Certified General Accountants Association of Canada

Ready for Year 2000– a Practical Guide for Small and Medium-Sized Businesses

Canada

Industry Canada Industrie Canada

DISCLAIMER

This booklet is not intended to provide a comprehensive analysis of year 2000 issues. Nor does it claim to provide specific guidance on implementation or problem resolution. No two organizations are alike, and the year 2000 problems they face will, in all likelihood, be dramatically different. As a result, this publication is intended to offer only general guidance, which may or may not apply to the specific situation encountered by a reader.

While great care has been taken to ensure the accuracy of the information in this booklet, no guarantee of any kind is offered by the publication, its author or its publisher. If readers require assurance that a particular business or organization will be ready for the year 2000, they are advised to engage the services of an experienced and reputable Y2K remediation consultant.

Cat. No. C2-451/1999
ISBN 0-662-64395-X
52847B

Industry Canada Industrie Canada

Table of Contents

NOTE TO READERS

This practical Year 2000 guide for small and medium-sized businesses has been made possible by the Certified General Accountants Association of Canada (CGA-Canada) in partnership with Industry Canada. We hope that this tool will assist you to successfully develop and implement an action plan that addresses your Year 2000 remediation efforts. We remind and encourage business to find out more about eligibility for Finance Canada's Year 2000 tax relief. For more information on Year 2000 government initiatives, please call 1 800 O-Canada (1 800 622-6232).

Managing the Millennium

The fact that some computer systems have a problem with the year 2000 is familiar to most of us by now. The "millennium bug" or "Y2K problem" has received unprecedented coverage in the media, and for good reason. Many computer systems cannot handle dates beyond Dec. 31, 1999 — they simply weren't programmed to cope with the next century and beyond.

Efforts to correct this defect have come to be known as "Y2K remediation." The term is apt, for it encompasses not only repairing the faulty programming of older hardware and software, but also planning for related contingencies — which will be needed. After all, even if your own operation has the Y2K problem well in hand, disruptions may still occur as a result of external factors beyond your control.

This booklet provides an overview of the problem and guidance — for CGAs and for small and medium-sized enterprises — on how to develop and manage a Y2K remediation plan.

Many small and medium-sized businesses have not considered the full impact that the millennium bug might have on their operations, or believe that only larger systems will be affected by Y2K. Because of their training, CGAs may be asked by their small and medium-sized business clients for guidance on information systems and Y2K remediation. This booklet can help CGAs and their clients evaluate the risks for their businesses, and develop plans to fix the problem if it can be fixed, or manage the problem if it can't.

For more information, contact your local CGA or one of the provincial/territorial CGA associations listed on page 39 of this booklet. Or visit CGA-Canada's web site: www.cga-canada.org which features a comprehensive segment on year 2000 issues.

Understanding the Year 2000 Problem

Year 2000 just happens to be a leap year, too.

Until recently, many computer systems were programmed to store and show the year portion of a date using only two digits. For example, "1984" would be entered, stored and displayed as "84"; a date of "Jan. 15, 1984" would be stored and displayed as "15/01/84" or "84/01/15." In programming terms, the two-digit code has several benefits: it is clear and easy to use, and it takes up less storage space in the computer's memory. The format also requires less room on a printout or screen display.

But the code also contains a serious design flaw. Relying on just two digits, most computer systems automatically assume that the century has a value of "19" for any year entered. Thus, "84" is treated as "1984." Left untouched, these systems would read a date of "00," entered to designate the year 2000, as "1900." Therein lies the problem. Unless corrected, the millennium bug will introduce errors into any computer calculation or task involving code for dates beyond Dec. 31, 1999.

That's not all. Yet another design flaw exists where year 2000 dates are concerned. In general, years that have "00" as the last two digits are not leap years — except every fourth century. Year 2000 just happens to be a leap year, too. Programs that do not recognize a date of "2000" also won't recognize in February 2000 that it's a leap year. If such systems are not corrected, they will be unable to accept Feb. 29, 2000, as a valid date.

YEAR 2000 COMPLIANCE

Computer systems that correctly handle dates for 2000 and beyond are said to be "Y2K-compliant." To be Y2K-compliant, computer hardware and software must meet the following criteria (as established by the British Standards Institution):

Programmers are notoriously independent, and no single industry standard exists for naming and handling the year code in computer programs.

- No value for a current date will cause any interruption in operation.
- Date-based functionality must behave consistently for dates prior to, during and after year 2000.
- In entering or storing data, the century field must either be explicitly included or clearly created by program logic.
- Year 2000 must be recognized as a leap year.

The only way to make problematic computer programs Y2K-compliant is to modify them or replace them. Unfortunately, the problem is pervasive. For the past 40 years or so, billions of lines of computer code have been written. Much of that programming is still in use. The Gartner Group (an information technology consulting firm) estimates that it will take more than a trillion dollars to correct computer programs around the world so that they can handle year codes for 2000 and beyond.

Even at this late date, there is no consensus on how the millennium bug is to be fixed. Programmers are notoriously independent, and no single industry standard exists for naming and handling the year code in computer programs. Every line of code in every computer program needs to be checked to ensure that year codes are in working order.

INTEGRATED IMPACT

Why should you care? Well, like it or not, we are all connected in the global village. During the past two decades, our world has come to rely increasingly on computers to

guide many aspects of daily life. Computer systems (in the form of embedded systems) are now used in everything from automobiles, airplanes, trains, ocean liners and freighters to electrical circuits, telephones, appliances and life-support systems in hospitals to satellites, their positioning systems and military defence systems to nuclear reactors and submarines, hydro-electric generators and power-grid management systems. And then there's the global financial system, which is particularly vulnerable to errors arising from year 2000.

In other words, just about every aspect of your business and your personal life has the potential to be touched by Y2K failures.

During the past few years, larger corporations, organizations and governments have been hard at work, updating their computer programs for year 2000 readiness. Some have already spent hundreds of millions of dollars and they expect to be ready when Jan. 1, 2000, arrives. The forecast for small and medium-sized enterprises, however, is not so bright.

LEGAL RAMIFICATIONS

What happens if you're not ready for year 2000? Well, the legal profession expects Y2K-related litigation to dominate court schedules throughout the first decade of the new millennium. Especially vulnerable are the following groups:

- Publicly traded companies that fail to meet the Y2K deadline, thus causing significant damage to the business and, hence, low or negative earnings per share. Lawsuits can be expected to target company managers, officers and directors; they may even be directed to the auditors.
- Business partners or suppliers that fail to deliver their goods or services in a timely manner, thus causing significant interruptions to other businesses. This type of business-to-business

litigation is expected to yield the majority of damage awards.

- Service providers causing death or injury to individuals as a result of Y2K-related problems. This category might include everything from life-support system failures to traffic accidents to power outages.
- Manufacturers whose goods suffer from embedded system failures. Customers or consumers suffering damages from such goods may join in class-action lawsuits.
- Software publishers whose goods fail to handle year 2000 issues. Businesses brought to their knees by the resulting system failures could sue the publishers for damages.
- Y2K consultants and other consulting firms that fail to deliver the promised solutions. Organizations that engage such experts, only to see their systems fail in year 2000, will be eager to apply to the courts for redress.

Each organization has its own unique exposure to Y2K litigation, so it's important to consult with your legal counsel well in advance of Jan. 1, 2000.

ENSURING BUSINESS CONTINUITY

In general, business continuity insurance does not cover damages arising from Y2K problems — either from internal or external sources. Indeed, most policies exclude such damages because year 2000 problems are seen to be within management's control.

Certain enterprises may be able to purchase specific Y2K insurance policies, covering items such as lost business revenues, directors' and officers' liability and third-party claims. Typically, before underwriting the policy, the insurance company engages one or more consultants to assess the risks and determine if the business is insurable. Such policies, however, come with a very high price tag attached.

NO SILVER BULLET

There are now some software tools on the market that may help to identify some year 2000 problems in some systems; but no single product can solve all year 2000 problems. The reason stems from human nature itself. No two programmers would code the same program the same way, even from the same specifications. How they code the logic, name the variables and design the data records is practically guaranteed to differ, even though their programs will achieve the same results.

No matter what the size of your business, getting ready for the year 2000 will involve everyone in your enterprise.

As year 2000 approaches, you can expect to hear a lot more about "silver bullet" solutions — special tools that promise to solve all your Y2K problems. While their promises will sound appealing, the best advice is *caveat emptor* — let the buyer beware.

GETTING STARTED

No matter what the size of your business, getting ready for the year 2000 will involve everyone in your enterprise, from senior management, if your business is big enough to support such a category, to junior clerk. You need to ensure that everyone understands the problem and its ramifications for every aspect of your activities.

If you or your staff work from home from time to time, for example, and you exchange information between your home and office computer systems, both systems need to be Y2K-ready.

Your senior management needs to approve the Y2K strategy that your organization develops — with or without the help of an outside adviser — and be part of the task force that will ensure the year 2000-related work gets done. It may be that your business is willing to live with some inconvenience caused by the millennium bug, and if that's the case, everyone in the

organization needs to be aware of the effects of that decision.

It is important to decide what Y2K compliance means for your business. Do you aspire to rid all of your systems of the millennium bug, or would you be willing to put up with some inconvenience arising from some forms of Y2K failures? You also need to know what type of Y2K failures would be fatal to your organization and what would merely cause hardship or inconvenience. You could decide to set a different level of compliance for these situations.

Different organizations have different deadlines for Y2K compliance. Some industries, such as the financial service sector, are governed by legislation and deadline directives for Y2K compliance. Be sure to set a realistic deadline for Y2K compliance for your business.

It's a matter of assurance — and reassurance — in the months before Jan. 1, 2000. If you set your goals, appoint a project manager to be responsible, and set your deadlines, you might not be "millennium bug-free" but you'll be "bug-ready."

GETTING STARTED CHECKLIST

✓	Task	By Whom	Start	Finish
	Ensure senior management understands the Y2K problem and its potential impact on the organization			
	Ensure general awareness of the Y2K issue within the organization			
	Develop and document an overall Y2K strategy for approval by senior management			
	Establish a Y2K task force staffed by senior managers			
	Establish a Y2K planning team and appoint a project manager			
	Define Y2K compliance for your organization			
	Set a deadline for project completion			

Assessing Your Exposure

The first step in preparing for year 2000 is to assess your exposure to risk. Take an inventory of (1) things that are under your direct control, such as your organization's computer systems (internal exposures), and (2) things that are not under your control, such as the vendors or customers on which your business depends (external exposures).

At this stage, don't attempt to evaluate whether a particular system is subject to Y2K problems or what the level of exposure is for individual items on your inventory. That will come later. First, compile the inventory, making it as comprehensive as possible. (By the way, this is a great opportunity to update your organization's fixed asset inventory or to develop a comprehensive systems inventory.)

Methods for dealing with internal and external exposures will necessarily differ. At least in theory, you have control over the internal exposures: they are within your power to correct. External exposures are beyond your direct control: your efforts in those areas will be limited to mitigating any negative impact.

If you lack the skills necessary to make such an assessment, consult with the Certified General Accountant (CGA) who handles your year-ends or who helps you with your tax returns. He or she should also be able to provide an outside perspective on how the year 2000 problem will affect your internal systems, and can either provide hands-on assistance or refer you to a reputable Y2K consultant. In any case, it's advisable to ask your CGA to review your findings to ensure that nothing major has been overlooked.

IDENTIFYING INTERNAL EXPOSURES

Begin by taking an inventory of all your computer systems. Start with the hardware, since it will be the most visible. For very small businesses, computer hardware may be as minimal as a file server and a few personal computers. For small to medium-sized enterprises, computer hardware may include:

- Servers
- Workstations
- Desktop computers
- Laptop/notebook computers
- Process control systems
- Manufacturing systems
- Telecommunication systems

Now take an inventory of the software used in your organization (including systems software). This inventory might include the following items:

- Applications software (either custom designed or purchased "off the shelf")
- Local area network (LAN) server software
- Operating systems for the workstations, desktop computers and laptop/notebook computers
- Control software for processing and manufacturing
- Telecommunications software

IDENTIFYING EXTERNAL EXPOSURES

You will also want to take an inventory of all the systems that are beyond your direct control but that might affect your operations. Think about possibilities like the following:

- Government agencies
- Business partners
- Suppliers
- Vendors

- Contractors (outsource vendors)
- Customers
- Banks and other financial institutions
- Telecommunication systems providers
- Third-party systems (such as postage and courier systems)

Start by preparing two lists, one for systems that are critical to your operations and one for secondary support systems.

Consider whether the year 2000 issue will adversely affect the ability of your business partners, suppliers and vendors to deliver goods or services that are key to your organization's continued operation. If, for example, a critical aspect of your business is carried out by an outside contractor, you'll want to ensure that your contractor is matching your Y2K preparations step for step.

Do you conduct any critical part of your operation via electronic communications (such as electronic data interchange or e-mail)? If so, then consider how your business might be affected by interruptions to telecommunication systems and service.

ASSESSMENT

Once you have taken a complete inventory of your operation's internal and external exposures to the year 2000 problem, you are ready to determine the extent of exposure for each item. Start by preparing two lists, one for systems that are critical to your operations ("mission-critical" systems) and one for secondary support systems.

To assess exposure, you want to determine if any component of a system has date dependencies. Note issues like the following:

- Data entry involving date information with year code
- Storage information with year code
- Calculations using date information with year code
- Sorting by date
- Displaying date information onscreen
- Printing date information on reports

If any of the components depends on a two-digit year code, your operation probably has a Y2K problem.

Clearly, you cannot determine with certainty the level of Y2K readiness held by any of the third parties on which your organization depends. The best you can do is to send them a formal query, asking them to indicate if they will be Y2K-compliant in time. Each party's response will likely initiate a different response on your part, based on your organization's level of integration and/or dependency.

If any of the components depends on a two-digit year code, your operation probably has a Y2K problem.

You now have detailed lists outlining the levels of Y2K exposure for your mission-critical systems and for your secondary support systems.

DISCLOSURE REQUIREMENTS

As you identify and assess your enterprise's exposure to the year 2000 problem, be aware of disclosure requirements imposed by government agencies and other authorities. Publicly traded companies must follow the disclosure requirements established by securities regulators in Canada and the United States. Shareholders of publicly traded companies as well as stakeholders of not-for-profit organizations should be duly informed of the organization's Y2K preparedness. The appropriate vehicle for such messages is the annual report, accompanied by financial statements.

Given the potential for future litigation, any public disclosure should be carefully reviewed by your organization's legal counsel.

AUDITING ISSUES

The impact on an organization from the year 2000 problem may be minimal, or it may be so pervasive that every aspect of the operation is likely to be affected. Usually, the year 2000

problem will affect the efficiency and effectiveness of an organization's operation; there may or may not be any material impact on the fair presentation of the financial statements. For that reason, auditors cannot be expected or required to assess an organization's year 2000 exposure during an audit.

The auditors' role is to assess whether the financial statements fairly present "the financial position, results of operations, and cash flows in accordance with generally accepted accounting principles" (*CICA Handbook*, section 5400.04). Even if the year 2000 issue has a major impact on an organization's operations and financial results, as long as the financial statements fairly present such results, the auditors have fulfilled their responsibility.

Small and medium-sized enterprises that require outside assistance to assess the impact of the year 2000 should not assume that their CGA will include such an assessment as part of the annual audit. Rather, they should arrange for Y2K services in a separate engagement, either with their CGA if he or she offers this service, or with a reputable Y2K consultant.

PROFESSIONAL GUIDELINES

CGAs should be aware of recommendations issued by the International Federation of Accountants (IFAC) and the Canadian Institute of Chartered Accountants (CICA) concerning the year 2000:

- IFAC IAPS 1011, Implications for Management and Auditors of the Year 2000 Issue, was published by the International Auditing Practices Committee, July 1998.
- The CICA has published a variety of Accounting Guidelines and Assurances and Related Services Guidelines that provide specific guidance for the treatment of the year 2000 issue in accounting and review and auditing engagements.

ASSESSMENT CHECKLIST				
✓	Task	By Whom	Start	Finish
	Identify internal and external exposures			
	ASSESSMENT OF INTERNAL EXPOSURES			
	Take complete inventory of hardware			
	Take complete inventory of software			
	Identify mission-critical systems			
	Identify secondary support systems			
	Assess the impact of Y2K-induced failures on all internal systems			
	Review insurance policies and assess legal and liability exposures			
	Identify disclosure requirements that your organization is required to meet			
	Evaluate risks and tradeoffs for all internal exposures			
	ASSESSMENT OF EXTERNAL EXPOSURES			
	Take complete inventory of external parties that may have a Y2K-related impact on the organization			
	Determine the impact of external party failures on mission-critical systems			
	Determine the impact of external party failures on secondary support systems			
	Identify disclosure requirements			
	Assess legal exposures to external party failures			

Evaluating the Risks and Tradeoffs

Not all computer systems are created equal. Some support a business's mission-critical functions; others support administrative or secondary functions. While you may want to correct all Y2K-related problems, your first priority is to fix those systems deemed "mission critical."

Two approaches can be taken with any system that is not Y2K-compliant:

1. It can be fixed ("remediated").
2. A "workaround" solution can be devised.

Depending on the situation, workarounds may be very cost effective, even if they only provide a temporary solution until you have the time to fix the problem. Suppose, for example, you know that your payroll system will not be ready when year 2000 arrives. A workaround is to arrange for a bank or one of the payroll service bureaus to take care of payroll for the first few months until you have the time to have your payroll system fixed or replaced.

Now determine the tradeoffs between remediation and workaround solutions for each of the internal and external exposures you have identified. The fact that some systems are not Y2K-compliant may result in a minor inconvenience, albeit one you can live with in the short term. For other systems, Y2K non-compliance may cripple the entire organization, an inconvenience you definitely want to live without.

If you lack the skills needed to evaluate the risks and tradeoffs outlined in this section, consult with a systems expert or your CGA. The process of evaluation is vital, for it will provide you with a list of priorities as you begin to develop your Y2K remediation plan.

EVALUATION CHECKLIST			
✓	Question the risk	Answer	From whom
	What if the system is not Y2K-compliant on the first business day in year 2000?		
	What if the system is not Y2K-compliant for the first business week in year 2000?		
	What if the system is not Y2K-compliant for the first month in year 2000?		
	What if the system cannot handle the date of Feb. 29, 2000?		
	What if the system can never be made Y2K-compliant?		

Developing a Year 2000 Plan

After identifying your enterprise's exposure to the year 2000 problem and assessing the risks and tradeoffs, you are ready to develop a Y2K remediation plan. There are a few things to consider, however, before you get into the details of your plan.

First, recognize that a shortage of skilled personnel may be the single biggest constraint to any planning effort. Staff assigned to Y2K projects must come from existing departments. You may not have the personnel to staff all your Y2K projects at once, and you'll be forced into some form of serial planning.

What if your organization lacks skilled personnel? In that case, you'll want to consider hiring that reputable Y2K consultant mentioned earlier. Realize that the later you start your Y2K projects, the higher your outsourcing costs will be as other organizations help to bid up the price attached to such services.

Do not overlook the need for additional hardware resources. Many Y2K projects involve duplicating entire systems for development and testing.

As the projects get under way, your organization cannot afford to "freeze" all the systems under review. Managing changes that are not related to the year 2000 problem will require extra effort in co-ordination, monitoring and planning during this period.

SYSTEM REMEDIATION

Whether you undertake the remediation plan as a hands-on project within your business, or choose to manage the project with the help of an outside consultant, the following questions should be answered as part of your remediation

plan. Consider each system on your exposure list and determine the following:

- What is covered by the warranty? Most off-the-shelf software is provided on an "as is" basis, and does not come with a warranty for suitability of use. Even if your vendor provided a guarantee that the software was suitable for the intended use, the guarantee is unlikely to cover any damage that may arise from such use (the so-called "waiver of liability" clause).
- Do you have the source code (the actual computer programs)? If you do not, remediation may be out of the question. Try to contact the company or individual in possession of the source code. If you cannot locate the code, you have only one course of action: replace the system. (Note that source code is generally not provided for off-the-shelf software.)
- If you have the source code, who owns the rights to it? You may be surprised to learn that, although your organization has the code, someone else holds the rights to it. If that's the case, try to contact the owner of the code for help with the remediation.
- Does the source code match the programs that are in use? A programmer or systems consultant might need to be called in to determine this.
- How much effort is required to make the system Y2K-compliant?
- What are the compliance deadlines? Experts recommend setting such deadlines at least three months before the point of impact.

Typically, you will *not* have the source code for each off-the-shelf system in need of remediation. Contact the manufacturer of the system to determine:

- The status of Y2K compliance for the version you have; and

- Whether a newer, Y2K-compliant version is available and at what cost.

SCHEDULES AND BUDGETS

Prioritize your projects, starting with those systems you think are "mission critical," followed by those for which a workaround solution may be acceptable.

Now you are ready to develop your Y2K remediation plan. For each of your systems, develop a timeline and a budget, and identify the resources (human and machine) needed to implement and test. Consider outsourcing specific projects, which may prove to be more cost effective in some cases — or it may be the only option available for your business. Once again, you must prioritize your projects, starting with those systems you think are "mission critical," followed by those for which a workaround solution may be acceptable.

Last but not least, you'll need to test to confirm that remediation efforts are effective.

As you consider each system, review the following options:

- **Eliminate** — Ask yourself if the business still needs the system. Why repair, replace or update a system if it is no longer required?
- **Repair** — For systems that continue to serve your needs, corrections to ensure compliance may be the appropriate option. You will, however, need to have the source code, the rights to it and the technical resources to make the corrections.
- **Replace** — For systems that cannot or should not be fixed (either because no source code is available or because the system no longer serves the needs of the organization), replacement may be appropriate. Consider off-the-shelf solutions, which may be less expensive and less risky. Avoid the temptation to re-engineer the business — this is not the time. Instead, focus on replacing outmoded functions with Y2K-compliant ones.

- **Update** — In many cases, the original vendor for an off-the-shelf application (either hardware or software) will have released an updated version that is Y2K-compliant. If so, it's easiest to get the updated application. Look carefully, however, at the vendor's claims that the new product is Y2K-compliant, and get the claims in writing.

Familiarity with some of the other techniques will make it easier for you to manage your remediation plan.

FIXING THE PROBLEM

Fixing systems to make them Y2K-compliant doesn't necessarily mean expanding the year code from two to four digits. That is simply one technique that can be used. Familiarity with some of the other techniques will make it easier for you to manage your remediation plan.

- **Date expansion** — While this is the most costly approach, it is also the most complete. Here a year field in a system is expanded to four digits, thus changing the way calculations using the field are handled. The solution is permanent — at least until the year 10,000. This approach means that data files and databases must be reorganized, and all programs that access such files and databases must be modified.
- **Date windowing** — This is by far the most popular technique and works in all situations where the data does not span more than 99 years. Instead of expanding the date field to four digits, you can modify the system so that it automatically interprets the two-digit year code as being in either the 20th or 21st century, depending on the current year. This technique requires you to set a 99-year window, picking any year as the base year (called the "pivot year"). For example, suppose 1960 is the base year in the date window. To determine which century the current year is in (suppose that the year value is 99), subtract the base year (in this case it is 60)

from the current year. If the result is positive, the current year is in the 20th century. If the result is negative (suppose, for example, the year value is 00), the current year is in the 21st century. At the beginning of every year, modify the system to increase the base year by one to slide forward.

- **Date encryption** — This is also a relatively simple technique that does not require expanding the year field to four digits. Instead, a four-digit year value is encrypted to fit into a two-digit field. When fetched, the "crammed" year value is decrypted by using a special routine back to four digits.
- **Century field** — Instead of expanding the year field to four digits, a "century field" is added to indicate whether the two-digit year belongs to the 1900s or the 2000s.

WORKAROUND SOLUTIONS

The key to a good workaround solution is to ensure that the workarounds yield the same results or achieve the same purpose as repairing the problem would do. Outsourcing the payroll system temporarily, as mentioned earlier, achieves an equivalent result in the short term. Or, suppose your building's security system is date-sensitive and will not be ready for Year 2000. You could, as a workaround solution, disable the electronic security system, and install locks until you have the time to fix or replace the electronic system. Faced with too many remediation projects or too little time, you may have to opt for workaround solutions. Review the risks you outlined earlier concerning how long a particular system could run after Jan. 1, 2000, without being Y2K-compliant.

REMEDIATION CHECKLIST				
✓	Task	By Whom	Start	Finish
	REMEDIATION			
	Develop a work plan and identify remediation/ workaround projects			
	Determine remediation approach (eliminate, repair, replace or update)			
	Select course of action for fixing the Y2K problem (date expansion, date windowing, date encryption or century field)			
	Convert programs, files and databases			
	Conduct unit tests			
	WORKAROUND			
	Identify workaround and determine duration			
	Develop workaround procedures			

Implementing the Plan

As with any endeavor, the key to a successful Y2K remediation project lies in its implementation. Each project requires:

- Appointing a manager;
- Assembling a team; and
- Identifying project objectives, timelines and budgets.

Establishing milestones and tracking progress are also critical when it comes to managing Y2K projects. Close monitoring ensures early detection when projects are delayed or go over budget. And the sooner corrective actions are taken, the less likely it is that the project will slide off course.

As you oversee your organization's Y2K projects, focus on concrete deliverables. Avoid the pitfall of "90% complete"—it offers no practical value. If every aspect of a Y2K project is 90% complete, then every aspect is incomplete. Break the project into its components and find out when each element will be finished.

IMPLEMENTATION CHECKLIST

✓	Task	By Whom	Start	Finish
	Appoint project manager			
	Establish resource requirements, timelines and budgets			
	Assemble project team			
	Establish milestones by identifying which systems need to be fixed first, and what constitutes completion			
	Monitor costs and track project progress			
	If new procedures are required, make sure staff are trained to use the new procedures			
	If workarounds are used, ensure staff can use the workarounds and are well informed of the impact			

Testing for Year 2000 Readiness

Typically, more than 50% of the resources and time allotted to a Y2K remediation project will be expended in testing. Indeed, it's fair to say that the design of the test plan and its execution are the most essential factors in a project's success. Even before a project gets under way, your test plan should be in development.

Ideally, you want your test to clearly demonstrate whether a system has become Y2K-compliant according to your specified criteria. Your plan should therefore include developing scripts for testing every possible condition and combination of conditions. This type of testing is known as "quality assurance" (QA).

QA testing generally involves the following phases:

- **Unit testing** — This phase is conducted for each program after it has been fixed to ensure that repairs have been implemented correctly and that no new errors have been introduced.
- **Integration testing** — If several programs are required to interact with each other within a system module, then they are tested together to ensure the interface works as it should.
- **System testing** — An entire system is tested. Where a system has different operating cycles (for example, most accounting systems have day-end, month-end, quarter-end and year-end cycles), each cycle must be tested.
- **Regression testing** — If an error is encountered during any phase of the testing, it must be corrected, and all phases of testing up to the point of failure must be repeated. This ensures that any new errors introduced by the "fix" are detected before the next stage of remediation gets under way.

TESTING CHECKLIST				
✓	Task	By Whom	Start	Finish
	Develop test procedures			
	Conduct unit tests			
	Conduct integration tests			
	Conduct system tests			
	Conduct regression tests			
	Involve end-users in testing remediated systems			
	Involve end-users in testing workarounds			

Business Continuity Planning

Time is running out for solving every aspect of the year 2000 problem. If you have a small or medium-sized enterprise, and you've not yet started your Y2K preparations, you may be unable to put every system you use in your operations into good order before the new millennium arrives.

Indeed, the risk of failure is not limited to organizations that have yet to develop a Y2K remediation plan. Let's say that you have done everything you can to limit the year 2000 problem within your organization. Your job is not over yet. You still have to limit the risks your business faces from Y2K failures on the part of business partners, government agencies, banks and the providers of the infrastructure services. One way or another, we all depend on services provided by the public infrastructure — telephone and telecommunication services, power, water, transportation and police and military protection.

That's where business continuity planning comes in. This "big picture" planning is intended to (1) reduce such risks and (2) ensure that your organization is able to maintain a specified minimum level of production and/or service in the face of major Y2K-related failures.

EXISTING CONTINUITY PLANS

Many businesses already have disaster recovery plans in place that ensure the continuity of core business processes by identifying, assessing and mitigating business risks. Most disaster recovery plans, however, cannot deal adequately with Y2K-related disruptions. For starters, they suggest alternatives for dealing with failures that arise from a single

cause, such as an earthquake, flood, power outage or act of terrorism. Y2K failures may stem from multiple causes, and the usual alternatives may not be viable.

Y2K failures may stem from multiple causes, and the usual alternatives may not be viable.

For example, a contingency identified as part of your continuity plan might suggest using a "hot site" or backup server if the main server goes down. But if the server failure stems from an inability to handle year 2000 dates, chances are the backup server or the hot site will have the same problem. Replacing corrupted databases using backup files (another technique commonly outlined in disaster recovery plans) may not even be an option. In all likelihood, the backup copy will suffer from the same Y2K problems as your business's databases.

Y2K CONTINUITY PLANS

Clearly, businesses require a Y2K business continuity plan to deal with failures like the ones just outlined. Typically, such a plan provides for (1) business impact analysis, (2) Y2K contingency strategies and (3) testing and validation.

PHASE I: BUSINESS IMPACT ANALYSIS

Your initial step is to assess the impact that a Y2K failure, from either internal or external causes, would have on your core business processes. You need to determine how vulnerable these processes are and imagine scenarios resulting from Y2K failure.

1. Assume that all your mission-critical systems are lost due to Y2K problems from internal or external sources.
2. Assess which aspects of your mission-critical systems are likeliest to fail.
3. Assess the impact from such failures and from the disruption of infrastructure services. Different organizations have

different levels of tolerance for such disruptions. Travel agencies, for example, could not easily survive telecommunications disruptions that affect reservation networks or telephone service. Other businesses, such as retail outlets or restaurants, could likely survive this type of disruption, at least in the short term.

4. Identify the minimum acceptable levels of production or service for each of your core business processes.
5. Determine the time that can elapse before recovery. Faced with a telecommunications failure, for example, a retail business would likely turn to cash-only sales or accept credit-card purchases up to a certain limit. In this way, the business could still operate for a time even without the benefit of online confirmation.

After you've assessed what impact the millennium bug would have on your mission-critical systems, you're ready to prepare your Y2K contingency strategies.

PHASE II: Y2K CONTINGENCY STRATEGIES

After you've assessed what impact the millennium bug would have on your mission-critical systems, you're ready to prepare your Y2K contingency strategies. These involve the specific details of "if 'x' fails, we'll do 'y'." Your strategies, however, should not be limited to overcoming any failure of your own systems; they must also encompass possible Y2K failures experienced by your business and trading partners, service providers and critical elements of the infrastructure within which your business operates.

Y2K contingency strategies deal with two types of failures — remediation failures and core business process failures. A separate contingency strategy should be prepared for each potential failure within these two categories.

- A remediation failure occurs when mission-critical systems have not been repaired in time for the year 2000. Such failures can also arise from errors in the remediation

process that are not detected during testing but that cause mission-critical systems to fail on or after Jan. 1, 2000.

- A core business failure stems from unforeseen problems that arise on or after Jan. 1, 2000. It doesn't matter if this failure results from problems within your business that you didn't anticipate, or problems that some other organization didn't anticipate. The effect will still be to disrupt your core business activities, and your contingency strategies will be aimed at getting your business back in operation as quickly as possible.

Remediation contingency strategies should focus on your mission-critical systems. For each system, you need to:

- Identify available alternatives if remediation efforts are not completed in time or are faulty;
- Assess whether system vendors or service providers are likely to be ready in time, and identify alternative vendors that will be ready; and
- Establish "trigger" dates for activating your contingency strategy or strategies.

Because of the nature of Y2K-related problems, errors in data processing may not be detected until the arrival of the year itself. Contingency strategies must therefore specify the techniques that you will apply when you discover these errors.

Such techniques will include:

- Identifying the last version of records prior to the onset of erroneous processing;
- Outlining procedures for resetting system dates, restoring databases, changing programs and system-run controls;
- Scheduling reprocessing cycles;
- Co-ordinating with systems and/or external parties with which your system interacts; and
- Repairing and recovering programs, systems, data,

customer relations and other affected areas.

You'll need to watch for plausible-but-erroneous data as one of the problem areas in your remediation contingency strategies.

CHECK THAT DATE

Y2K contingency strategies must address date issues other than Jan. 1, 2000. Critical Y2K dates will vary by industry and business application, but may include:

- Dec. 30, 1999 (last business date in 1999)
- Dec. 31, 1999 (last day in 1999)
- Jan. 1, 2000 (first day in 2000)
- Jan. 3, 2000 (first business day in 2000)
- Jan. 10, 2000 (first seven-digit date)
- Jan. 31, 2000 (last day of first month)
- Feb. 29, 2000 (leap year day)
- Oct. 10, 2000 (first eight-digit date)
- Dec. 31, 2000 (last day in 2000)

Core business contingency strategies are broader in scope than remediation contingency strategies. Your first step is to identify those processes on which the operation and survival of your business depend. A core business process may involve internal and external resources. For example, if you operate a retail store, replenishing goods is a core business process that may involve:

- Internal data processing systems, such as those used for purchase orders and inventory control;
- Other business processes, such as placing orders, tracking the receipt of goods and shipping goods to the retail store; and
- External systems that you use to manufacture and deliver the goods.

Core business contingency strategies are vital to any Y2K project for, despite your best efforts to remediate and test business systems and processes, the potential still exists for some of the core business processes to fail. You should put each of your core business processes through the following six-step process:

Despite your best efforts, the potential still exists for some of the core business processes to fail.

1. **Identify the alternatives.** Can an alternative process provide acceptable levels of production or service? If, for example, the core business process involves ordering parts from a supplier, a possible alternative might be to stock additional inventory before the arrival of year 2000. That way, you will be able to withstand a short delay should the supplier develop Y2K-related problems. You will also buy yourself some extra time, which may enable you to place an order with another supplier.

2. **Assess the cost and benefits.** It's important to select an alternative that is practical and cost-effective. Make sure that:

- The alternative can provide an acceptable (minimum) level of output;
- There is adequate time to establish, test and implement the alternative; and
- All costs, including acquisition, testing, implementation, training and maintenance are identified.

3. **Develop and document the contingency strategies.** You will want to add the following strategies to your Y2K arsenal:

- The quick fix — Can you over-stock items or use a different process? Document any possibilities now so that clear heads can prevail if a contingency arises.
- Partial replacement — Can a problematic automated component be replaced with a manual process or a new component?
- Complete replacement — Can an entire system be replaced? Also consider the timing issues for implementing any replacement system.

- Outsourcing — Can you arrange for an external party to provide the required service should your system fail?

4. **Determine the trigger conditions.** What conditions will activate the contingency strategy? Your plan must be tested and ready for deployment well before Dec. 31, 1999.

Rehearse or drill your team as often as possible so that, should a failure arise, the team is ready.

5. **Appoint the key person.** Typically, this will be the operational or divisional manager in charge of the core business process. This individual assumes "ownership" of the process and is responsible for checking for Y2K failures and activating the contingency strategy.
6. **Establish and train the business resumption team.** For each core business process, identify and train a small team to implement the contingency strategies. You may choose to select just one person or you may require several people in different departments. Rehearse or drill your team as often as possible so that, should a failure arise, the team is ready to put the contingency strategies into operation.

PHASE III: TESTING AND VALIDATION

At this point, you need to test each of your contingency strategies to evaluate how effective your business continuity plan is. If your business is subject to regulatory or statutory requirements or has some level of exposure to Y2K litigation, ask your legal counsel to review your contingency strategies to ensure that they comply with governmental regulations and that liabilities and legal exposures are adequately addressed.

In general terms, testing and validation involves:

- Reviewing the business continuity plan to determine whether the organization can indeed survive Y2K problems through its contingency strategies;
- Developing a comprehensive, documented test plan;

- Establishing the test team (recognizing the impact testing may have on operations);
- Using external resources where appropriate;
- Executing the test plan, following the predetermined test procedures;
- Assessing the test results and identifying failures;
- Ensuring the business resumption team is trained; and
- Updating contingency strategies where weaknesses are identified.

In spite of your best efforts, your organization may still encounter unforeseen Y2K problems — problems that could cripple operations. Your only safeguard is a properly designed and tested set of contingency strategies.

BUSINESS CONTINUITY CHECKLIST

✓	Task	By Whom	Start	Finish
	BUSINESS IMPACT ANALYSIS			
	Identify core business processes			
	Identify mission-critical systems			
	Identify minimum acceptable levels of production or service from core business processes or mission-critical systems			
	CONTINGENCY STRATEGIES			
	Assess exposures to remediation failures			
	Develop remediation contingency strategies			
	Assess exposures to core business failures			
	Develop core business contingency strategies			
	TESTING AND VALIDATION			
	Review business continuity plan			
	Develop test plan			
	Conduct tests			
	Assemble business resumption team			
	Rehearse or drill business resumption team			

A Word about Personal Preparedness

Depending on your level of risk aversion, you may or may not want to be on an airplane as 1999 changes into 2000.

No one can tell you in advance what you will personally encounter in the way of year 2000 problems. Much depends on what you do, where you are and your state of readiness. Purchasing a Y2K "survival kit" seems excessive; but there are specific steps you can take to mitigate any personal impact from Y2K. Here are some issues to consider when planning for year 2000:

- Before Jan. 1, 2000, make arrangements to have on hand two weeks' worth of cash. While your bank may well be Y2K-compliant on the first business day of 2000, you probably won't want to risk running out of cash or enduring long lineups, should local ATM outlets fail.
- Keep a hard copy of the December 1999 statement of all your investments, RRSPs, insurance policies and so on. Just in case an insurer's or financial institution's records do get mixed up, you will still have up-to-date proof of ownership.
- For the same reason, keep a hard copy of the December 1999 statement of all your credit cards and bank cards. Also store up-to-date hard copies of any 1999 assessments, such as those for property or business tax.
- Postpone elective surgery. You don't want to be in a hospital on or near Jan. 1, 2000. Even a minor surgical procedure can sometimes have complications. Why chance a life-support system failure if it can be avoided?
- Depending on your level of risk aversion, you may or may not want to be on an airplane as 1999 changes into 2000. A modern plane has more than 500 embedded systems.

Granted, most of those systems do not have date dependencies, but no one really knows what risks the date rollover poses to air transportation. And there's the destination to consider, too. Are you confident that the airport control system at your destination will be Y2K-compliant?

- If you nix flying, you probably won't want to be traveling by ocean liner, either. Most cruise ships contain numerous embedded and navigation control systems. Then again, if you're a risk-taker, this may be the sort of millennium thrill you've been looking for.
- Consider adding an alternative heating system to your residence if your present system depends on electricity. Most utilities expect to be Y2K-compliant, but some areas may be subject to temporary blackouts. Can you maintain an acceptable level of comfort in your home — in January — without heat, bearing in mind that most central heating systems require electricity to operate properly?

Ready for Year 2000

Don't wear yourself out worrying about the year 2000 problem. Yes, there are likely to be a few rough spots — in both your business and your personal life. But after reading this booklet, you should have a better idea of what the year 2000 implies. You will also have a general understanding of how to develop and implement a Y2K remediation plan for your business. If you lack the skills required to assess your enterprise's exposure to Y2K-related risks or to implement a remediation project or contingency strategies, contact a reputable consultant or professional adviser.

A wealth of information on the year 2000 issue is now available on the world wide web as well as at your library or local bookstore. An annotated list of useful web sites and some of the better-known books and publications is available through CGA-Canada's own web site:
English: http://www.cga-canada.org/eng/resource/y2k.htm
French: http://www.cga-canada.org/fr/resource/y2k_f.htm

These sources are published online so that CGA-Canada can keep the information you need current and can add new information and links as January 1, 2000, approaches.

For more information on how a Certified General Accountant (CGA) can help with your year 2000 preparations, contact your local CGA Association.

ABOUT THE AUTHOR

John W. Yu, M.Sc., CDP, FCGA, is the co-founder of an Internet company (www.CGAonline.net) providing online services to accountants. He is the executive editor of two online magazines (www.accountantsledger.com and www.itaudit.org) and is also the technical editor of *CGA Magazine*'s "Micromation" column.

For More Information

CGA-British Columbia
1555 West 8th Avenue
Vancouver V6J 1T5
Tel: (604) 732-1211
Fax (604) 732-1252
Toll free: 1-800-565-1211

CGA-Alberta
1410-555 4th Avenue S.W.
Calgary T2P 3E7
Tel: (403) 299-1300
Fax: (403) 299-1339
Toll free: 1-800-661-1078

CGA-Northwest Territories
P.O. Box 128, 3rd Floor
5016 50th Avenue
Yellowknife X1A 2N1
Tel: (867) 873-5620
Fax: (867) 873-4469

CGA-Yukon Territory
P.O. Box 5358
Whitehorse Y1A 4Z2
Tel: (867) 668-4461
Fax: (867) 667-5790

CGA-Saskatchewan
4-2345 Avenue C North
Saskatoon S7L 5Z5
Tel: (306) 955-4622
Fax: (306) 373-9219

CGA-Manitoba
4 Donald Street South
Winnipeg R3L 2T7
Tel: (204) 477-1256
Fax: (204) 453-7176
Toll free: 1-800-282-8001

CGA-Ontario
240 Eglinton Avenue East
Toronto M4P 1K8
Tel: (416) 322-6520
Fax: (416) 322-6481
Toll free: 1-800-668-1454

Ordre des comptables généraux licenciés du Québec
445, boul St-Laurent
Bureau 450
Montréal H2Y 2Y7
Tel: (514) 861-1823
Fax: (514) 861-7661

CGA-New Brunswick
Commerce Building
P.O. Box 1395
24-236 St. George Street
Moncton E1C 1W1
Tel: (506) 857-0939
Fax: (506) 855-0887
Toll free: 1-877-462-4262

CGA-Nova Scotia
5251 Duke Street
Suite 416
Halifax B3J 1P3
Tel: (902) 425-4923
Fax: (902) 425-4983

CGA-Prince Edward Island
P.O. Box 812
Charlottetown C1A 7L9
Tel: (902) 368-7237
Fax: (902) 368-3627

CGA-Newfoundland
AGRA Building
Suite 103, 133 Crosbie Road
St. John's A1B 1H3
Tel: (709) 579-1863
Fax: (709) 579-0838
Toll free: 1-800-563-2426

Caribbean Region Office
c/o Systems - CGA
P.O. Box 16B
Letchworth Office Complex
The Garrison
St. Michael, Barbados
West Indies
Tel: (246) 429-5201
Fax: (246) 429-4379

CGA-Bermuda
c/o Bermuda College
South Shore Road
PO Box PG 297
Paget PG BX, Bermuda
Tel: (441) 236-9000
Fax: (441) 239-4011

CGA-Bahamas
P.O. Box SS 5047
Nassau, Bahamas
Tel: (242) 393-0224
Fax: (242) 393-7570

Asia Pacific Region Office
Room 1008, Lippo Centre
Tower 2, 89 Queensway
Hong Kong
Tel: 011-852-2858-1712
Fax: 011-852-2559-4536

Certified General Accountants
Association of Canada
700 – 1188 West Georgia Street
Vancouver, British Columbia
Canada V6E 4A2
Telephone: (604) 669-3555
Fax: (604) 689-5845
Toll Free: 1-800-663-1529
Web Site: www.cga-canada.org

Industry Canada Industrie Canada
Canada

Task Force Year 2000 Secretariat
Industry Canada
300 Slater Street
North Tower, 18th Floor
Ottawa, Ontario
K1A 0C8
Web Site: Strategis.ic.gc.ca/sos2000
or Call 1 800 O-CANADA (1 800 622-6232)