the functionality tested will be determined by the magnitude of the risk; for example, the number of moon position calculations will vary. If the inventory item is low risk, basic functionality will be tested. For example. the moon position may be ignored, as it has minimal effect on the orbit calculations.

System testing is required for all date affected inventory items. If certification is not performed at the integration level. certification is required at the system level.

3.5.5. **Acceptance Test Level.** Acceptance testing involves testing the entire information system, including interfaces with operational data. The degree of acceptance testing is based on risk level, as Table 3-5 describes. Acceptance testing should be done in a Y2K compliant environment with duplicate databases to avoid the risk of contaminating production systems and data.

Example: Refer to the example described for system testing. Operational scenarios developed for or by the ground systems operation team are performed in an operational environment using existing operational procedures. For systems that contain renovated code, the above tests are conducted using the current date, and results are compared against a known baseline. For Y2K testing, these tests are repeated for each of the relevant dates in Table 3-1. If the orbit determination inventory item is high risk, operational scenarios and operational data are used to verify that the system meets all operational requirements. The interfaces to the

WSGT and the ground control system will be tested to the maximum extent possible, as described in Table 3-5. If the inventory item is medium **risk,** the operational requirements tested will be determined by the magnitude of the **risk.** If the inventory item is low risk, testing is optional.

3.5.6. **End-to-End Test Level.** End-to-end testing validates **NASA** overall readiness to perform its organizational mission for the Y2K. End-to-end testing validates critical system processing, interfaces, and data across the enterprise through the testing of selected mission or business threads. End-to-end testing verifies that a defined set of interrelated systems, which collectively support a key mission or business function or thread, interoperate as intended in an operational environment. Table 3-6 describes test criteria for end-to-end testing.

Example: Refer to the example described for system testing. Testing a critical thread may consist of receiving current time, position, and attitude data from WSGT, performing orbit calculations, and sending the orbit data over the LAN to one ground control station.

If the enterprise is high risk, critical threads will be tested as described in Table 3-6. If the inventory item is medium risk, selected operational scenarios will be tested. If the inventory item is low risk, end-to-end testing is optional.

The complexity of end-to-end testing varies depending on the type of system In the case of human rated inventory items, the end-to-end testing may involve multiple systems across multiple **NASA** Centers and may involve interfaces external to **NASA. NASA** Centers are responsible for identifying and prioritizing the mission processing threads to be exercised for end-to-end testing and for coordinating with other NASA Centers and external interfaces to **NASA** to support these end-to-end tests.

3.6 **Test Facilities and Test Tools.** Testing on the scale demanded by the Year 2000 program may require a larger, more robust testing environment than may currently exist. Centers should review the applicability of local test environments for Y2K testing and enhance the existing environments where practical.

Centers should evaluate tool libraries that support existing testing activities for applicability to Y2K testing. Where practical, Centers should also consider acquiring additional Y2K test tools if use of the tools provides additional risk mitigation or improves budget/schedule performance.

3.7 **Test Documentation.** Test documentation must be included for low, medium, and high **risk** inventory items. Test plan details may vary depending upon the risk level. For example, a high risk system must have a separate test plan, while a low risk system may use the blank checklist as a test plan and the completed checklist as a test report. Test requirements in Table 3-7 apply to system level tests. Documentation at other test levels shall be consistent with existing Center practices.

3.8. **Test Activity Metrics and Progress Reporting.** Centers should establish processes and metrics for reporting test activity and progress. Metrics should reflect progress against key test milestones and include key indicators of test processes and results.

Table 3-1. Time-Shift Test Dates for Y2K Time Shift Testing

Tests			Risk Level		
Date(s)	Day of Week	Purpose	Low	Medium	High
01/01/1999	Friday	Tests "99" Character Strings	*	*	*
04/09/1999	Friday	Tests "99" Character Strings	*	*	*
09/09/1999	Thursday	Tests Programmers Default Date	*	*	*
12/31/1999	Friday	Tests "99" Character Strings	*	*	*
12/31/1999 > 01/01/2000	Friday > Saturday	Y2K rollover – note 01/01/1900 was a Monday	Required***	Required***	Required
01/01/2000 > 01/02/2000	Saturday > Sunday	Y2K - note 01/02/1900 was a Tuesday	Optional	Optional	Optional
02/28/2000 > 02/29/2000	Monday > Tuesday	Tests Leap Year	Required	Required	Required
02/29/2000 > 03/01/2000	Tuesday > Wednesday	Tests Leap Year	Optional	Optional	Recommended
Day 365>366 (Y2000)	Saturday > Sunday	Julian Day rollover – Leap Year Test	Required**	Required**	Required**
Year 2000, Day 366 > Year 2001, Day 001	Sunday > Monday	Julian Day rollover – Leap Year Test	Optional**	Optional**	Recommended**
02/28/2004 > 02/29/2004	Saturday > Sunday	Tests Leap Year	Optional	Optional	Optional
02/29/2004 > 03/01/2004	Sunday > Monday	Tests Leap Year	Optional	Optional	Optional
Critical Business Dates	System Dependent	Boundary Testing around date	Recommended	Recommended	Required
Window Dates	System Dependent	Tests Window Boundaries and Backward Time Test****	Recommended	Recommended	Required
Random Dates in Year 2000	Varies	Regression test to ensure system works for various dates in the year 2000	Required	Required	Required

Legend
The ">"represents a rollover of the system clock(s) from the first date to the second date.
Critical business dates for accounting systems examples: Fiscal year rollover, quarterly dates, and year-end dates. For non-business systems, dates are those systems refer to dates which trigger periodic system processes such as backup or purge dates, or planning and scheduling processes. Fiscal year end processes need to be tested using 9/30/1997>10/01/1999 to ensure that the fiscal year changes to 2000.
* Strongly recommended for business systems, e.g., payroll, human resources, financial tracking, and those using COBOL. Optional for other systems.
** Requirements apply to systems using Julian Dates only. Requirements do not apply to other systems.

*** Low and medium risk inventory items that opt to power down during the January 1, 2000 rollover are not required to test the 12/31/1999>01/01/2000 date. These inventory items must, at a minimum, conduct time shift testing for random dates in the Year 2000 ensure general functionality is validated.
**** Backward Time Test (for window dates) ensures that 20th century data is accessible when system clocks are set to the 21st century.

Criteria			
	Low	Medium	High
Unit Test	**Required**	**Required**	**Required**
Test Coverage	All functions to maximum extent practical	**Same as Low** Risk	**Same as Low Risk**
Entrance Criteria	Components: Renovated Units except for COTS	Same **as Low** Risk	**Same as Low Risk**
Exit Criteria	Unit: Performs correctly for time-shift dates	Same **as Low** Risk	**Same** as **Low** Risk

Table 3-3. Integration Level Test
(Required only for renovated inventory items. However, may be used to certify COTS products.)

Criteria	Risk Level		
	Low	Medium	**High**
Integration Test	**Recommended**	**Required**	**Required**
'rest Cover ge	Related system components: renovated units except for COTS.	Same as **Low** Risk	Same as **Low** Risk
Entrance Criteria	System Components: Y2K compliant Data: **Test** data aged for time-shift dates	Same as Low Risk	Same as Low **Risk**
Exit Criteria	Renovated system components: Perform to specification for time-shift dates	Same as **Low** Risk	Same as **Low** Risk

Table 3-4. System Level Test

Criteria	Risk Level		
	Low	Medium	High
System Test	Required	Required	Required
Test Coverage	System Functions: Basic Interfaces: Tested to the maximum extent practical based on risk impacts and availability of compliant interfaces. Testing should include data bases, system-to-system, and user interfaces. Interfaces may be simulated. Operational I'rocedures: Review Data: Derived from subsets of operational data.	Systein Functions: Varies based on magnitude of risk Interfaces: Same as Low Risk Operational Procedures: Review & selectively test based on magnitude of risk Data: Same as Low Risk	System Functions : All to niaxiniuni extent practical Interfaces: Same as Low Risk Operational Procedures: Test procedures Data: Same as Low Risk
Entrance Criteria	System Components: Y2K conipliant. Data: Data aged for time-shift dates	Same as Low Risk	Sanie as Low Risk
Exit Criteria	System Functions, Interfaces and Data: Perform correctly for time-shift dates Operational Procedures: Support Y2K operations	Systein Functions, Interfaces and Data: Perform correctly for time-shift dates Operational I'rocedures: Support Y2K operations Perforinance Test (Recommended): Within acceptable limits	System Functions, Interfaces and Data: Perform correctly for time-shift dates Operational Procedures: Support Y2K operations Performance Test (Recommended): Within acceptable limits. Stress Test (Recornmended): Within acceptable limits.

Table 3-5. Acceptance Test Level

Criteria	**Risk** Level		
	Low	Medium	High
Acceptance 'I'est	**Optional**	**Recommended**	**Required**
I'est Coverage	*NIP;*	Varies based on magnitude of risk	System Requirements
Entrance Criteria	N/A	Systems: Certified compliant. Interfaces: Varies based on magnitude of risk Data: Operational Data aged for time-shift dates.	Systems: All certified compliant. Interfaces: Tested to the maximum extent practical. Testing should include data bases, system-to-system, external, and user interfaces. Interfaces may be simulated if testing with operational interfaces is not practical. Data: Operational Data aged for time-shift dates.
Exit Criteria	N/A	System Functions, Interfaces and Data: Perform correctly for time-shift dates.	System Functions, Interfaces and Data: Perform correctly for time-shift dates.

Table 3-6. End-to-End Test Level

Criteria	Risk Level		
	Low	Medium	High
End-to-End Test	**Optional**	**Recommended**	**Required**
Test Coverage	N/A	Selected operational scenarios	Critical Mission Threads
Entrance Criteria	N/A	Systems: Acceptance Tested Interfaces: External interfaces and others that support the operational scenarios Scenarios: Defined for testing; varies based on magnitude of risk Data: Operational Data aged for time-shift dates	Systems: Acceptance Tested. Interfaces: Interfaces that support critical Mission Threads Mission Threads: Defined for testing Data: Operational Data aged for time-shift dates
Exit Criteria	N/A	System Functions & Interfaces perform correctly for the time-shift dates	Operational mission: Meet mission requirements for the time-shift dates

Table 3-7. Test Documentation

Criteria	Risk Level		
	Low	Medium	High
Documentation Maintained by Organization	'lest Plan/Test Procedures: Optional Completed Checklist: Required Certification Form signed by NASA Official: Required	'restPlan/Test Procedures: Optional (depends on risk magnitude). 'lest Report or Completed Checklist: Required Certification Form signed by NASA Official: Required	Test Plan/Test Procedures: Required Test Report or Completed Checklist: Required Certification Form signed by NASA Official: Required

Table 3-8. Y2K Minimum Required Tests Summary

Criteria	Risk Level		
	Low		
Time Shift Dates (applicable to each test level)	12/31/1999 > 01/01/2000 02/28/2000 > 02/29/2000	12/31/1999 > 01/01/2000 02/28/2000 > 02/29/2000	12/31/1999 > 01/01/2000 02/28/2000 > 02/29/2000 Critical Business Dates Window Dates
Random Dates in 2000	Regression tests to Validate Functionality	Regression tests to Validate Functionality	Regression tests to Validate Functionality
Unit Test Level	All functions in renovated unit (except COTS) - to maximum extent practical	All functions in renovated unit (except COTS) - to maximum extent practical	All functions in renovated unit (except COTS) - to maximum extent practical
Integration Test Level	Related system components: renovated units except for COTS. However, may be used to certify COTS products.	Related system components: renovated units except for COTS. However, may be used to certify COTS products.	Related system components: renovated units except for COTS. However, may be used to certify COTS products.
System Test Level	System Functions: Basic Interfaces: Maximum extent practical based on risk impacts Operational Procedures: Review Data: Derived from subsets of operational data	System Functions: Varies based on magnitude of risk. Interfaces: Maximum extent practical based on risk impacts Operational Procedures: Review & selectively test based on magnitude of risk Data: Derived from subsets of operational data.	System Functions : All Interfaces: Maximum extent practical based on risk impacts Operational Procedures: Test Procedures Data: Derived from subsets of operational data
Acceptance Test Level			System Requirements
End-To-End Test Level			Critical Mission Threads

Section 4. Guidelines on Y2K Compliance Criteria

This section provides general guidelines for NASA Centers to follow when determining the compliance of inventory items. Inventory items should satisfy four date-related criteria; items meeting all four can be considered "Y2K-compliant." Table 4-1 lists criteria for use in assessing inventory items for Y2K compliance.

Table 4.1. Criteria for Y2K Compliance

Criterion	Description
General integrity	No value for current date will cause interruptions in normal operation.
Date integrity	All manipulations of calendar-related data (dates, durations, days of week, etc.) will produce desired results for all valid date values within the application domain.
Explicit century	Date elements in interfaces and data storage permit specifying century to eliminate date ambiguity.
Implicit century	For any date element represented without century, the correct century is unambiguous for all manipulations involving that element.

4.1. Criteria for Y2K compliance. Criterion serves as a high-level requirement for hardware and software. The following discussion elaborates on each:

4.1.1. **General integrity**. As a system date advances normally on a host processor, each date rollover must not lead either the host process or any software executing there to erroneous processing. The best recognized high-risk date change is the rollover to 2000. The term "desired results" in Table 4-1 is intentionally broad and must be interpreted for specific technologies and applications.

4.1.2. **Date integrity**. This criterion primarily covers the correctness of manipulations of date data as enumerated in Table 4-2. These manipulations need to be reliable only over the range of dates that an application is expected to handle. For example, sales-order processing may handle dates from 5 years in the past to 1 year in the future. In contrast, an employee database may store dates of birth from early in the 20th century to planned retirement dates well into the 21st century.

4.1.3. **Explicit century.** This criterion essentially requires the capability to store explicit values for century. For example, third-party products that can use a 4-digit year in all date data elements stored and passed across each interface (including the user interface) would satisfy this criterion. A base-and-offset representation of dates that covers all centuries of interest would also satisfy this criterion. Whether this capability should be used to eliminate century ambiguity is part of the last criterion.

Table 4-2. Variety of Manipulation of Date Data

Category	Examples of manipulation
Arithmetic	• Calculate the duration between two dates • Calculate date based on starting date and duration • Calculate day of week, day within year, week within year
Branching	• Compare two dates
Format	• Convert between date representation (YMD, Julian, etc.) • Reference same data address with different variables
Data storage	• Storing and retrieving • Sorting and merging • Searching • Indexing on disk file or database table • Moving data within primary memory
Extended semantics	• "99" as special value for year • "99.365" as special value for Julian date • "00" as special value for year

4.1.4. **Implicit century.** This last criterion requires that, if the century is not explicitly provided, its value can be correctly inferred with 100 percent accuracy from the value of date provided. For example, the range of values for an "invoice date" would very rarely span more than 10 years. Because the century can always be guessed correctly for an invoice date with a 2-digit year, this date data element would satisfy this criterion. Note that this criterion permits cost-risk tradeoffs that minimize changes to existing date formats.

4.2. **Interpretation of the Criteria.** Although the four criteria fully define Y2K compliance, compliance represents a balance between cost and risk rather than an absolute "yardstick." Such a balance will vary according to programmatic or business needs and technology. Table 4-3 contains an interpretation of the criteria as an example. Note the importance of clearly identifying the calendar by name, the specific date ranges for relevant compliance, reasonable latitude in date format, and situations under which implicit century values will be tolerated. Also note that certain exceptions are included to support important options for optimal cost/risk tradeoff.

4.3. Standardizing the format for date data is an important part of Y2K compliance. For **NASA** systems, the Federal Information Processing Standard (FIPS) **4**-1, *Representation of Calendar Date and Ordinal Date for Information Interchange,* applies. FIPS **4**-1 adopts the **ANSI** standard X3.30-1988(R1991). The standard provides for implementation of both **4**-

digit and 2-digit year formats in date information. In March 1996, the National Institutes of Standards (NIST) issued a change notice to the standard recommending the use of the 4-digit year format in information that is interchanged with other organizations. Also, in March 1996, NIST issued a Computer Systems bulletin on "The Millennium Rollover: The Y2K Problem."

4.4. NASA will use only the 4-digit date format defined in FIPS 4-1 for external data exchanges, unless an alternative format is mutually negotiated, and will follow the guidance contained in the March 1996 MST bulletin. The year should encompass a 2-digit century that precedes, and is contiguous with, a 2-digit year-of-century (e.g., 1999, 2000, etc.). The 4-digit date format is recommended but not required for internal **NASA** systems and applications. Alternative formats or expansion approaches (e.g., windowing)–may be appropriate given cost or other technical considerations.

Table 4-3. Interpretive Example of Y2K Compliance Criteria

Criterion	Description of criterion	Interpretation of criterion
General integrity	No value for current date will cause interruptions in normal operation.	• All software on all platforms will function correctly for all values of system date between 1955-01-01 and 2035-12-31. • Of special interest are the following dates and the ability to roll over to the correct next date: 1998-12-31, 1999-09-09. 1999-12-31, 2000-01-01, 2000-02-28, 2000-02-29, 2000-03-01, 2000-12-31.2001-01-01
Date integrity	All manipulations of calendar-related data (dates. durations. days of week. etc.) will produce desired results for all valid date values within the application domain.	• All date values and calculations are based on the Gregorian calendar as defined in *Encyclopedia Britannica*, 15th edition. 1994. p. 430. • Computing assets must correctly handle all representation and manipulation of dates with values between 1900-01-01 and 2050-12-31. Especially important is that all years in this 150-year range divisible by 4 are leap years except 1900. • All software developed for NASA must initialize all date elements with either all zeros (0000-00-00) or null values. Null values are defined for each application by the development facilities. such as language compilers. A null-value feature is strongly recommended in third-party-software selection. • All developed software must not contain literals or constants for dates unless required to capture specific business rules such as calculations of payroll deductions. • All developed software must not use special date values as logical flags, such as "99" as year to mean "no end date" or "00" to mean "does not apply." Exceptions: Valid date ranges in existing developed or existing third-party software may start with the oldest date value in the application's archived data rather than with 1900-01-01 when there is no business need to supoort earlier dates.
Explicit century	Date elements in interfaces and data storage permit specifying century to eliminate date ambiguity	• All developed and third-party software must permit the use of date formats that explicitly specify century in all date data stored or transmitted. The format of these date elements muss be YYYYMMDD or YYYYJJJ as specified by ANSI X3.30-1985(R1991) unless superseded by another application-specific standard or convention. • In storing or transmitting date data. some applications must conform to domain-specific standards, contractual agreements. or application program interfaces to necessary third-party products whose date formats must supersede ANSI X3.30 as appropriate within the application. • Third-party products must permit formatting data with explicit century in the user interface. • All developed applications using third-party products must always explicitly supply century and never rely on those products' default value for century. Exceptions: • For date data formatted for a user interface, it is acceptable to use punctuation (slash, hyphen. period. comma) within a formatted date, to spell out or abbreviate the name of the month, or to reorder year-month-day to serve customs among the end-users. • DBMSs that cannot store date in conformance with SQL standards but do store century explicitly (such as "DD-mmm-YYYY") are acceptable. • Default values for century are permitted only when supplied by data-entry aids and the end-user can verify the defaulted value before committing the data.
Implicit century	For any date element represented without century. the correct century is unambiguous for all manipulations involving that element.	• Century must be explicit in all date data stored or transmitted unless the correct century *can* be. inferred with 100% accuracy based on the value for date. Explicit century is preferred where practical. Developed and third-party software may imply century in the user interface in the format, YYMMDD or YYJJJ (as specified by ANSI X3.30). • In storing or transmitting date data. some applications must conform to domain-specific standards whose requirements for dates may supersede ANSI X3.30 as appropriate within the application. Exceptions: For date data formatred for a user interface. it is acceptable to use punctuation such as slash within a formatted date. to spell out or abbreviate the nanie of the month. or to reorder year-month-day to serve customs among the end-usen.

Appendix A

Certification Signoff Form Examples

APPENDIX AI
NASA Center Level

Y2000 Inventory Item Certification for

Vendor Certified Products

Completion of this form indicates that the vendor documentation certifies the listed products are Y2K compliant.

NASA Center: _____

Inventory Item	Inventory No.	Date Certified	NASA Manager	NASA Manager Signature	Date

Comments:

I certify these inventory item meets the **NASA** Y2000 compliance requirements.

Y2000 Project Manager

Name _____ Signature _____ Date _____

APPENDIX A2
NASA Center Level

Y2000 Inventory Item Certification

for NASA Tested Items

Completion of *this* form indicates that the inventory item identified below including its components (hardware, software, firmware, and COTS) has passed the **NASA** Y2K required test. Based on these tests, the inventory item is now ready for operational or production use.

NASA Center: _____ Inventory Item: _____ Inventory No. _____

Date Certified: _____ Mission Critical ____ Non-Mission Critical ____

Risk Level: _____ Level of Test Conducted_____

Comments:

I certify this inventory item successfully meets NASA Y2000 test requirements commensurate with its **risk** level.

NASA Manager

Name _____ Signature _____ Date _____

Y2000 Project Manager

Name _____ Signature _____ Date _____

APPENDIX A3
NASA Center Level

Y2000 Inventory item Certification

For Not Date Affected Items

Completion of this form indicates that the inventory items identified below are not affected by the Y2K rollover.

NASA Center: _____

Inventory Item	Inventory No.	Date Certified	NASA Manager	Manager Signature	Date

Comments:

I certify that the inventory items above are not date affected.

Y2000 Project Manager

Name _____ Signature _____ Date _____

Appendix B

Certification-Checklist Example

Appendix B
Sample NASA Y2K Compliance Checklist

NASA Manager _____ **Date** _____

Inventory Item _____ **Inventory No.** _____

The purpose of this checklist is to ensure **NASA** inventory item components are Y2K compliant. This form is to be used for the Y2K testing and certification process for all of the developed, COTS and Government off-the-shelf (GOTS) software, hardware, and firmware.

Please respond to each question with the appropriate answer.

1. Please urovide uroduct information	
a. Name of product	
b. Name of Vendor (if COTS or GOTS)*	
c. Operational date of product (current or a future date)*	
d. Planned or actual replacement/retirement date of product	Retirement date_____ Replacement date_____
e. For planned replacements what is the contingency plan and under what conditions will it be invoked?*	
f. What are the safety critical portions of the product if any?"	
2. Each product has its own window of time, before and after the present date, in which it functions. Planning and scheduling products work with dates that are weeks, months, and years in the future. For your product and its window of time, verify its ability to successfully process data containing dates with no adverse effect on the application's functionality and with no impact on the customer or end user beyond adjustment to approved changes in procedures and data formats.	
a. Dates in 20" century (1900s)	Verified ( ) No( ) N/A( )
b. Dates in 21" century (2000s)	Verified ( ) No( ) N/A( )
c. Dates across century boundary (mix 1990s & 2000s)	Verified ( ) No( ) N/A( )

d. Crosses 1999 to 2000 successfully	Verified ( ) No( ) N/A( )

Other/Indirect Date Usage	
3. Have you verified performance (and corrected if necessary)?	
a. Dates embedded as parts of other fields	Verified ( ) No( ) N/A( )
b. Dates used as part of a sort key	Verified ( ) No( ) N/A( )
c. Usage of values in date fields for special purposes that are not dates (e.g. using 9999 or 99 to mean "never expire")	Verified ( ) No( ) N/A( )
d. Date dependent activation/deactivation of: passwords, accounts, commercial licenses	Verified ( ) No( ) N/A( )
e. Date representation in the operating product's file product (creation dates and modification dates of files and directories)	Verified ( ) No( ) N/A( )
f. Date dependent audit information	Verified ( ) No( ) N/A( )
g. Date dependencies in encryption/decryption algorithms	Verified ( ) No( ) N/A( )
h. Date dependent random number generators	Verified ( ) No( ) N/A( )
i. Date dependencies in firmware	Verified ( ) No( ) N/A( )
j. Personal Computer BIOS and RTC does not reset the year to 1980 or 1984 on reboots after 31 Dec 1999 (corrections by operating product utilities allowed)	Verified ( ) No( ) N/A( )
Leap Year	
4. Product accurately recognizes and processes Year 2000 as a leap year.	
a. February 29, 2000 is recognized as a valid date	Verified ( ) No( ) N/A( )
b. Julian date 00060 is recognized as February 29, 2000	Verified ( ) No( ) N/A( )
c. Julian date 00366 is recognized as December 31, 2000	Verified ( ) No( ) N/A( )
d. Arithmetic operations recognize Year 2000 has 366 days	Verified ( ) No( ) N/A( )
Usage of **Dates Internally**	
5. Internal application usage of dates and date fields must be clear and unambiguous in the context of the products which use them.	
a. Display of dates is clear and unambiguous (the ability to correctly determine which century a date belongs either by explicit display, i.e. 4-digit year,	Verified ( ) No( ) N/A( )

or product or customer inference)	
b. Printing of dates is clear and ,unambiguous	Verified ( ) No( ) N/A( )
c. Input of dates is clear and unambiguous	Verified ( ) No( ) N/A( )
d. Storage of dates is clear and unambiguous	Verified ( ) No( ) N/A( )
6. External interactions are identified and validated to correctly function for all dates.	
a. Interaction between this product and any other external time source. if existing, has been verified for correct operation.	Verified ( ) No( ) N/A( )
b. You and the responsible organization for each interface have negotiated an agreement dealing with Year 2000 issues	Verified ( ) No( ) N/A( )
Date Field Type	
7. Describe the type of date fields used by the Product, in either software or databases:	
a. Does the product use 4-digit year data fields?	Verified ( ) No( ) N/A( )
b. Does the product use 2-digit Year data fields'?	Verified ( ) No( ) N/A( )
c. If 2 digit, does the product use a century logic technique to correctly infer the century'?	Verified ( ) No( ) N/A( )
d. At what date will the century logic fix fail?	
e. Are there any internal data types for dates'?	Yes( ) No ( )
If yes to e, what is the range of dates that the date field can represent'?	
Year 2000 Testing Information	
8. Please provide the following information with regard to testing the product for Year 2000 compliance	
a. Testing Organization	
b. Name of Test Team Chief	
c. Date that Year 2000 compliance testing was completed	
d. How was Year 2000 compliance determined'? (certified by vendor or contractor, tested in-house, inspected but not tested, etc.)	
e. Are the test data sets available for regression testing on the next-version release for questions 2,3,4,5,6,7d, and 7e?	Yes( ) No ( )

f. Are the detailed test results and reports available for review and audit for questions 2,3,4,5,6,7d, and 7e?	Yes ( ) No ( )
g. Do you follow a defined process for tracking the status of all Year 2000 problems reported, changes made, testing, compliance, and return to production?	Yes ( ) No ( )

Name of Interface External to the Inventory Item	Interfacing System	Test Date	NASA Signature

Component Name	H/W S/W F/W COTS	Test Date	NASA Signature

Appendix *C*

Glossary of Terms

July **2,** 1998

Appendix C
Glossary of Terms

Acceptance Testing

Testing the entire information system, including interfaces with operational data.

Application

A computer program designed to help people perform a certain type of work. Depending on the work for which it was designed. an application can manipulate text, numbers, graphics, or a combination of these elements.

Application testing

Required for each converted **or** replaced application.

Backward time testing

The ability to access all twentieth century data when system clocks are set to twenty-first century dates.

Baseline testing

Establishes the functional, interoperability, and performance baselines for system components undergoing Year 2000 renovation in advance of the application of the conversions. Such a baseline serves as the expected results for any regression testing after renovation.

Business area

A grouping of business functions and processes focused on the production of specific outputs.

Business cycle date

Recurring dates established because of the business cycle (e.g. payday, month end, year-end, quarterly reporting).

Business function

A group of logically related tasks that are performed together to accomplish an objective.

Business risk

The possibility that a business operation or service will fail because of a Y2K problem.

Certification

Indicates that an inventory item, including its system component (hardware, software, firmware, and COTS), has passed the **NASA** Year 2000 test criteria on the basis of its **risk** level. Vendors may also certify Y2K compliance.

Component

A single resource with defined characteristics. The component concept is used in defining precise specifications for testing the validity of various resources. These components are also defined by their relationship to other components.

Configuration management

The continuous control of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.

Contingency plan

In the context of the Year 2000 program, a plan for responding to the loss of a system because of a Year 2000 problem. In general, a contingency plan describes the steps the enterprise would take--including the activation of manual or contract processes--to ensure the continuity of its core business processes in the event of a Year 2000-induced system failure.

Conversion

The process of making changes to databases or source code.

Critical process

An information processing function needed to deliver a primary business service or mission objective.

Critical thread

Threads are a subset of processes and datasets (data threads) across an enterprise that produces or delivers a service or end product. Critical threads are those enterprise or end-to-end threads that are critical to the business or mission.

Database

An aggregation of data; a file consisting of a number of records or tables, each of which is constructed of files of a particular type, together with a collection of operations that facilitate searching, sorting, recombination, and similar operations.

End-to-End testing

Validation of all system processing, interfaces, and data across the enterprise by testing critical threads.

Entrance criteria

Conditions needed to begin testing.

Exit criteria

Conditions needed to successfully complete testing.

High Risk System

The system is classified as high‘risk if it meets any one of the following three criteria:

- Safety or human life is jeopardized by long or short term disruption of the service or product.
- Unscheduled disruptions in the service or product cannot be tolerated.
- Unscheduled disruption of service will put **NASA** at a disadvantage

Infrastructure

The computer and communication hardware, software, databases, people, and policies supporting the enterprise’s information management functions.

Integration testing

Testing to determine that the related information system components perform to specification.

Interface

A boundary across which two systems communicate. An interface might be a hardware connector used to link to other devices, or it might be a convention used to allow communication between two software systems.

Inventory

In the context of a Year 2000 program, the process of determining the components that comprise the agency’s systems portfolio. The inventory should include all applications, databases, files, and related system components that will require inspection to locate date data and related date computations.

Low Risk System

The system is classified as low risk if it meets either of the following criteria:

- Long duration, unscheduled disruption in the service or product can be tolerated. For example, disruption for up to 25 hours can be tolerated.
- Alternative means can provide a minimum-level of the same service or product.

Medium Risk System

The system is classified as medium **risk** if it meets either of the following criteria:

- Unscheduled disruptions for more than a short period of time will put NASA at a disadvantage. For example, disruptions for more than 1 hour will put NASA at a disadvantage.
- Only short duration, unscheduled disruptions in the service or product can be tolerated. For example, unscheduled disruptions for 3 hours or less can be tolerated.

Metrics

Means by which software engineers measure and predict aspects of processes, resources, and products that are relevant to the software engineering activity.

Mission-critical System

Mission Critical System - A system is classified mission critical if it meets any one of the following four criteria:

- Requires special management attention because of its importance to the Agency mission or impact on the administration of Agency programs, finances, property, or other resources.
- Involves functions that affect safety or human life.
- System has high impact or risk. Negative impact on system would place **NASA** at significant or irreparable disadvantage. Failure has potential for catastrophic or significant loss of tangible assets or resources.
- Significant financial value.

Non-Mission Critical System

The system is non-mission critical if it meets any one of the following two criteria:

- Requires management attention because it supports important, but non-mission critical, functions or processes.
- System has minimal impact and risk. Negative impact on system would have minimal impact on missions or critical administrative processes. Failure has potential for loss of some tangible assets or resources.

Operating system

The software that schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running.

Performance testing

Testing to assess how well a system meets specified performance requirements. Examples of performance requirements include specified system response times under normal workloads (e.g., defined transaction volumes) and specified levels of system availability and mean times to repair.

Platform

The foundation technology of a computer system. Typically, a specific combination of hardware and operating system.

Production

The system environment where the agency performs its routine environment information processing activities.

Regression testing

Testing to demonstrate that newly added or modified system components (hardware or software) have not compromised system functionality and performance (i.e., have not introduced new errors).

Renovation

Conversion of an existing application.

Replacement

Development of a new application or upgrade of an existing application.

Retirement

Decommissioning of an existing application or component.

Risk assessment

A continuous process performed during all phases of system development to provide an estimate of the damage. loss, or harm that could result from a failure to successfully develop individual system components.

Risk based testing

Selective testing of system components, interfaces and data based on impacts of their failures to the business or mission.

Risk management

A management approach designed to reduce risks inherent to system development.

Standard

In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development.

Stress testing

Testing to analyze system behavior under increasingly heavy workloads (e.g., higher transaction rates) and severe operating conditions (e.g., high error rates and lower component availability rates).

System testing

Testing to determine that the results generated by the enterprise's information systems and their components are accurate and that the systems perform to specification.

Test

The process of exercising a product to identify differences between expected and actual behavior.

Test facility

A computer system isolated from the production environment dedicated to testing and validating applications and system components.

Time shift test

Setting system clocks to a future date for validation of Year 2000 compliance.

Unit testing

Testing to determine that individual program modules perform to specification.

Utilities

Computer programs designed to perform maintenance work on the system or on system components--for example, a storage backup program, a disk or file recovery program, or a resource editor.

Validation

The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

Windowing

A technique for inferring the century from 2-digit year dates. Example: all years 70-99 are interpreted as century 1970-1999, and all years 00-69 are interpreted as 2000-2069.

Window boundaries

Dates at the extremes of the windows. For the Windowing example, window boundaries are 69-71 and 99-01.

Window dates

2-digit year dates occumng within a window. For the Windowing example, 70 - 99 are window dates.

Year 2000 compliant

"Year 2000 compliant" means, with respect to information technology, that the information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it." (48 CFR Part 39.002)

Year 2000 critical business cycle date

Information system critical processing dates (e.g. day of the week, month, quarter, year) determined by the business cycle.

Year 2000 event horizons

The first date prior to January 1, 2000 that systems encounter a date on or after January 1, 2000 and the last date on or after January 1, 2000 that systems encounter a date prior to January 1, 2000.

Year 2000 problem

The potential problems and its variations that might be encountered in any level of computer hardware and software from microcode to application programs. files, and databases that need to correctly interpret year-date data represented in 2-digit-year format.

Appendix D

Date Dependency Checklist

July 2, 1998

Appendix D
Date Dependency Checklist

The following is a sample list of common date usages found in automated information systems. Components of inventory items not impacted by dates will exhibit none of these date usages. A specific inventory component may, however, require that additional forms of date usage be examined to determine date dependency (or non-dependency) because of the nature of the component and/or its functionality. Similarly. some forms of date usage may not apply to a given component.

Note that various date formats may be employed in each of the usages identified in the checklist below and that verification of non-date dependency may require checking for several different date formats for a given usage. Verification may be accomplished by various means, for example, inspection, observation, scanning, or by using automated tools (e.g., commercial Y2K code scanners), as appropriate for the component.

In general, for compliance assessment purposes, a component of an inventory item is said to have no date impact if the following conditions apply:

- There is no use of dates in the component.
- No dates are generated within the component.
- No date manipulation/calculations/comparisons are performed.
- No date logic of any kind is performed.
- No date moves are performed.
- Dates are neither input nor output from the component.
- Although date fields are not used for date representations, it is ensured they are also not used for other purposes such as "9's comparison" fields (e.g., use of 9999 as a termination code)

Data Dependency Checklist

Inventory Item: _____ Inventory No.: ____

Inventory Item Component Name and Version/Date/Model Number (as appropriate): _____

_____

Organization Performing Date Dependency Check: _____

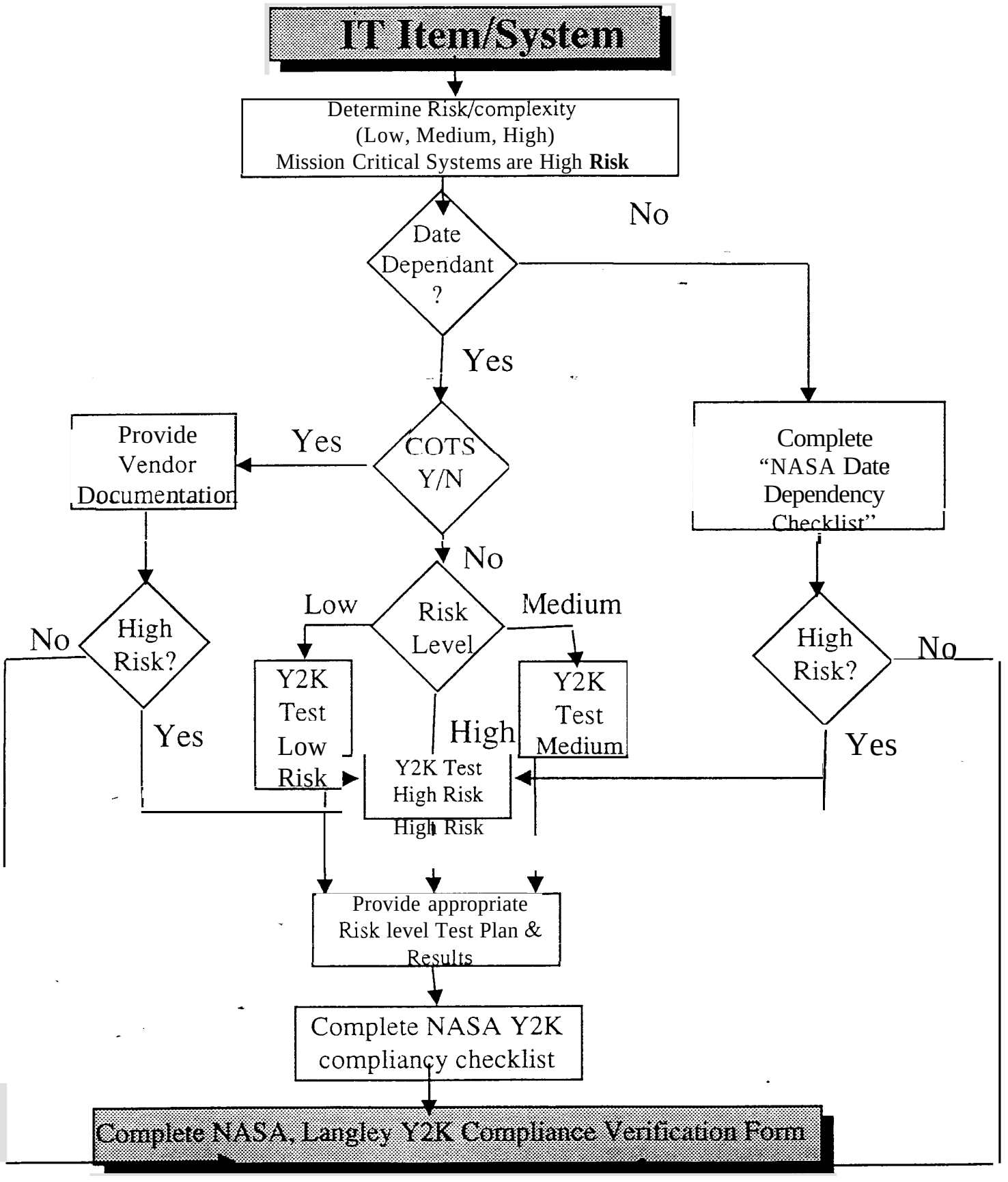
Name of Individual/Team Lead Performing Date Dependency Check: _____

Checklist	Yes	No	N/A	How Verified
Date used explicitly in code				
Date calculations in computation algorithms				
Dates embedded as parts of other fields				
Dates used as part of a sort key				
Use of data files with dates in them				
Usage of values in date fields for special purposes that are not dates (e.g. using 9999 or 99 to mean "never expire").				
Date-dependent activatioddeactivation of: passwords, accounts, commercial licenses				
Date-dependent activatioddeactivation of: scripts. subprograms, programs, other code execution				
Date-dependent activatioddeactivation of system functionality, alarms, exception procedures				
Date-dependent activatioddeactivation of operational procedures, backups, logging				
Date representation in file products (creation dates and modification dates of files and directories)				
Date dependent audit information				
Date dependencies in encryption/decryption algorithms				

Checklist	Yes	No	N/A	How Verified
Date-dependent random number generators				
Use of internal data types for dates				
Use of system date utilities or functions				
Use of software libraries that employ date functions, date-related information, or accept date input				
Date dependencies in firmware				
Display of dates				
Printing of dates				
Graphical displays or plots that portray date-related information				
Operator input of dates				
Operator input information (e.g., commands-data) that may be date-related				
Input of dates from disk				
Input of dates from tape				
Input of dates from CD ROM				
Input of dates from databases				
Input of dates from external systems				
Messages or E-mail that contain dates in header infomation				
Storage of dates on disk				
Storage of dates on tape				
Storage of dates on CD ROM				
Storage of dates in databases				
Data transfers across external interfaces, either as input to the component or output from it.				
Programmable Logic Controller (PLC) date displays				
Embedded systems or subsystems that employ dates				
Digital panels/readouts containing dates				

Y2K COMPLIANCE VERIFICATION

Decision Tree For Documentation And Testing: Requirements



BASED ON "NASA YEAR 2000 AGENCY TEST AND CERTIFICATION GUIDELINES AND REQUIREMENTS"

NASA Langley Research Center
Y2K (Y2000) Compliance Verification Form

- IT Item Name/System, Short Description & Risk Level

- Documentation attachments (check off the applicable)

  - ☐ No Date Dependency Checklist
  - ☐ Vendor Documentation for COTS Products (Software, Hardware, Firmware)
    specify _____
  - ☐ Y2K Test Plan (appropriate to risk level)
  - ☐ Y2K Test Results (appropriate to risk level)
  - ☐ System Documentation
  - ☐ Y2K Compliancy Checklist
  - ☐ Project Plan for major Y2K Renovations
  - ☐ Other _____

- Comments:

I certify the IT Item/System provided has been tested for Y2K compliance in accordance with **"NASA** Y2000 Test and Certification Guidelines and Requirements" document and that the test(s) results indicate that the IT Item/System is compliant. -

-Contractor Official _____ Date _____

Concurrence

-NASA (Technical Official) _____ Date _____