United States General Accounting Office

GAO

Accounting and Information
Management Division

August 1998

Year 2000 Computing Crisis: Business Continuity and Contingency Planning

GAO/AIMD-10.1.19

Preface

Time is running out for solving the Year 2000 problem. Many federal agencies will not be able to renovate and fully test all of their mission critical systems and may face major disruptions in their operations. At the same time, systems that have been renovated and tested may encounter unanticipated Year 2000 problems.

Despite the efforts of each business, state and local government, and federal agency to race against time and to renovate, validate, and implement their mission-critical information systems every organization remains vulnerable to the disruption of its business processes. Because most federal organizations are highly dependent on information technology to carry out their business, Year 2000-induced failures of one or more mission critical systems may have a severe impact on their ability to deliver critical services. For example:

- The nation's air transportation may face major delays and disruptions because the airlines may not be able to file flight plans with the Federal Aviation Administration.

- Taxpayers may not receive timely tax refunds because the Internal Revenue Service may be unable to process their tax returns.

- Payments to veterans and retirees may be delayed or disrupted by the failure of mission-critical systems supporting the nation's benefit payment systems.

- College students may not receive student education loans promptly.

The risk of failure is not limited to the organization's internal information systems. Many federal agencies also depend on information and data provided by their business partners—including other federal agencies, hundreds of state and local agencies, international organizations, and private sector entities. Finally, every organization also depends on services provided by the public infrastructure—including power, water, transportation, and voice and data telecommunications.

Because of these risks, agencies must have business continuity and contingency plans to reduce the risk of Year 2000 business failures. Specifically, every federal agency must ensure the continuity of its core business processes by identifying, assessing, managing, and mitigating its Year 2000 risks. This effort should not be limited to the risks posed by the Year 2000-induced failures of internal information systems, but must include the potential Year 2000 failures of others, including business partners and infrastructure service providers. One weak link in the chain of critical dependencies and even the most successful Year 2000 program will fail to protect against major disruption of business operations.

The business continuity planning process focuses on reducing the risk of Year 2000-induced business failures. It safeguards an agency's ability to produce *a minimum acceptable level* of outputs and services in the event of failures of internal or external mission-critical information systems and services. It also links risk management and mitigation efforts to the agency's Year 2000 program, and helps to identify alternate resources and processes needed to operate the agency core business processes. While it does not offer a long-term solution to Year 2000-induced failures, it will help the agency to prepare for a potential crisis, and may facilitate the restoration of normal service at the earliest possible time in the most cost-effective manner.

This guide provides a conceptual framework for helping large agencies to manage the risk of potential Year 2000-induced disruptions to their operations. It provides information on the scope and challenge and offers a structured approach for reviewing the adequacy of agency Year 2000 business continuity and contingency planning efforts.

The guide addresses business continuity and contingency planning issues that are common to most large enterprises. Given the many differences among organizations, we are not prescribing a single, rote approach to business continuity planning. Agencies must tailor their Year 2000 business continuity planning efforts in response to their unique needs while ensuring that the guide's concepts and principles are effectively applied in their business environment to achieve necessary results in the most cost efficient manner.

The guide builds upon our previously issued Year 2000 assessment guide,[1] and draws on a variety of other sources, including research and publications of the Gartner Group, the Disaster Recovery Institute of Canada, the Department of Information Resources for the State of Texas, and the Electrical Engineering Institute of England.

The guide addresses four phases supported by program and project management activities:

- Initiation,
- Business Impact Analysis,
- Contingency Planning, and
- Testing.

In addition to program and project management, the four phases are united by a common theme of accountability at all levels.

If you have any comments or questions about the guide, please contact us, or E. Randolph Tekeley, Technical Assistant Director, at (202) 512-4070; or Mirko J. Dolak, Technical Assistant Director, at (202) 512-6362. We can also be reached by e-mail at ***willemssenj.aimd@gao.gov***, ***rhodesk.aimd@gao.gov***, ***tekeleye.aimd@gao.gov,*** *and* ***dolakm.aimd@gao.gov.***

[1] Year 2000 Computing Crisis: An Assessment Guide, (GAO/AIMD10.1.14, issued as an exposure draft in Feb. 1997; issued final in Sept. 1997).

An electronic versions of this guide is available from GAO’s World Wide Web server at the following Internet address: ***<http://www.gao.gov/special.pubs/bcpguide.pdf>.***

Joel Willemssen

Joel C. Willemssen
Director
Civil Agencies Information Systems

Keith A. Rhodes
Technical Director
Office of the Chief Scientist

Contents

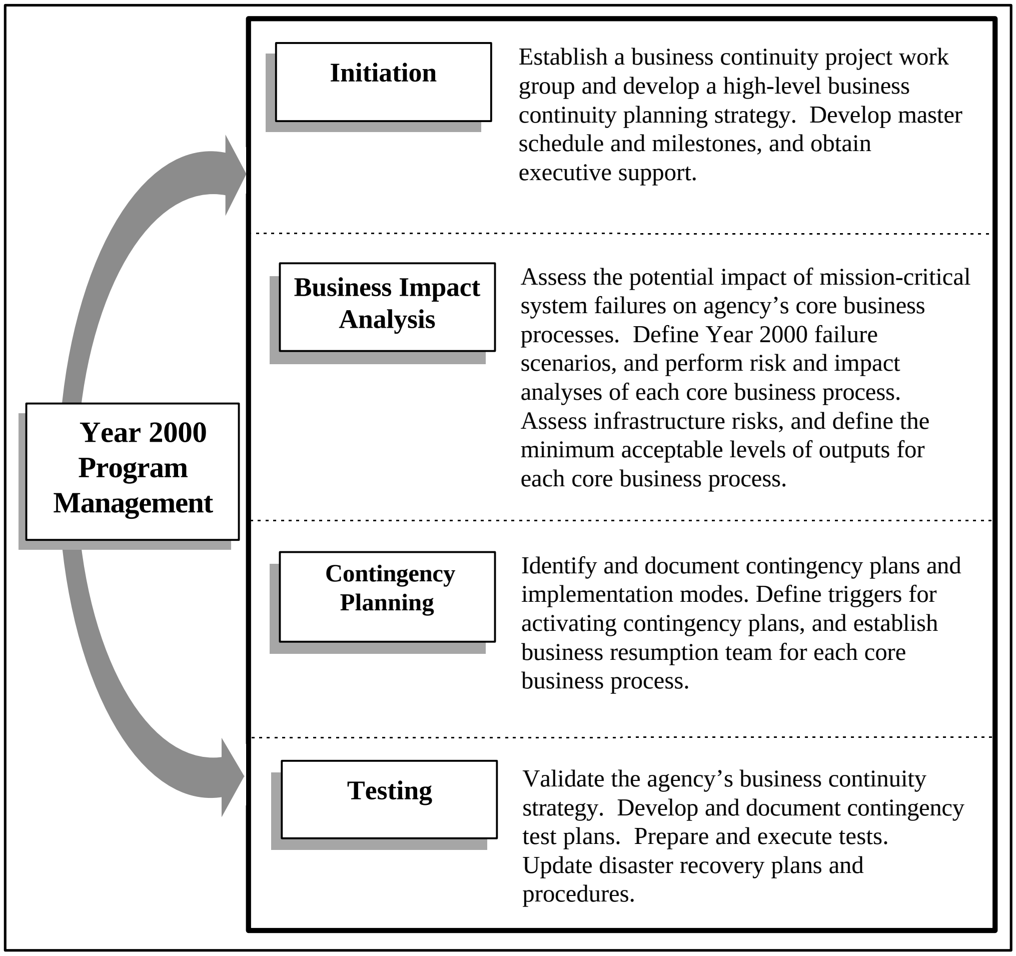
Business Continuity Planning and the Year 2000 Problem

The Year 2000 problem, while technical in nature, is primarily a business problem, with many organizations facing the risk of Year 2000-induced interruptions or failures of their core business processes. Time is running out and many federal organizations may not be able to renovate or replace all of their mission critical systems in time. Organizations must reduce the risk and potential impact of Year 2000-induced information system failures on their core business processes by implementing rigorous business continuity planning processes.

This guide presents a structured approach to aid federal agencies in business continuity and contingency planning. The guide draws on the work of leading organizations in the information technology industry and incorporates their guidance and practices. Many of the Year 2000-related concepts and practices presented in the guide build upon existing best practices in the contingency and disaster recovery areas.

The guide describes four phases--supported by agency Year 2000 program management--with each phase representing a major Year 2000 business continuity planning project activity or segment.

Year 2000 Business Continuity Planning Structure



Initiation

Establish a business continuity project work group and develop a high-level business continuity planning strategy. Develop master schedule and milestones, and obtain executive support.

Business Impact Analysis

Assess the potential impact of mission-critical system failures on agency's core business processes. Define Year 2000 failure scenarios, and perform risk and impact analyses of each core business process. Assess infrastructure risks, and define the minimum acceptable levels of outputs for each core business process.

Contingency Planning

Identify and document contingency plans and implementation modes. Define triggers for activating contingency plans, and establish business resumption team for each core business process.

Testing

Validate the agency's business continuity strategy. Develop and document contingency test plans. Prepare and execute tests. Update disaster recovery plans and procedures.

1.0 Initiation

Executive management needs to be fully aware of the potentially devastating financial, organizational, and political consequences of the failure of one or more mission-critical information systems. Executives responsible for the agency's core business processes must work with the Chief Information Officer, the Chief Financial Officer, and the Year 2000 program manager to reduce the risk of Year 2000-induced business failures. Agency managers must dedicate sufficient resources and staff for the business continuity planning tasks, and ensure that senior managers support this effort.

Key Processes

1.1 Establish a business continuity project work group
1.2 Develop and document a high-level business continuity planning strategy
1.3 Identify core business processes
1.4 Define roles and assign responsibilities
1.5 Develop a master schedule and milestones
1.6 Implement a risk management process and establish reporting system
1.7 Assess existing business continuity, contingency, and disaster recovery plans and capabilities
1.8 Implement quality assurance reviews

1.1 Establish a business continuity project work group

Establish, within the agency's Year 2000 program office, a business continuity work group. The group should report to executive management and include representatives from the agency's major business units, domain experts in relevant functional areas, business continuity and disaster recovery specialists, operational analysts, and contract specialists. Access to legal advice is also a necessity. This group should work closely with the Year 2000 program manager and staff to ensure access to information on the status of the agency's Year 2000 renovation, validation, and implementation efforts.

1.2 Develop and document a high-level business continuity planning strategy

A high-level business continuity planning strategy provides the agency's executive management with a high-level overview of the Year 2000 business risks and solutions. The strategy should address the project structure, its relationship with the Year 2000 program, metrics and reporting requirements, and the initial cost and schedule estimates.

The risk of business failure is not limited to the organization's internal information systems, but includes risks associated with the potential failure of embedded microprocessors installed in a wide range of building and industrial process control systems. Many federal agencies also depend on information and data provided by their business partners—including other federal agencies, hundreds of state and local *agencies, international organizations, and private sector entities. Finally, every organization also depends on services provided by the public infrastructure--including power, water, transportation, and voice and data telecommunications.*

1.3 Identify core business processes

Analyze agency business plans and work with business process owners and Year 2000 program staff to identify core business processes and supporting mission-critical systems for each business area. Ensure that all key business dependencies are clearly identified, including infrastructure and external sources of critical supplies and information. Identify executives responsible for the operation and continuity of each core business process. Use ownership of core business processes to promote executive ownership of the planning effort.

1.4 Define roles and assign responsibilities

Define roles and assign responsibilities for leading the planning effort and for performing analyses and designing business alternatives, including contingent operations for sustained and prolonged disruption. Appoint individuals to lead the development of contingency plans for each of the core business processes. Define responsibilities for documenting the business continuity plan and defining the essential operational activities comprising it.

Ensure that individuals responsible for the various business continuity and contingency planning activities are held accountable for the successful completion of individual tasks, and that the core business process owners are responsible and accountable for meeting the milestones for the development and testing of contingency plans for their core business processes.

1.5 Develop a master schedule and milestones

Develop a schedule for the planning effort and the delivery of interim and final products. Link the schedule to critical stages in the Year 2000 program effort. Update as required.

1.6 Implement a risk management process and establish reporting system

Manage the business continuity planning tasks and activities as a sub-project within the Year 2000 program office. Assist business units in the development of individual contingency plans. Rank business risks and focus the planning effort on the greatest risk to critical core business processes. Identify project risks and develop metrics. Establish reporting system, reporting requirements, and formats. Track estimates and after each step is completed update estimates as needed, especially when new information significantly alters the estimates. Estimate and assign risk to each mission-critical system undergoing renovation or replacement. Track and compare actual costs against estimates.

1.7 Assess existing business continuity, contingency, and disaster recovery plans and capabilities

Assess existing business continuity, contingency, and disaster recovery plans for their applicability. Identify weaknesses and strengths of existing plans.

1.8 Implement quality assurance reviews

*Task the agency's quality assurance staff to review the business continuity planning processes. For example, use the quality assurance office staff to ensure that the business continuity team reviews existing contingency plans and that the existing contingency and disaster recovery plans are updated and incorporated into the business continuity plan***.** *The quality assurance reviews should examine the worst case scenarios to ensure that a feasible backup strategy--including private sector solutions--can be successfully implemented in a national emergency.*

2.0 Business Impact Analysis

The principal objective of the Year 2000 business impact analysis is to determine the effect of mission-critical information system failures on the viability and operations of agency core business processes. During the assessment phase of the Year 2000 program, agencies have assessed the impact of potential Year 2000-induced failures on core business areas and associated processes. The business impact analysis takes this process further and provides greater detail. It examines business process composition and priorities, dependencies, cycles, and service levels, and, most important, the business process dependency on mission-critical information systems.

Key Processes

2.1 Define and document information requirements, methods, and techniques to be used in developing the business continuity plan
2.2 Define and document Year 2000 failure scenarios
2.3 Perform risk and impact analyses of each core business process
2.4 Assess and document infrastructure risks
2.5 Define the minimum acceptable level of outputs and services for each core business process

2.1 Define and document information requirements, methods, and techniques to be used in developing the business continuity plan

Define the information requirements for constructing a business continuity plan. These requirements generally fall into four categories: (1) business process composition, execution cycles, and support, (2) operational priorities, service levels, dependencies, and relationships, (3) the primary and collateral Year 2000 business risks and the business scope of their impact, (4) and the costs and benefits of business continuity strategies and alternatives. Each area has detailed information requirements that are essential to providing effective business continuity. For example, the analysis of business process support should provide information on the technical, functional, organizational, and infrastructure support requirements. When collected, analyzed, and synthesized, the information defines a model of critical processes and risks to the business.

2.2 Define and document Year 2000 failure scenarios

Assess business vulnerabilities and their impacts and define the Year 2000 risk scenarios. Assume the loss of all mission-critical information systems due to post-implementation failures or delays in renovation and testing. Consider the possibility that Year 2000 date problems may be encountered earlier than expected, and address the potential disruption of essential infrastructure services, including electric power, telecommunications, and transportation. Focus agency business continuity and contingency planning efforts on likely failure scenarios.

2.3 Perform risk and impact analyses of each core business process

Monitor the status and progress of the Year 2000 program and review and verify risk metrics and critical milestones for all mission-critical systems undergoing renovation or replacement. Evaluate Year 2000-related risks posed by customers, suppliers, information technology vendors, and business partners.

Determine the impact of internal and external information system failures and infrastructure services on each core business process. Consider acquiring business impact analysis tools. These tools will provide consistent analytical structure and processes, and help to standardize the impact analyses throughout the enterprise. For the core business processes and supporting business areas, analyze both manual and automated functional requirements, manual and automated system support requirements, infrastructure support requirements, suppliers, customers, service levels, processing cycles, and the external and internal business drivers. Identify critical functions, recovery priorities and timing, and dependencies to other systems and processes.

If a core business process receives data from an external organization, contact that organization and obtain the status of its Year 2000 remediation effort. If there are reasons to be concerned, address these concerns in contingency plans.

Estimate the potential cost of service disruptions. In estimating impacts, address the duration of each disruption. Consider using a scorecard to aggregate and track the risk and impact information.

2.4 Assess and document infrastructure risks

Monitor the Year 2000 readiness of the public infrastructure, including power and telecommunications services. Assess the risk of service outages, and the potential impact of outages on the core business processes. Review existing contingency and disaster recovery plans to determine whether emergency services may be available to mitigate outages.

2.5 Define the minimum acceptable level of outputs and services for each core business process

For each core business process, define the minimum acceptable level of output and the recovery time objective.

3.0 Contingency Planning

Contingency planning integrates and acts on the results of business impact analysis. The output of this process is a business continuity plan consisting of a set of contingency plans--with a single plan for each core business process and infrastructure component. Each plan should provide a description of the resources, staff roles, procedures, and timetables needed for its implementation.

Key Processes

3.1 Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core business process
3.2 Identify and document contingency plans and implementation modes
3.3 Define and document triggers for activating contingency plans
3.4 Establish a business resumption team for each core business process
3.5 Develop and document "zero day" strategy and procedures

3.1 Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core business process

Assess benefits, costs, and risks of alternative contingency strategies. Select a strategy that is practical, cost-effective, and appropriate to the organization. In addition, the alternatives and strategies should provide a high level of confidence in recovery capability.

Three important factors in the selection process are

- *functionality: the degree to which the replacement functionality supports the production of a minimum acceptable level of output for a given core business process,*
- *deployment schedule: the time needed to acquire, test, and implement, and*
- *cost: life-cycle cost, including acquisition, testing, training, and maintenance.*

The goal is to maximize the functionality and speed of business resumption.

3.2 Identify and document contingency plans and implementation modes

Develop a contingency plan including strategies capable of meeting minimum acceptable output requirements for each core business process. Consider the following strategies:

- *quick fix,*
- *partial replacement,*
- *full redundancy or replacement, and*
- *outsourcing to the private sector.*

Consider three basic implementation modes for the quick fix, partial, and full replacement of functionality provided by failed mission-critical systems:

- *automated replacement,*
- *semi-automated replacement, and*
- *manual replacement.*

Some core business processes may be fully supported by compliant off-the-shelf application packages that can be purchased and rapidly installed. However, even projects that rely on off-the-shelf replacement packages may fall behind schedules. A semi-automated alternative can implement "bare bones" functionality, using a combination of compliant off-the-shelf applications, such as accounting software or standard database products. A manual alternative normally requires hiring and training of additional staff. While this is not a desirable solution, in some instances it may be used to replace all or part of a failed automated process. Finally, redundant business services may be provided through outsourcing contracts.

3.3 Define and document triggers for activating contingency plans

Once the business continuity planning team selects the best contingency alternative for each core business process, it must then define triggers that would implement each plan. The information needed to define the implementation triggers for contingency plans is derived from two key sources:

- *the <u>deployment schedule</u> for each contingency plan and*
- *the <u>implementation schedule</u> for the renovated or replaced mission-critical systems.*

The deployment schedule establishes the date at which the contingency plan must be implemented if is to be to be fully tested before December 31, 1999. For example, if the contingency plan calls for an 8-month deployment schedule, the tentative implementation date should be set for April 30, 1999.

3.4 Establish a business resumption team for each core business process

Work with core business process owners to establish business resumption teams and business resumption priorities. These teams would be responsible for managing the implementation of contingency plans and would deal with a wide range of operational problems, including the potential failures of systems thought to be renovated and tested, and the potential failures of external systems and data exchanges.

3.5 Develop and document “zero day” strategy and procedures

Develop a risk-reduction strategy and procedures for the period between Thursday, December 30, 1999, and Monday, January 3. This strategy may include an agencywide shutdown of all of its information systems on Friday, December 31, 1999, and a phased power-up on Saturday, January 1, 2000. The agency may consider extending the shutdown to infrastructure systems, including local area networks, elevators, and building management systems.

4.0 Testing

The objective of business continuity testing is to evaluate whether individual contingency plans are capable of providing the desired level of support to the agency's core business processes and whether the plans can be implemented within a specified period of time. In instances where a full-scale test may be too costly, the agency may consider end-to-end testing of key contingency plan components. An independent audit of the plan can validate the soundness of the proposed contingency strategy. Similarly, a legal review can provide assurance that the plans comply with government regulations and that liabilities and exposures are being adequately addressed.

Key Processes

4.1 Validate business continuity strategy
4.2 Develop and document contingency test plans
4.3 Establish test teams and acquire contingency resources
4.4 Prepare for and execute tests
4.5 Validate the capability of contingency plans
4.6 Rehearse business resumption teams
4.7 Update the business continuity plan based upon lessons learned and re-test if necessary
4.8 Update disaster recovery plans and procedures

4.1 Validate business continuity strategy

Develop and implement a strategy for validating the business continuity plan within the time that remains. A typical strategy defines a minimum number of individual and joint exercises that combine training with testing. There are several common techniques that can be employed, including reviews, rehearsals, and quality assurance audits.

4.2 Develop and document contingency test plans

Define and document the contingency test plans. Review the test plans and make needed changes. Ensure that management approves the plans. Disseminate the documents, provide guidance, and establish a help desk. Test plans should address the following:

- *test objectives,*
- *test approach,*
- *required equipment and resources,*
- *necessary personnel,*
- *schedules and locations,*
- *test procedures, and*
- *expected results and exit criteria.*

4.3 Establish test teams and acquire contingency resources

Establish test teams responsible for preparing and executing the contingency plan tests. Test preparation may include hiring and training needed staff.

4.4 Prepare for and execute tests

Assign responsibilities to test team members, including executives, observers, and contractors.

4.5 Validate the capability of contingency plans

Validate the functional capability of each contingency plan. Examine test results for accuracy and consistency and note discrepancies. For each contingency plan, ensure that

- *the plan adequately supports a core business function;*
- *there is adequate capability to manage, record, and track the contingency transactions through the alternative business process;*
- *the manual activities in particular, and the alternative business process in general, meet an acceptable level of performance;*
- *an acceptable level of quality control is provided to critical parts of the alternative business process, and an acceptable level of integrity and consistency is provided to alternative databases; and*
- *an acceptable level of security is provided to the data captured by an alternative data capture mechanism.*

4.6 Rehearse business resumption teams

Rehearse business resumption teams to ensure that each team and team member is familiar with business resumption procedures and their roles.

4.7 Update the business continuity plan based upon lessons learned and re-test if necessary

Resolve shortcomings and problems noted during testing and update each continuity plan. When under time constraints, prioritize the problem areas. For example, procedural problems involving internal administrative functions are not as serious as technical problems directly affecting the resumption of operations. Ongoing changes in systems, software, applications, communication, and operations will also require updates to the plan. A re-test may be required to ensure that the problems do not recur and that the updated plan does provide the specified capability.

4.8 Update disaster recovery plans and procedures

Update disaster recovery plans. Ensure that all newly developed or acquired contingency applications and other software components are included in the disaster recovery update cycle.

Selected Year 2000 Resources

There are many readily accessible sources of useful information on the Year 2000 problem, with many government and industry organizations establishing Year 2000 web sites. These sites provide information about Year 2000 business continuity and contingency planning issues.

Selected Year 2000 Web Sites

Federal Year 2000 Web Sites

❑ The President's Council on Year 2000 Conversion
<http://www.y2k.gov/>

❑ CIO Council Subcommittee on Year 2000
<http://www.itpolicy.gsa.gov/mks/yr2000/y201toc1.htm>

❑ MITRE/ESC Year 2000 Homepage
Y2K Contingency Management Plan Outline
<http://www.mitre.org:80/research/y2k/docs/CONTINGENCY_PLAN.html>

❑ Federal Deposit Insurance Corporation
Guidance Concerning Contingency Planning
<http://www.fdic.gov/banknews/fils/1998/fil9851b.html>

General Year 2000 Sites

❑ The Year 2000 Information Center
<http://www.year2000.com>

❑ The Institute for Electrical Engineers in the United Kingdom
<http://www.iee.org.uk/2000risk>

Business Continuity and Contingency Planning Sites

❑ Department of Information Resources for the State of Texas
Guidelines for Contingency Planning
<http://www.dir.state.tx.us/oops/ctgyplan/index.html>

❑ Disaster Recovery Institute of Canada
<http://www.dr.org/ppover.htm>

❑ University of Wisconsin - Disaster Management Center
<http://epdwww.engr.wisc.edu/dmc>

❑ Disaster Recovery Journal
<http://www.drj.com>

❑ The Journal of Business Continuity
<http://www.business-continuity.com/business_continuity.html>

Glossary

The definitions in this glossary were developed by the project staff or were drawn from other sources, including the Computer Dictionary: The Comprehensive Standard For Business, School, Library, and Home, Microsoft Press, Washington, D.C., 1991; The Year 2000 Resource Book, Management Support Technology Corp., Framingham, Massachusetts, 1996; The Year 2000 and 2-Digit Dates: A Guide for Planning and Implementation, International Business Machines Corporation, 1997; Denis Howe's "Free On-line Dictionary of Computing," at **<*http://wombat.doc.ic.ac.uk/*>**; and the Gartner Group's "IT Glossary" at **<*http://gartner5.gartnerweb.com/gartner/itglossary/dlist.html*>**.

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.

Architecture A description of all functional activities to be performed to achieve the desired mission, the system elements needed to perform the functions, and the designation of performance levels of those system elements. An architecture also includes information on the technologies, interfaces, and location of functions and is considered an evolving description of an approach to achieving a desired mission.

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

Business function A group of logically related tasks that are performed together to accomplish a mission-oriented objective.

Business plan An action plan that the enterprise will follow on a short-term and/or long-term basis. It specifies the strategic and tactical objectives of the enterprise over a period of time. The plan, therefore, will change over time. Although a business plan is usually written in a style unique to a specific enterprise, it should concisely describe "what" is planned, "why" it is planned, "when" it will be implemented, by "whom" it will be implemented, and "how" it will be assessed. The architects of the plan are typically the principals of the enterprise.

Contingency plan In the context of the Year 2000 program, a plan for responding to the loss or degradation of essential services due to a Year 2000 problem in an automated system. 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.

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

Metrics Measures by which processes, resources, and products can be assessed.

Mission-critical system A system supporting a core business activity or process.

Portfolio In the context of the Year 2000 program, an inventory--preferably automated--of an agency's information systems and their components grouped by business areas.

Quality assurance All the planned and systematic actions necessary to provide adequate confidence that a product or service will satisfy given requirements for quality.

Risk assessment An activity performed to identify risks and estimate their probability and the impact of their occurrence; it is used during system development to provide an estimate of damage, loss, or harm that could result from a failure to successfully develop individual system components.

Risk management A management approach designed to prevent and reduce risks, including system development risks, and lessen the impact of their occurrence.

Strategic IRM plan A long-term, high-level plan that defines how the agency will use information technology to effectively accomplish the agency's missions, goals, and objectives.

Strategic plan A long-term, high-level plan that identifies broad business goals and provides a roadmap for their achievement.

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

Test facility An environment that partially represents the production environment but is isolated from it, and is dedicated to the testing and validation of processes, applications, and system components.

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.

Year 2000 problem The potential problems that might be encountered by computer hardware, software, or firmware in processing year-date data for years beyond 2000.

(511469)